IN THE MATTER OF AN INDEPENDENT REVIEW PROCESS
BEFORE THE INTERNATIONAL CENTRE FOR DISPUTE RESOLUTION

AFILIAS DOMAINS NO. 3 LIMITED,

Claimant

v.

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS,

Respondent

ICDR Case No. _____

EXHIBITS TO
WITNESS STATEMENT OF JONATHAN M. ROBINSON

LIST OF EXHIBITS

Exhibit No.	Description
JMR-1	Jonathan Robinson, Candidate Statement for GNSO Chair (28 Sep. 2012)
JMR-2	Jonathan Robinson, Candidate Statement for GNSO Chair (8 Nov. 2013)
JMR-3	Jonathan Robinson, Candidate Statement for GNSO Chair (3 Oct. 2014)
JMR-4	ICANN, *News Release: Jonathan Robinson Recognized with 2014 ICANN Leadership Award* (13 Oct. 2014), *available at* https://www.icann.org/news/announcement-2014-10-13-en (last accessed on 12 July 2018)
JMR-5	Afilias, *News Release: Afilias Chairman Jonathan Robinson Wins ICANN's 2016 Leadership Award at ICANN 57* (7 Nov. 2016), *available at* https://afilias.info/news/2016/11/07/afilias-chairman-jonathan-robinson-wins-icann%E2%80%99s-2016-leadership-award-icann-57 (last accessed on 12 July 2018)
JMR-6	NTIA, Improvement of Technical Management of Internet Names and Addresses; Proposed Rule [Docket No. 980212036-8036-01] (20 Feb. 1998), *available at* https://www.ntia.doc.gov/federal-register-notice/1998/improvement-technical-management-internet-names-and-addresses-proposed- (last accessed on 23 Sep. 2018)
JMR-7	ICANN, Memorandum of Understanding between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers (25 Nov. 1999), *available at* https://www.icann.org/resources/unthemed-pages/icann-mou-1998-11-25-en (last accessed on 14 Feb. 2018)
JMR-8	ICANN, Articles of Incorporation of Internet Corporation for Assigned Names and Numbers (as revised on Nov. 21, 1998), *available at* https://www.icann.org/resources/pages/articles-2012-02-25-en (last accessed on 26 Sep. 2018)
JMR-9	ICANN, Bylaws for Internet Corporation for Assigned Names and Numbers (15 Dec. 2002), *available at* https://www.icann.org/resources/unthemed-pages/bylaws-2002-12-15-en (last accessed on 10 Sep. 2018)
JMR-10	ICANN, Registry Agreement between Internet Corporation for Assigned Names and Numbers and Network Solutions, Inc. (10 Nov. 1999), *available at* https://archive.icann.org/en/nsi/nsi-registry-agreement-04nov99.htm (last accessed on 14 May 2018)
JMR-11	NTIA, Statement of Policy on the Management of Internet Names and Addresses [Docket No. 980212036-8146-02] (5 June 1998), *available at* https://www.ntia.doc.gov/print/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses (last accessed on 23 Sep. 2018)

Exhibit No.	Description
JMR-12	ICANN, New gTLD Application Submitted to ICANN by Afilias Domains No. 3 Limited, Application ID: 1-1013-6638 (13 June 2012)
JMR-13	ICANN, New gTLD Application Submitted to ICANN by Charleston Road Registry Inc., Application ID: 1-1681-58699 (13 June 2012)
JMR-14	ICANN, New gTLD Application Submitted to ICANN by Schlund Technologies GmbH, Application ID: 1-1013-77165 (13 June 2012)
JMR-15	ICANN, New gTLD Application Submitted to ICANN by Nu Dot Co. LLC, Application ID: 1-1296-36138 (13 June 2012)
JMR-16	ICANN, New gTLD Application Submitted to ICANN by Web.com Group, Inc., Application ID: 1-1009-97005 (13 June 2012)
JMR-17	ICANN, New gTLD Application Submitted to ICANN by DotWeb Inc., Application ID: 1-956-26846 (13 June 2012)
JMR-18	Derek Vaughn, *InetServices, Industry Insights & News: Inside the High Stakes Auction for .WEB* (25 July 2017), *available at* https://www.inetservices.com/blog/inside-the-high-stakes-auction-for-web/ (last accessed on 23 Sep. 2018)
JMR-19	Peter Lamantia, ".WEB Acquired for $135 Million. Too much? How does it compare?," *Authentic Web*, *available at* https://authenticweb.com/brand-tlds-digital-strategies/dot-web-acquired-for-135-million/ (last accessed on 23 Sep. 2018)
JMR-20	Kevin Murphy, "Verisign likely $135 million winner of .web gTLD," *Domain Incite* (1 Aug. 2016), *available at* http://domainincite.com/20820-verisign-likely-135-million-winner-of-web-gtld (last accessed on 23 Sep. 2018)
JMR-21	Cybele Negris, "How a $135 million auction affects the domain name industry and your business," *BIV* (10 Aug. 2016), *available at* https://biv.com/article/2016/08/how-135-million-auction-affects-domain-name-indust (last accessed on 23 Sep. 2018)
JMR-22	"The Next Big Domain Extension" in *This Week in SEO 60: Brands, Domains, and Youtube*, *available at* https://supremacyseo.com/TWS60 (last accessed on 23 Sep. 2018)
JMR-23	ICANN, Bylaws for Internet Corporation for Assigned Names and Numbers (as amended 18 June 2018), *available at* https://www.icann.org/resources/pages/governance/bylaws-en (last accessed on 4 Sep. 2018)

EXHIBIT JMR-1

Candidate Statement for GNSO Council Chair

Candidate: Jonathan Robinson

Date: 28 September 2012

I am pleased to accept the nomination and to sincerely thank Jeff Neuman, Registries Stakeholder Group Councillor and Vice Chair of the GNSO Council for making it.

Personal Qualifications

I am an experienced company director, manager and specialist in a variety of areas which are directly relevant to the complex blend of issues that the GNSO Council has to navigate. As well as specialist domain name industry experience, I have broader international and multi-stakeholder environment experience gained in the academic, not-for-profit and public purpose areas. I have lived and worked for extended periods of time in both the developed and developing world. My style is that I value careful consideration, balanced judgement and ultimately, productive output.

My recent professional experience has included:

- Over 10 years as main board director of public, quoted company, Group NBT plc
- Over 10 years as non-executive director of Afilias Limited (.info, mobi & .pro)
- 3 x 2 years as a member elected non-executive director, Nominet (UK) Ltd (.uk)

Prior to the development of ICANN, I was involved in work which involved active participation in a series of international meetings and included a term as deputy chairman on the board of the Internet Council of Registrars (CORE) back in 1997. Since ICANN's inception, I have attended a minimum of one ICANN meeting per year and every meeting since being elected to the GNSO Council in December 2010.

I hold a BSc (Physics) and a PhD (Engineering) degree from the University of CapeTown, South Africa. I previously undertook research at the University of Cambridge, Cambridge, UK, Imperial College, London, UK and the Lawrence Berkeley Laboratories, University of California, USA.

Role of the GNSO Council

It is evident to all that ICANN is at an absolutely critical point in its development. The organisation has recently embarked on the execution phase of the most ambitious project and role in its history; and it is therefore now facing unprecedented operational and broader challenges, including to the ICANN model itself. ICANN's role and work is the focal point of international attention and scrutiny like never before, including from governments and a significant array of other interests.

It is within this broader context that we, the GNSO Council, need to re-establish, re-assert and re-focus on our essential role and function. The core role of the GNSO Council is to manage policy development in generic top level domain names and we need to be, and be seen to be, functional, effective and productive in undertaking that role. In doing this well, we will play our proper part in reinforcing, underpinning and adding value to the ICANN multi-stakeholder model.

Role of the GNSO Council Chair

The GNSO is one of three supporting organisations; however the GNSO Council is arguably the only place where the full diversity of the multi-stakeholder model comes together in full and in one, relatively small melting pot. Embracing diversity and ensuring effective output is a great challenge for the Council and therefore the councillors, the ICANN policy staff and the Council leadership, especially the chair. I relish that challenge and feel that a fair, consensual approach with a focus on output is required to meet it.

In addition to managing the diversity of input, the sheer volume of work that the Council needs to deal with is an on-going challenge. Inroads have been made to dealing with the workload through practical enhancements in the way we work, such as maintaining schedules of on-going projects and the recent introduction of a consent agenda. I expect that further improvements to the functioning of the Council as well as to prioritising and managing of workload should be possible and will seek to achieve this.

The Council attracts significant attention because of its high profile and important role. The chair must be cognisant of this and I believe that a good chair needs to be effective at engaging with the broader community, in order to ensure that the role and work of the Council is properly understood and appreciated. This is clearly a delicate position because it is not about representing specific positions that the Council may take or have taken but more about ensuring that the role, function and scope of the GNSO Council is properly understood and effectively represented.

I currently serve on the Council as a representative of the Registries Stakeholder Group (RySG). My vote in the Council is directed by the RySG and, should I be elected as chair, it will continue to be so. The role of the chair is clearly distinct from and fundamentally different to the advocacy oriented role of a councillor representing a particular interest or stakeholder group within the Council. I understand the principle and practice of this and therefore, the change in role and behaviour that becoming a chair requires.

The fundamental job of the GNSO Council Chair is to ensure that the Council is and remains as productive and effective as possible. This can be achieved by recognising the diversity of views that necessarily exist within the Council and then facilitating a fair balance of these views whilst remaining focussed on the necessary output.

Summary

It is an honour to be nominated and, should I be elected, it will be a tremendous privilege to serve a term as GNSO Council Chair. The job is no doubt a challenging one, perhaps even more so than ever before. I trust that this statement gives confidence to fellow councillors, and the groups that they represent on the Council, that I have the personal qualities, maturity and professional experience to do the job to the high standard it merits.

However, if elected, I will not expect to do the job alone but to work with the support of councillors, Vice Chairs and ICANN staff. I will work collaboratively and, whenever appropriate or necessary, rely on expertise other than my own.

I believe we should place significant value on the effective functioning of a GNSO Council where councillors can feel free to raise issues and vigorously argue the positions of the groups and the stakeholders that they represent. However, ultimately we should measure our success by the productive and effective output of the Council. As a councillor and prospective Chair, I would like to see us all to be part of a GNSO Council that is respected and highly valued for our role and contribution, both by our immediate stakeholders as well as the broader ICANN and global internet communities.

EXHIBIT JMR-2

Candidate Statement for GNSO Council Chair

Candidate: Jonathan Robinson

Date: 8 November 2013

I am pleased to accept the nomination to continue in the role of Council Chair for a second term.

Overview

I previously (September 2012) provided a comprehensive candidate statement. The statement detailed my Personal Qualifications, as well as my views on the Role of the GNSO Council, and that of the GNSO Council Chair. Much of that statement remains relevant a year later and it is therefore appended to this document. For reference, it can also be located online here:

http://gnso.icann.org/en/elections/robinson-statement-28sep12-en.pdf

What follows in this candidate statement is in the form of an update to the 2012 statement.

Role of the GNSO Council

The fundamental basis on which the Council operates has not changed in the past year. The ICANN bylaws and the GNSO Operating Procedures are essentially the same.

However, the GNSO and the GNSO Council have been challenged in numerous ways by the roll-out of the most substantial project in ICANN's history; the bringing to market of hundreds of new generic top-level domains (gTLDs). Apart from the sheer volume of work, there has been a range of challenging issues to consider including, for example; the speed and efficiency of the Policy Development Process (PDP), the distinction and synergy between policy and implementation, early engagement of the ICANN GAC with the GNSO PDP, the role of the GNSO Council in providing policy advice to the board and concern over the possible development of generic names policy outside of the GNSO.

The Council needs to, in consultation with GNSO Stakeholder Groups and Constituencies, embrace many of the challenges it faces whilst recognising appropriate limits. Recently, it has done so by, for example, recognising the need to improve the efficiency of the PDP and commencing work on that. Similarly, it has also chartered a GNSO working group to investigate the issue of policy and implementation. There are many such areas for continuous improvement, in addition to the bread and butter work of the Council, typically relating to the steady commissioning, developing and overseeing the accurate execution of generic names related policy work.

Role of the GNSO Council Chair

The role of the chair is, together with the Council vice-chairs, to ensure that the GNSO has a well-managed and effective council that works well with itself, the groups that make up the GNSO and the appropriate ICANN staff. The chair should also ensure that the Council is effectively connected with the GNSO SGs and constituencies through direct contact with councillors and, where appropriate, with the leadership or membership of the relevant GNSO groups.

The chair also has a form of public relations role in ensuring that the policy work of the GNSO is effectively articulated and understood in the broader community. For this reason, outreach and engagement with key ICANN staff, the ICANN board and other ICANN SO & ACs is also vital.

In addition to the effective week to week and month to month management of the Council's routine activities, the chair also needs, together with the Vice Chairs and others, to look outwards and think ahead. The GNSO Council sits within the GNSO, the GNSO in turn within the ICANN bottom-up, multi-stakeholder model and ICANN itself within the broader international internet governance framework.

Summary

The GNSO Council's ability to effectively commission and develop policy has to be seen, in part, as some of the proof of the effectiveness of the ICANN model. To the extent that our work goes well, we can be seen as part of the proof of the value and effectiveness of the model. To the extent that it does not, the opposite is true. A good chair and an effective council will play a significant part in ensuring the GNSO policy development does go well and, where it does not go as well as it could, to look for reasons why and appropriate responses to make sure it does go better in future.

I very much look forward to working with the Council, the Vice Chairs and the GNSO as a whole to ensure that we make a major contribution and that we are as successful as we possibly can be in our critical role at the heart of ICANN's multi-stakeholder model. It is both a privilege and a responsibility to work in the role as GNSO Council chair, something I appreciate, understand and welcome.

Appendix 1

Previous Candidate Statement for GNSO Council Chair

Date: 28 September 2012

Personal Qualifications

I am an experienced company director, manager and specialist in a variety of areas which are directly relevant to the complex blend of issues that the GNSO Council has to navigate. As well as specialist domain name industry experience, I have broader international and multi-stakeholder environment experience gained in the academic, not-for-profit and public purpose areas. I have lived and worked for extended periods of time in both the developed and developing world. My style is that I value careful consideration, balanced judgement and ultimately, productive output.

My recent professional experience has included:

- Over 10 years as main board director of public, quoted company, Group NBT plc
- Over 10 years as non-executive director of Afilias Limited (.info, mobi & .pro)
- 3 x 2 years as a member elected non-executive director, Nominet (UK) Ltd (.uk)

Prior to the development of ICANN, I was involved in work which involved active participation in a series of international meetings and included a term as deputy chairman on the board of the Internet Council of Registrars (CORE) back in 1997. Since ICANN's inception, I have attended a minimum of one ICANN meeting per year and every meeting since being elected to the GNSO Council in December 2010.

I hold a BSc (Physics) and a PhD (Engineering) degree from the University of CapeTown, South Africa. I previously undertook research at the University of Cambridge, Cambridge, UK, Imperial College, London, UK and the Lawrence Berkeley Laboratories, University of California, USA.

Role of the GNSO Council

It is evident to all that ICANN is at an absolutely critical point in its development. The organisation has recently embarked on the execution phase of the most ambitious project and role in its history; and it is therefore now facing unprecedented operational and broader challenges, including to the ICANN model itself. ICANN's role and work is the focal point of international attention and scrutiny like never before, including from governments and a significant array of other interests.

It is within this broader context that we, the GNSO Council, need to re-establish, re-assert and re-focus on our essential role and function. The core role of the GNSO Council is to manage policy development in generic top level domain names and we need to be, and be seen to be, functional, effective and productive in undertaking that role. In doing this well, we will play our proper part in reinforcing, underpinning and adding value to the ICANN multi-stakeholder model.

Role of the GNSO Council Chair

The GNSO is one of three supporting organisations; however the GNSO Council is arguably the only place where the full diversity of the multi-stakeholder model comes together in full and in one, relatively small melting pot. Embracing diversity and ensuring effective output is a great challenge for the Council and therefore the councillors, the ICANN policy staff and the Council leadership, especially the chair. I relish that challenge and feel that a fair, consensual approach with a focus on output is required to meet it.

In addition to managing the diversity of input, the sheer volume of work that the Council needs to deal with is an on-going challenge. Inroads have been made to dealing with the workload through practical enhancements in the way we work, such as maintaining schedules of on-going projects and the recent introduction of a consent agenda. I expect that further improvements to the functioning of the Council as well as to prioritising and managing of workload should be possible and will seek to achieve this.

The Council attracts significant attention because of its high profile and important role. The chair must be cognisant of this and I believe that a good chair needs to be effective at engaging with the broader community, in order to ensure that the role and work of the Council is properly understood and appreciated. This is clearly a delicate position because it is not about representing specific positions that the Council may take or have taken but more about ensuring that the role, function and scope of the GNSO Council is properly understood and effectively represented.

I currently serve on the Council as a representative of the Registries Stakeholder Group (RySG). My vote in the Council is directed by the RySG and, should I be elected as chair, it will continue to be so. The role of the chair is clearly distinct from and fundamentally different to the advocacy oriented role of a councillor representing a particular interest or stakeholder group within the Council. I understand the principle and practice of this and therefore, the change in role and behaviour that becoming a chair requires.

The fundamental job of the GNSO Council Chair is to ensure that the Council is and remains as productive and effective as possible. This can be achieved by recognising the diversity of views that necessarily exist within the Council and then facilitating a fair balance of these views whilst remaining focussed on the necessary output.

Summary

It is an honour to be nominated and, should I be elected, it will be a tremendous privilege to serve a term as GNSO Council Chair. The job is no doubt a challenging one, perhaps even more so than ever before. I trust that this statement gives confidence to fellow councillors, and the groups that they represent on the Council, that I have the personal qualities, maturity and professional experience to do the job to the high standard it merits.

However, if elected, I will not expect to do the job alone but to work with the support of councillors, Vice Chairs and ICANN staff. I will work collaboratively and, whenever appropriate or necessary, rely on expertise other than my own.

I believe we should place significant value on the effective functioning of a GNSO Council where councillors can feel free to raise issues and vigorously argue the positions of the groups and the stakeholders that they represent. However, ultimately we should measure our success by the productive and effective output of the Council. As a councillor and prospective Chair, I would like to see us all to be part of a GNSO Council that is respected and highly valued for our role and contribution, both by our immediate stakeholders as well as the broader ICANN and global internet communities.

EXHIBIT JMR-3

Candidate Statement for GNSO Council Chair

Candidate: Jonathan Robinson

Date: 3 October 2014

I am pleased to accept the nomination to continue in the role of Council Chair for a final term.

Overview

I previously (September 2012) provided a comprehensive candidate statement. The statement detailed my personal qualifications, as well as my views on the Role of the GNSO Council, and that of the GNSO Council Chair. Much of that statement remains relevant and it can be accessed here:

http://gnso.icann.org/en/elections/robinson-statement-28sep12-en.pdf

The 2012 statement follows as an appendix in this document and was updated with a candidate statement in November 2013 which can be found here:

http://gnso.icann.org/en/elections/robinson-statement-08nov13-en.pdf

Role of the GNSO Council

The fundamental basis on which the Council operates remains unchanged. The ICANN bylaws and the GNSO Operating Procedures are essentially the same. However, it is noteworthy that the process of reviewing the GNSO has now commenced.

The GNSO, the GNSO Council and arguably the whole ICANN multi-stakeholder model continue to face challenges from within and without. For example, the implementation and roll-out of the new gTLD programme has continued to throw up policy related issues and questions as well as test the relationship between policy and implementation . In addition, the overarching theme of the transition of stewardship of the IANA function and the associated accountability work have significantly attracted the attention of the broader community, arguably resulting in a distraction from the core GNSO business of policy development work.

Notwithstanding the existence of challenges, the Council has managed to function effectively. We have run regular meetings with comprehensive agendas including important discussion items and motions for key stages of specific policy development work. All of which are conducted in a collegial and constructive atmosphere. The Council has shown the discipline to stick to established principles and procedures of operation while recognising the need to be receptive to dynamic circumstances. The Council has also asserted its positon where appropriate in order to reinforce both its role and the boundaries of its responsibility where necessary.

The tone for the work of the GNSO Council over the past year was set by the first ever induction and development session for the Council which was held at the end of the annual meeting in Buenos Aires. Initiatives for improvement and development were discussed and have been monitored throughout the course of the year. Ensuring that new councillors are appropriately inducted to the Council and oriented within the GNSO is a critical component of ensuring the effective working of the GNSO Council.

Role of the GNSO Council Chair

My view has been consistent in that the role of the Chair, together with the Council vice-chairs, is to ensure that the GNSO has a well-managed and effective council that functions well as a council as well as with the groups that make up the GNSO and the appropriate ICANN staff. The Chair should therefore seek to ensure that the Council is effectively connected with the GNSO SGs and constituencies through having direct contact with individual councillors and, where appropriate, with the leadership or membership of the relevant GNSO groups.

The Chair also has a form of public relations role in ensuring that the policy work of the GNSO is effectively articulated and understood in the broader community. For this reason, outreach and engagement with key ICANN staff, the ICANN board and other ICANN SO & ACs is vital. This creates challenges at times, such as when and how the Chair can represent the GNSO.

In addition to the effective week to week and month to month management of the Council's routine activities, the Chair also needs, together with the Council vice chairs and others, to look beyond the GNSO and to think ahead. The GNSO Council sits within the GNSO, the GNSO in turn within the ICANN bottom-up, multi-stakeholder model and ICANN itself within the broader international internet governance framework. Good progress has been made in the regular meetings with the ccNSO as well as with the GAC through the GAC / GNSO Consultation Group and the recent appointment of a GNSO Liaison to the GAC. This cross community and related work remains an area which needs focus and attention from the Chair.

Summary

The GNSO Council's ability to effectively commission and develop policy has to be seen, in part, as some of the proof of the effectiveness of the ICANN multi-stakeholder model. To the extent that our work goes well, we can be seen as part of the proof of the value and effectiveness of the model. To the extent that it does not, the opposite is true. A good chair and an effective council will play a significant part in ensuring the GNSO policy development does go well and, where it does not go as well as it could, to look for reasons why and appropriate responses to make sure it does go better in future.

I very much look forward to working with the Council, the Vice Chairs and the GNSO as a whole to ensure that we make a major contribution and that we are as successful as we possibly can be in our critical role at the heart of ICANN's multi-stakeholder model. There is a significant opportunity to build on some of the key initiatives that the Council has taken and with which I have been closely involved with as chair. It is both a privilege and a responsibility to work in the role as GNSO council chair, something I appreciate, understand and welcome.

Appendix 1

2012 Candidate Statement for GNSO Council Chair

Date: 28 September 2012

Personal Qualifications

I am an experienced company director, manager and specialist in a variety of areas which are directly relevant to the complex blend of issues that the GNSO Council has to navigate. As well as specialist domain name industry experience, I have broader international and multi-stakeholder environment experience gained in the academic, not-for-profit and public purpose areas. I have lived and worked for extended periods of time in both the developed and developing world. My style is that I value careful consideration, balanced judgement and ultimately, productive output.

My recent professional experience has included:

- Over 10 years as main board director of public, quoted company, Group NBT plc
- Over 10 years as non-executive director of Afilias Limited (.info, mobi & .pro)
- 3 x 2 years as a member elected non-executive director, Nominet (UK) Ltd (.uk)

Prior to the development of ICANN, I was involved in work which involved active participation in a series of international meetings and included a term as deputy chairman on the board of the Internet Council of Registrars (CORE) back in 1997. Since ICANN's inception, I have attended a minimum of one ICANN meeting per year and every meeting since being elected to the GNSO Council in December 2010.

I hold a BSc (Physics) and a PhD (Engineering) degree from the University of CapeTown, South Africa. I previously undertook research at the University of Cambridge, Cambridge, UK, Imperial College, London, UK and the Lawrence Berkeley Laboratories, University of California, USA.

Role of the GNSO Council

It is evident to all that ICANN is at an absolutely critical point in its development. The organisation has recently embarked on the execution phase of the most ambitious project and role in its history; and it is therefore now facing unprecedented operational and broader challenges, including to the ICANN model itself. ICANN's role and work is the focal point of international attention and scrutiny like never before, including from governments and a significant array of other interests.

It is within this broader context that we, the GNSO Council, need to re-establish, re-assert and re-focus on our essential role and function. The core role of the GNSO Council is to manage policy development in generic top level domain names and we need to be, and be seen to be, functional, effective and productive in undertaking that role. In doing this well, we will play our proper part in reinforcing, underpinning and adding value to the ICANN multi-stakeholder model.

Role of the GNSO Council Chair

The GNSO is one of three supporting organisations; however the GNSO Council is arguably the only place where the full diversity of the multi-stakeholder model comes together in full and in one, relatively small melting pot. Embracing diversity and ensuring effective output is a great challenge for the Council and therefore the councillors, the ICANN policy staff and the Council leadership, especially the Chair. I relish that challenge and feel that a fair, consensual approach with a focus on output is required to meet it.

In addition to managing the diversity of input, the sheer volume of work that the Council needs to deal with is an on-going challenge. Inroads have been made to dealing with the workload through practical enhancements in the way we work, such as maintaining schedules of on-going projects and the recent introduction of a consent agenda. I expect that further improvements to the functioning of the Council as well as to prioritising and managing of workload should be possible and will seek to achieve this.

The Council attracts significant attention because of its high profile and important role. The Chair must be cognisant of this and I believe that a good chair needs to be effective at engaging with the broader community, in order to ensure that the role and work of the Council is properly understood and appreciated. This is clearly a delicate position because it is not about representing specific positions that the Council may take or have taken but more about ensuring that the role, function and scope of the GNSO Council is properly understood and effectively represented.

I currently serve on the Council as a representative of the Registries Stakeholder Group (RySG). My vote in the Council is directed by the RySG and, should I be elected as chair, it will continue to be so. The role of the Chair is clearly distinct from and fundamentally different to the advocacy oriented role of a councillor representing a particular interest or stakeholder group within the Council. I understand the principle and practice of this and therefore, the change in role and behaviour that becoming a chair requires.

The fundamental job of the GNSO Council Chair is to ensure that the Council is and remains as productive and effective as possible. This can be achieved by recognising the diversity of views that necessarily exist within the Council and then facilitating a fair balance of these views whilst remaining focussed on the necessary output.

Summary

It is an honour to be nominated and, should I be elected, it will be a tremendous privilege to serve a term as the GNSO Council Chair. The job is no doubt a challenging one, perhaps even more so than ever before. I trust that this statement gives confidence to fellow councillors, and the groups that they represent on the Council, that I have the personal qualities, maturity and professional experience to do the job to the high standard it merits.

However, if elected, I will not expect to do the job alone but to work with the support of councillors, vice chairs and ICANN staff. I will work collaboratively and, whenever appropriate or necessary, rely on expertise other than my own.

I believe we should place significant value on the effective functioning of a GNSO Council where councillors can feel free to raise issues and vigorously argue the positions of the groups and the stakeholders that they represent. However, ultimately we should measure our success by the productive and effective output of the Council. As a councillor and prospective chair, I would like to see us all to be part of a GNSO Council that is respected and highly valued for our role and contribution, both by our immediate stakeholders as well as the broader ICANN and global internet communities.

EXHIBIT JMR-4

Search ICANN.org

Log In | Sign Up

ICANN

Jonathan Robinson Recognized with 2014 ICANN Leadership Award

This page is available in:
English | العربية | Español | Français | Русский | 中文 | Português

Jonathan Robinson has been awarded the 2014 ICANN Leadership Award for his contributions to the effectiveness of ICANN's multistakeholder model.

Robinson received the award in recognition of his devotion to the multistakeholder model, his extraordinary generosity of time, energy, knowledge and expertise, friendship and leadership, and his collegial leadership style that has increased civility and effectiveness within the community.

Assuming the role as Chair of the Generic Names Supporting Organization Council in 2012, Robinson has worked closely with the other 22 members of the Council to strengthen collaborative work within the GNSO and together with other ICANN bodies. These efforts to further open channels of communications between ICANN's diverse participants are

critical to the effective functioning and development of the multistakeholder organization. Introducing innovations such as initiating the first induction and development session for the GNSO Council has helped to ensure the well-informed involvement and early success of others as leadership participants within the multistakeholder environment.

Robinson is an experienced company director and entrepreneur with a focus on business development in the domain name services and related sectors. He is co-founder of Group NBT (now NetNames) and served as a Board Director and Chief Operating Officer of the London listed Group for 10 years until 2009. Since 2010, he has continued to work actively in the domain name industry, including through his involvement and board position with domain registry operator, Afilias Ltd.

ICANN gave its first Leadership Award at ICANN's 48th Public Meeting in Buenos Aires in November 2013 to Lesley Cowley, then-CEO of Nominet, the .UK top-level domain registry.

The ICANN staff leadership team selects the winner of this annual award unanimously, based on an individual's leadership in protecting and promoting the multistakeholder model.

Details

ICANN Announcements

13 Oct 2014

Civil Society

DNS Marketplace

Developing World

Government

Technology

More Announcements

Participate Now in the Sunrise and Trademark Claims Survey

ICANN Board to Hold Public Board Meeting During Genval Workshop

Next Steps On Reviews

Registration Directory Service (RDS-WHOIS2) Review Team Draft Report & Recommendations


YouTube


Twitter


LinkedIn


Flickr


Facebook


Newsletters


Community Wiki


ICANN Blog

Who We Are

Contact Us

Accountability & Transparency

Governance

Help

Data Protection

© 2018 Internet Corporation for Assigned Names and Numbers. Privacy Policy
Terms of Service Cookies Policy

EXHIBIT JMR-5

NEWS

Get the latest news from Afilias and its Industry Experts.

Afilias Chairman Jonathan Robinson Wins ICANN's 2016 Leadership Award at ICANN 57

Robinson's contribution recognized a second time!

Hyderabad, Telangana, India – November 05, 2016 – Afilias, a leading domain registry operator, congratulates Jonathan Robinson, Executive Chairman of Afilias' Board of Directors, on receiving the

Internet Corporation for Assigned Names and Numbers (ICANN) 2016 Leadership Award for his contributions to the ICANN and broader internet community.

As Chair of the Generic Names Supporting Organization (GNSO) Council, ICANN's policy body, from 2012 to 2015, Robinson strengthened collaborative work within the Council as well as with other ICANN bodies. His commitment to fostering communication and collaboration among ICANN's diverse participants is a personal passion which was recognized with an ICANN Leadership Award in 2014. Following on from his work on the GNSO Council Robinson continued to co-chair the IANA Stewardship Transition working group. It is for his work as co-chair of this Group that he is now being recognized.

"I am honored to receive the award, especially in the company of so many other distinguished recipients" said Robinson at the award presentation ceremony at the 57th ICANN meeting in Hyderabad. "With this meeting of the ICANN community, immediately after the IANA Transition, we begin a new era of internet stewardship. It has been my privilege to serve in a leadership role, encouraging the essential collaboration and hard work that is required."

"The IANA transition places even more responsibility on ICANN, which relies heavily on community members for direction, inspiration and accountability" said Hal Lubsen, President and CEO of Afilias. "It is gratifying to see Jonathan recognized for his leadership, effectiveness and contributions to the multi-stakeholder model that we now rely upon completely for stewardship of the unified global Internet."

Robinson has extensive executive and non-executive experience in the domain name industry over many years. He was a founder of NetBenefit in 1995, a supplier of domain name management and associated services, which was listed in London in June 1999. Jonathan served as a main board director at NetBenefit from 1999 to 2009. Having served as a director of Afilias since 2001, Robinson was appointed Executive Chairman in 2014.

About Afilias

Afilias is the world's second largest domain registry, with millions of domain names under management. Afilias powers a wide variety of top-level domains, including TLDs for countries, cities, brands, communities and generic terms. Afilias' specialized technology makes Internet addresses more accessible and useful through a broad range of applications, including Internet domain registry services, managed DNS, and mobile Web services. For more information on Afilias services, visit www.afilias.info.

PRESS RELEASES

Afilias Moves to the US
Aug 30, 2018

New .LLC Domain Landrush Period Begins July 9
(General Availability Begins July 23rd)
Jul 9, 2018

MORE

Products & Services
Careers
Directors of the Company
Executive Officers & Key Employees
Policies
Sustainability

gTLDs
ccTLDs
IDN e-mail
ZoneHawk

Afilias' New Domains
dotBrand Services
Managed Registry Services

Device Atlas
goMobi
mobiReady
mobiForge

One-Click DNSSEC
FlexDNS Platform

News
Press Releases
Blog
Events
In the News
Resources

Contact Us
Offices
Press Inquiries
Support
Request Information
FAQ

Afilias Email Newsle
Afilias Facebo Link
Afilias Twitter Link
Afilias YouTu Link
Afilias Linked Link
Afilias Google

© Afilias, Inc. All rights reserved.

EXHIBIT JMR-6

Published on *National Telecommunications and Information Administration* (https://www.ntia.doc.gov)

Improvement of Technical Management of Internet Names and Addresses; Proposed Rule

Date:
February 20, 1998
Docket Number:
980212036-8036-01

[Federal Register: February 20, 1998 (Volume 63, Number 34)]
[Proposed Rules]
[Page 8825-8833]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:fr20fe98-24]

[[Page 8825]]

Part IV

Department of Commerce

National Telecommunications and Information Administration

---

15 CFR Chapter XXIII

Improvement of Technical Management of Internet Names and Addresses; Proposed Rule

[[Page 8826]]

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

15 CFR Chapter XXIII

[Docket No. 980212036-8036-01]
RIN 0660-AA11

Improvement of Technical Management of Internet Names and Addresses

AGENCY: National Telecommunications and Information Administration (NTIA), Commerce.

ACTION: Proposed rule; request for public comment.

SUMMARY: This document sets forth ways to improve technical management of the Internet Domain Name System (DNS). Specifically, it describes the process by which the Federal government will transfer management of the Internet DNS to a private not-for-profit corporation. The document also proposes to open up to competition the administration of top level domains and the registration of domain names.

DATES: Comments must be received by March 23, 1998.

ADDRESSES: Comments may be mailed to Karen Rose, Office of International Affairs, National Telecommunications and Information Administration (NTIA), Room 4701, U.S. Department of Commerce, Contact Information Redac or sent via electronic mail to Contact n ormation Redacted Messages to that address will receive a reply in acknowledgment. Comments submitted in electronic form should be in ASCII, WordPerfect (please specify version), or Microsoft Word (please specify version) format. Comments received will be posted on the NTIA website at http://www.ntia.doc.gov. Detailed information about electronic filing is available on the NTIA website, http://www.ntia.doc.gov/domainname/domainname130.htm. Paper submissions should include three paper copies and a version on diskette in the formats specified above.

FOR FURTHER INFORMATION CONTACT: Karen Rose, NTIA, (202) 482-0365.

SUPPLEMENTARY INFORMATION:

Authority: 15 U.S.C. 1512; 47 U.S.C. 902(b)(2)(H); 47 U.S.C. 902 (b)(2)(I); 47 U.S.C. 902(b)(2)(M); 47 U.S.C. 904(c)(1).

I. Introduction

On July 1, 1997, The President directed the Secretary of Commerce to privatize, increase competition in, and promote international participation in the domain name system. Domain names are the familiar and easy-to-remember names for Internet computers (e.g. ``www.ecommerce.gov''). They map to unique Internet Protocol (IP) numbers (e.g., 98.37.241.30) that serve as routing addresses on the Internet. The domain name system (DNS) translates Internet names into the IP numbers needed for transmission of information across the network. On July 2, 1997, the Department of Commerce issued a Request for Comments (RFC) on DNS administration (62 FR 35896). This proposed rule, shaped by over 430 comments received in response to the RFC, provides notice and seeks public comment on a proposal to transfer control of Internet domain names from government to a private, nonprofit corporation.

II. Background

Today's Internet is an outgrowth of U.S. government investments in packet-switching technology and communications networks carried out under agreements with the Defense Advanced Research Projects Agency (DARPA), the National Science Foundation (NSF) and other U.S. research agencies. The government encouraged bottom-up development of networking technologies through work at NSF, which established the NSFNET as a network for research and education. The NSFNET fostered a wide range of applications, and in 1992 the U.S. Congress gave the National Science Foundation statutory authority to commercialize the NSFNET, which formed the basis for today's Internet.

As a legacy, major components of the domain name system are still performed by or subject to agreements with agencies of the U.S. government.

A. Assignment of Numerical Addresses to Internet Users

Every Internet computer has a unique IP number. The Internet Assigned Numbers Authority (IANA), headed by Dr. Jon Postel of the Information Sciences Institute (ISI) at the University of Southern California, coordinates this system by allocating blocks of numerical addresses to regional IP registries (ARIN in North America, RIPE in Europe, and APNIC in the Asia/Pacific region), under contract with DARPA. In turn, larger Internet service providers apply to the regional IP registries for blocks of IP addresses. The recipients of those address blocks then reassign addresses to smaller Internet service providers and to end users.

B. Management of the System of Registering Names for Internet Users

The domain name space is constructed as a hierarchy. It is divided into top-level domains (TLDs), with each TLD then divided into second-level domains (SLDs), and so on. More than 200 national, or country-code, TLDs (ccTLDs) are administered by their corresponding governments or by private entities with the appropriate national government's acquiescence. A small set of generic top-level domains (gTLDs) do not carry any national identifier, but denote the intended function of that portion of the domain space. For example, .com was established for commercial users, .org for not-for-profit organizations, and .net for network service providers. The registration and propagation of these key gTLDs are performed by Network Solutions, Inc. (NSI), a Virginia-based company, under a five-year cooperative agreement with NSF. This agreement includes an optional ramp-down period that expires on September 30, 1998.

C. Operation of the Root Server System

The root server system contains authoritative databases listing the TLDs so that an Internet message can be routed to its destination. Currently, NSI operates the ``A'' root server, which maintains the authoritative root database and replicates changes to the other root servers on a daily basis. Different organizations, including NSI, operate the other 12 root servers. In total, the U.S. government plays a direct role in the operation of half of the world's root servers. Universal connectivity on the Internet cannot be guaranteed without a set of authoritative and consistent roots.

D. Protocol Assignment

The Internet protocol suite, as defined by the Internet Engineering Task Force (IETF), contains many technical parameters, including protocol numbers, port numbers, autonomous system numbers, management information base object identifiers and others. The common use of these protocols by the Internet community requires that the particular values used in these fields be assigned uniquely. Currently, IANA, under contract with DARPA, makes these assignments and maintains a registry of the assigned values.

III. The Need For Change

From its origins as a U.S.-based research vehicle, the Internet is rapidly becoming an international medium for commerce, education and communication. The traditional means

[[Page 8827]]

of organizing its technical functions need to evolve as well. The pressures for change are coming from many different quarters:

There is widespread dissatisfaction about the absence of competition in domain name registration.

Mechanisms for resolving conflict between trademark holders and domain name holders are expensive and cumbersome.

Without changes, a proliferation of lawsuits could lead to chaos as tribunals around the world apply the antitrust law and intellectual property law of their jurisdictions to the Internet.

Many commercial interests, staking their future on the successful growth of the Internet, are calling for a more formal and robust management structure.

An increasing percentage of Internet users reside outside of the U.S., and those stakeholders want a larger voice in Internet coordination.

As Internet names increasingly have commercial value, the decision to add new top-level domains cannot continue to be made on an ad hoc basis by entities or individuals that are not formally accountable to the Internet community.

As the Internet becomes commercial, it becomes inappropriate for U.S. research agencies (NSF and DARPA) to participate in and fund these functions.

IV. The Future Role of the U.S. Government in the DNS

On July 1, 1997, as part of the Clinton Administration's Framework for Global Electronic Commerce, the President directed the Secretary of Commerce to privatize, increase competition in, and promote international participation in the domain name system.

Accordingly, on July 2, 1997, the Department of Commerce issued a Request for Comments (RFC) on DNS administration, on behalf of an

inter-agency working group previously formed to explore the appropriate future role of the U.S. government in the DNS. The RFC solicited public input on issues relating to the overall framework of the DNS system, the creation of new top-level domains, policies for registrars, and trademark issues. During the comment period, over 430 comments were received, amounting to some 1500 pages.1

\1\ The RFC and comments received are available on the Internet at the following address: .

This discussion draft, shaped by the public input described above, provides notice and seeks public comment on a proposal to improve the technical management of Internet names and addresses. It does not propose a monolithic structure for Internet governance. We doubt that the Internet should be governed by one plan or one body or even by a series of plans and bodies. Rather, we seek to create mechanisms to solve a few, primarily technical (albeit critical) questions about administration of Internet names and numbers.

We expect that this proposal will likely spark a lively debate, requiring thoughtful analysis, and appropriate revisions. Nonetheless, we are hopeful that reasonable consensus can be found and that, after appropriate modifications, implementation can begin in April, 1998. Recognizing that no solution will win universal support, the U.S. government seeks as much consensus as possible before acting.

V. Principles for a New System

Our consultations have revealed substantial differences among Internet stakeholders on how the domain name system should evolve. Since the Internet is changing so rapidly, no one entity or individual can claim to know what is best for the Internet. We certainly do not believe that our views are uniquely prescient. Nevertheless, shared principles have emerged from our discussions with Internet stakeholders.

A. Stability

The U.S. government should end its role in the Internet number and name address systems in a responsible manner. This means, above all else, ensuring the stability of the Internet. The Internet functions well today, but its current technical management is probably not viable over the long term. We should not wait for it to break down before acting. Yet, we should not move so quickly, or depart so radically from the existing structures, that we disrupt the functioning of the Internet. The introduction of a new system should not disrupt current operations, or create competing root systems.

B. Competition

The Internet succeeds in great measure because it is a decentralized system that encourages innovation and maximizes individual freedom. Where possible, market mechanisms that support competition and consumer choice should drive the technical management of the Internet because they will promote innovation, preserve diversity, and enhance user choice and satisfaction.

C. Private, Bottom-Up Coordination

Certain technical management functions require coordination. In these cases, responsible, private-sector action is preferable to government control. A private coordinating process is likely to be more flexible than government and to move rapidly enough to meet the changing needs of the Internet and of Internet users. The private process should, as far as possible, reflect the bottom-up governance that has characterized development of the Internet to date.

D. Representation

Technical management of the Internet should reflect the diversity of its users and their needs. Mechanisms should be established to ensure international input in decision making.

In keeping with these principles, we divide the name and number functions into two groups, those that can be moved to a competitive system and those that should be coordinated. We then suggest the creation of a representative, not-for-profit corporation to manage the coordinated functions according to widely accepted objective criteria. We then suggest the steps necessary to move to competitive markets in

those areas that can be market driven. Finally, we suggest a transition plan to ensure that these changes occur in an orderly fashion that preserves the stability of the Internet.

VI. The Proposal

A. The Coordinated Functions

Management of number addresses is best done on a coordinated basis. As technology evolves, changes may be needed in the number allocation system. These changes should also be undertaken in a coordinated fashion.

Similarly, coordination of the root server network is necessary if the whole system is to work smoothly. While day-to-day operational tasks, such as the actual operation and maintenance of the Internet root servers, can be contracted out, overall policy guidance and control of the TLDs and the Internet root server system should be vested in a single organization that is representative of Internet users.

Finally, coordinated maintenance and dissemination of the protocol parameters for Internet addressing will best preserve the stability and interconnectivity of the Internet.

We propose the creation of a private, not-for-profit corporation (the new corporation) to manage the coordinated functions in a stable and open institutional framework. The new corporation should operate as a private

[[Page 8828]]

entity for the benefit of the Internet as a whole. The new corporation would have the following authority:

1. To set policy for and direct the allocation of number blocks to regional number registries for the assignment of Internet addresses;

2. To oversee the operation of an authoritative root server system;

3. To oversee policy for determining, based on objective criteria clearly established in the new organization's charter, the circumstances under which new top-level domains are added to the root system; and

4. To coordinate the development of other technical protocol parameters as needed to maintain universal connectivity on the Internet.

The U.S. government would gradually transfer existing IANA functions, the root system and the appropriate databases to this new not-for-profit corporation. This transition would commence as soon as possible, with operational responsibility moved to the new entity by September 30, 1998. The U.S. government would participate in policy oversight to assure stability until the new corporation is established and stable, phasing out as soon as possible and in no event later than September 30, 2000. The U.S. Department of Commerce will coordinate the U.S. government policy role. In proposing these dates, we are trying to balance concerns about a premature U.S. government exit that turns the domain name system over to a new and untested entity against the concern that the U.S. government will never relinquish its current management role.

The new corporation will be funded by domain name registries and regional IP registries. Initially, current IANA staff will move to this new organization to provide continuity and expertise throughout the period of time it takes to establish the new corporation. The new corporation should hire a chief executive officer with a background in the corporate sector to bring a more rigorous management to the organization than was possible or necessary when the Internet was primarily a research medium. As these functions are now performed in the United States, the new corporation will be headquartered in the United States, and incorporated under U.S. law as a not-for-profit corporation. It will, however, have and report to a board of directors from around the world.

It is probably impossible to establish and maintain a perfectly representative board for this new organization. The Internet community is already extraordinarily diverse and likely to become more so over time. Nonetheless, the organization and its board must derive legitimacy from the participation of key stakeholders. Since the organization will be concerned mainly with numbers, names and protocols, its board should represent membership organizations in each of these areas, as well as the direct interests of Internet users.

The board of directors for the new corporation should be balanced to equitably represent the interests of IP number registries, domain name registries, domain name registrars, the technical community, and Internet users (commercial, not-for-profit, and individuals). Officials of governments or intergovernmental organizations should not serve on

the board of the new corporation. Seats on the initial board might be allocated as follows:

Three directors from a membership association of regional number registries, representing three different regions of the world. Today this would mean one each from ARIN, APNIC and RIPE. As additional regional number registries are added, board members could be designated on a rotating basis or elected by a membership organization made up of regional registries. ARIN, RIPE and APNIC are open membership organizations that represent entities with large blocks of numbers. They have the greatest stake in and knowledge of the number address system. They are also representative internationally.

Two members designated by the Internet Architecture Board (IAB), an international membership board that represents the technical community of the Internet.

Two members designated by a membership association (to be created) representing domain name registries and registrars.

Seven members designated by a membership association (to be created) representing Internet users. At least one of those board seats could be designated for an individual or entity engaged in non-commercial, not-for-profit use of the Internet, and one for individual end users. The remaining seats could be filled by commercial users, including trademark holders.

The CEO of the new corporation would serve on the board of directors.

The new corporation's processes should be fair, open and pro-competitive, protecting against capture by a narrow group of stakeholders. Its decision-making processes should be sound and transparent; the bases for its decisions should be recorded and made publicly available. Super-majority or even consensus requirements may be useful to protect against capture by a self-interested faction. The new corporation's charter should provide a mechanism whereby its governing body will evolve to reflect changes in the constituency of Internet stakeholders. The new corporation should establish an open process for the presentation of petitions to expand board representation.

In performing the functions listed above, the new corporation will act much like a standard-setting body. To the extent that the new corporation operates in an open and pro-competitive manner, its actions will withstand antitrust scrutiny. Its standards should be reasonably based on, and no broader than necessary to promote its legitimate coordinating objectives. Under U.S. law, a standard-setting body can face antitrust liability if it is dominated by an economically interested entity, or if standards are set in secret by a few leading competitors. But appropriate processes and structure will minimize the possibility that the body's actions will be, or will appear to a court to be, anti-competitive.

B. The Competitive Functions

The system for registering second-level domain names and the management of the TLD registries should become competitive and market-driven.

In this connection, we distinguish between registries and registrars. A ``registry,'' as we use the term, is responsible for maintaining a TLD's zone files, which contain the name of each SLD in that TLD and each SLD's corresponding IP number. Under the current structure of the Internet, a given TLD can have no more than one registry. A ``registrar'' acts as an interface between domain-name holders and the registry, providing registration and value-added services. It submits to the registry zone file information and other data (including contact information) for each of its customers in a single TLD. Currently, NSI acts as both the exclusive registry and as the exclusive registrar for .com, .net, .org, and .edu.

Both registry and registrar functions could be operated on a competitive basis. Just as NSI acts as the registry for .com, .net, and .org, other companies could manage registries with different TLDs such as .vend or .store. Registrars could provide the service of obtaining domain names for customers in any gTLD. Companies that design Web sites for customers might, for example, provide registration as an adjunct to other services. Other companies may perform this function as a stand-alone business.

There appears to be strong consensus that, at least at this time, domain name

registration--the registrar function--should be competitive. There is disagreement, however, over the wisdom of promoting competition at the registry level.

Some have made a strong case for establishing a market-driven registry system. Competition among registries would allow registrants to choose among TLDs rather than face a single option. Competing TLDs would seek to heighten their efficiency, lower their prices, and provide additional value-added services. Investments in registries could be recouped through branding and marketing. The efficiency, convenience, and service levels associated with the assignment of names could ultimately differ from one TLD registry to another. Without these types of market pressures, they argue, registries will have very little incentive to innovate.

Others feel strongly, however, that if multiple registries are to exist, they should be undertaken on a not-for-profit basis. They argue that lack of portability among registries (that is, the fact that users cannot change registries without adjusting at least part of their domain name string) could create lock-in problems and harm consumers. For example, a registry could induce users to register in a top-level domain by charging very low prices initially and then raise prices dramatically, knowing that name holders will be reluctant to risk established business by moving to a different top-level domain.

We concede that switching costs and lock-in could produce the scenario described above. On the other hand, we believe that market mechanisms may well discourage this type of behavior. On balance, we believe that consumers will benefit from competition among market oriented registries, and we thus support limited experimentation with competing registries during the transition to private sector administration of the domain name system.

C. The Creation of New gTLDs

Internet stakeholders disagree about who should decide when a new top-level domain can be added and how that decision should be made. Some believe that anyone should be allowed to create a top-level domain registry. They argue that the market will decide which will succeed and which will not. Others believe that such a system would be too chaotic and would dramatically increase customer confusion. They argue that it would be far more complex technically, because the root server system would have to point to a large number of top-level domains that were changing with great frequency. They also point out that it would be much more difficult for trademark holders to protect their trademarks if they had to police a large number of top-level domains.

All these arguments have merit, but they all depend on facts that only further experience will reveal. At least in the short run, a prudent concern for the stability of the system requires that expansion of gTLDs proceed at a deliberate and controlled pace to allow for evaluation of the impact of the new gTLDs and well-reasoned evolution of the domain space. The number of new top-level domains should be large enough to create competition among registries and to enable the new corporation to evaluate the functioning, in the new environment, of the root server system and the software systems that enable shared registration. At the same time, it should not be so large as to destabilize the Internet.

We believe that during the transition to private management of the DNS, the addition of up to five new registries would be consistent with these goals. At the outset, we propose that each new registry be limited to a single top-level domain. During this period, the new corporation should evaluate the effects that the addition of new gTLDs have on the operation of the Internet, on users, and on trademark holders. After this transition, the new corporation will be in a better position to decide whether or when the introduction of additional gTLDs is desirable.

Individual companies and consortia alike may seek to operate specific generic top-level domains. Competition will take place on two levels. First, there will be competition among different generic top-level domains. Second, registrars will compete to register clients into these generic top-level domains. By contrast, existing national registries will continue to administer country-code top-level domains if these national government seek to assert those rights. Changes in the registration process for these domains are up to the registries administering them and their respective national governments.

Some have called for the creation of a more descriptive system of top-level domains based on industrial classifications or some other easy to understand schema. They suggest that having multiple top-level domains is already confusing and that the addition of new generic TLDs will make it more difficult for users to find the companies they are seeking.

Market driven systems result in innovation and greater consumer choice and satisfaction in the long run. We expect that in the future, directory services of various sorts will make it easy for users to find the sites they seek regardless of the number of top-level domains.

Attempts to impose too much central order risk stifling a medium like the Internet that is decentralized by nature and thrives on freedom and innovation.

D. The Trademark Dilemma

It is important to keep in mind that trademark/domain name disputes arise very rarely on the Internet today. NSI, for example, has registered millions of domain names, only a tiny fraction of which have been challenged by a trademark owner. But where a trademark is unlawfully used as a domain name, consumers may be misled about the source of the product or service offered on the Internet, and trademark owners may not be able to protect their rights without very expensive litigation.

For cyberspace to function as an effective commercial market, businesses must have confidence that their trademarks can be protected. On the other hand, management of the Internet must respond to the needs of the Internet community as a whole, and not trademark owners exclusively. The balance we strike is to provide trademark holders with the same rights they have in the physical world, to ensure transparency, to guarantee a dispute resolution mechanism with resort to a court system, and to add new top-level domains carefully during the transition to private sector coordination of the domain name system.

There are certain steps that could be taken in the application process that would not be difficult for an applicant, but that would make the trademark owner's job easier. For instance, gTLD registrants could supply basic information--including the applicant's name and sufficient contact information to be able to locate the applicant or its representative. To deter the pirating of domain names, the registry could also require applicants to certify that it knows of no entity with superior rights in the domain name it seeks to register.

The job of policing trademarks could be considerably easier if domain name databases were readily searchable through a common interface to determine what names are registered, who holds those domain names, and how to contact a domain name holder. Many trademark holders find the current registration search tool, who is, too limited in its functioning to be effective for this purpose. A more robust and flexible search tool, which features multiple field or string searching and retrieves similar names, could be

[[Page 8830]]

employed or developed to meet the needs of trademark holders. The databases also could be kept up to date by a requirement that domain name registrants maintain up-to-date contact information.

Mechanisms that allow for on-line dispute resolution could provide an inexpensive and efficient alternative to litigation for resolving disputes between trademark owners and domain name registrants. A swift dispute resolution process could provide for the temporary suspension of a domain name registration if an adversely affected trademark holder objects within a short time, e.g. 30 days, of the initial registration. We seek comment on whether registries should be required to resolve disputes within a specified period of time after an opposition is filed, and if so, how long that period should be.

Trademark holders have expressed concern that domain name registrants in faraway places may be able to infringe their rights with no convenient jurisdiction available in which the trademark owner could file suit to protect those rights. At the time of registration, registrants could agree that, in the event of a trademark dispute involving the name registered, jurisdiction would lie where the registry is domiciled, where the registry database in maintained, or where the ``A'' root server is maintained. We seek comment on this proposal, as well as suggestions for how such jurisdictional provisions could be implemented.

Trademark holders have also called for the creation of some mechanism for ``clearing'' trademarks, especially famous marks, across a range of gTLDs. Such mechanisms could reduce trademark conflict associated with the addition of new gTLDs. Again, we seek comment on this proposal, and suggested mechanisms for trademark clearance processes.

We stop short of proposals that could significantly limit the flexibility of the Internet, such as waiting periods or not allowing any new top-level domains.

We also do not propose to establish a monolithic trademark dispute resolution process at this time, because it is unclear what system would work best. Even trademark holders we have consulted are divided on this question. Therefore, we propose that each name registry must establish minimum dispute resolution and other procedures related to

trademark considerations. Those minimum procedures are spelled out in Appendix 2. Beyond those minimums, registries would be permitted to establish additional trademark protection and trademark dispute resolution mechanisms.

We also propose that shortly after their introduction into the root, a study be undertaken on the effects of adding new gTLDs and related dispute resolution procedures on trademark and intellectual property right holders. This study should be conducted under the auspices of a body that is internationally recognized in the area of dispute resolution procedures, with input from trademark and domain name holders and registries. The findings of this study should be submitted to the board of the new corporation and considered when it makes decisions on the creation and introduction of new gTLDs. Information on the strengths and weaknesses of different dispute resolution procedures should also give the new corporation guidance for deciding whether the established minimum criteria for dispute resolution should be amended or maintained. Such a study could also provide valuable input with respect to trademark harmonization generally.

U.S. trademark law imposes no general duty on a registrar to investigate the propriety of any given registration.2 Under existing law, a trademark holder can properly file a lawsuit against a domain name holder that is infringing or diluting the trademark holder's mark. But the law provides no basis for holding that a registrar's mere registration of a domain name, at the behest of an applicant with which it has an arm's-length relationship, should expose it to liability.3 Infringers, rather than registrars, registries, and technical management bodies, should be liable for trademark infringement. Until case law is fully settled, however, registries can expect to incur legal expenses in connection with trademark disputes as a cost of doing business. These costs should not be borne by the new not-for-profit corporation, and therefore registries should be required to indemnify the new corporation for costs incurred in connection with trademark disputes. The evolution of litigation will be one of the factors to be studied by the group tasked to review Internet trademark issues as the new structure evolves.

\2\ See generally MDT Corp. v. New York Stock Exchange, 858 F. Supp. 1028 (C.D. Calif. 1994).

\3\ See Lockheed Martin Corp. v. Network Solutions, Inc., 1997 WL 721899 (C.D. Calif. 11/17/97); Panavision International v. Toeppen, 1996 U.S. Dist. LEXIS 20744, 41 U.S.P.Q.2d 1310 (C.D. Calif. 1996).

E. The Intellectual Infrastructure Fund

In 1995, NSF authorized NSI to assess new domain name registrants a $50 fee per year for the first two years, 30 percent of which was to be deposited in a fund for the preservation and enhancement of the intellectual infrastructure of the Internet (the ``Intellectual Infrastructure Fund'').

In excess of $46 Million has been collected to date. In 1997, Congress authorized the crediting of $23 Million of the funds collected to the Research and Related Activities Appropriation of the National Science Foundation to support the development of the Next Generation Internet. The establishment of the Intellectual Infrastructure Fund currently is the subject of litigation in the U.S. District Court for the District of Columbia.

As the U.S. government is seeking to end its role in the domain name system, we believe the provision in the cooperative agreement regarding allocation of a portion of the registration fee to the Internet Intellectual Infrastructure Fund should terminate on April 1, 1998, the beginning of the ramp-down period of the cooperative agreement.

VII. The Transition

A number of steps must be taken to create the system envisioned in this paper.

1. The new not-for-profit organization must be established and its board chosen.
2. The membership associations representing (1) registries and registrars, and (2) Internet users, must be formed.
3. An agreement must be reached between the U.S. government and the current IANA on the transfer of IANA functions to the new organization.
4. NSI and the U.S. government must reach agreement on the terms and conditions of NSI's evolution into one competitor among many in the

registrar and registry marketplaces. A level playing field for competition must be established.

5. The new corporation must establish processes for determining whether an organization meets the transition period criteria for prospective registries and registrars.

6. A process must be laid out for making the management of the root server system more robust and secure, and, for transitioning that management from U.S. government auspices to those of the new corporation.

A. The NSI Agreement

The U.S. government will ramp down the NSI cooperative agreement and phase it out by the end of September 1998. The ramp down agreement with NSI should reflect the following terms and conditions designed to promote competition in the domain name space.

[[Page 8831]]

1. NSI will effectively separate and maintain a clear division between its current registry business and its current registrar business. NSI will continue to operate .com, .net and .org but on a fully shared-registry basis; it will shift operation of .edu to a not-for-profit entity. The registry will treat all registrars on a nondiscriminatory basis and will price registry services according to an agreed upon formula for a period of time.

2. As part of the transition to a fully shared-registry system, NSI will develop (or license) and implement the technical capability to share the registration of its top-level domains with any registrar so that any registrar can register domain names there in as soon as possible, by a date certain to be agreed upon.

3. NSI will give the U.S. government a copy and documentation of all the data, software, and appropriate licenses to other intellectual property generated under the cooperative agreement, for use by the new corporation for the benefit of the Internet.

4. NSI will turn over control of the ``A'' root server and the management of the root server system when instructed to do so by the U.S. government.

5. NSI will agree to meet the requirements for registries and registrars set out in Appendix 1.

B. Competitive Registries, Registrars, and the Addition of New gTLDs

Over the past few years, several groups have expressed a desire to enter the registry or registrar business. Ideally, the U.S. government would stay its hand, deferring the creation of a specific plan to introduce competition into the domain name system until such time as the new corporation has been organized and given an opportunity to study the questions that such proposals raise. Should the transition plan outlined below, or some other proposal, fail to achieve substantial consensus, that course may well need to be taken.

Realistically, however, the new corporation cannot be established overnight. Before operating procedures can be established, a board of directors and a CEO must be selected. Under a best case scenario, it is unlikely that the new corporation can be fully operational before September 30, 1998. It is our view, based on widespread public input, that competition should be introduced into the DNS system more quickly.

We therefore set out below a proposal to introduce competition into the domain name system during the transition from the existing U.S. government authority to a fully functioning coordinating body. This proposal is designed only for the transition period. Once the new corporation is formed, it will assume authority over the terms and conditions for the admission of new top-level domains.

Registries and New gTLDs

This proposal calls for the creation of up to five new registries, each of which would be initially permitted to operate one new gTLD. As discussed above, that number is large enough to provide valuable information about the effects of adding new gTLDs and introducing competition at the registry level, but not so large as to threaten the stability of the Internet during this transition period. In order to designate the new registries and gTLDs, IANA must establish equitable, objective criteria and processes for selecting among a large number of individuals and entities that want to provide registry services. Unsuccessful applicants will be disappointed.

We have examined a number of options for recognizing the development work already underway in the private sector. For example, some argue for the provision of a ``pioneer preference'' or other grand fathering mechanism to limit the pool of would-be registrants to those who, in response to previous IANA requests, have already invested in

developing registry businesses. While this has significant appeal and we do not rule it out, it is not an easy matter to determine who should be in that pool. IANA would be exposed to considerable liability for such determinations, and required to defend against charges that it acted in an arbitrary or inequitable manner. We welcome suggestions as to whether the pool of applicants should be limited, and if so, on what basis.

We propose, that during the transition, the first five entities (whether from a limited or unlimited pool) to meet the technical, managerial, and site requirements described in Appendix 1 will be allowed to establish a domain name registry. The IANA will engage neutral accounting and technical consultancy firms to evaluate a proposed registry under these criteria and certify an applicant as qualified. These registries may either select, in order of their qualification, from a list of available gTLDs or propose another gTLD to IANA. (We welcome suggestions on the gTLDs that should be immediately available and would propose a list based on that input, as well as any market data currently available that indicates consumer interest in particular gTLDs.)

The registry will be permitted to provide and charge for value-added services, over and above the basic services provided to registrars. At least at this time, the registry must, however, operate on a shared registry basis, treating all registrars on a nondiscriminatory basis, with respect to pricing, access and rules. Each TLD's registry should be equally accessible to any qualified registrar, so that registrants may choose their registrars competitively on the basis of price and service. The registry will also have to agree to modify its technical capabilities based on protocol changes that occur in Internet technology so that interoperability can be preserved. At some point in the future, the new organization may consider the desirability of allowing the introduction of non-shared registries.

Registrars

Any entity will be permitted to provide registrar services as long as it meets the basic technical, managerial, and site requirements as described in Appendix 1 of this paper. Registrars will be allowed to register clients into any top-level domain for which the client satisfies the eligibility rules, if any.

C. The Root Server System

IANA and the U.S. government, in cooperation with NSI, the IAB, and other relevant organizations will undertake a review of the root server system to recommend means to increase the security and professional management of the system. The recommendations of the study should be implemented as part of the transition process to the new corporation.

D. The .us Domain

At present, the IANA administers .us as a locality based hierarchy in which second-level domain space is allocated to states and US territories.4 This name space is further subdivided into localities. General registration under localities is performed on an exclusive basis by private firms that have requested delegation from IANA. The .us name space has typically been used by branches of state and local governments, although some commercial names have been assigned. Where registration for a locality has not been delegated, the IANA itself serves as the registrar.

\4\ Management principles for the .us domain space are set forth in Internet RFC 1480, (http://www.isi.edu/in-notes/rfc1480.txt)

Some in the Internet community have suggested that the pressure for unique identifiers in the .com gTLD could be relieved if commercial use of the .us space was encouraged. Commercial

[[Page 8832]]

users and trademark holders, however, find the current locality-based system too cumbersome and complicated for commercial use. Expanded use of the .us TLD could alleviate some of the pressure for new generic TLDs and reduce conflicts between American companies and others vying for the same domain name.

Clearly, there is much opportunity for enhancing the .us domain space, and the .us domain could be expanded in many ways without displacing the current geopolitical structure. Over the next few months, the U.S. government will work with the private sector and state

and local governments to determine how best to make the .us domain more attractive to commercial users. It may also be appropriate to move the gTLDs traditionally reserved for U.S. government use (i.e. .gov and .mil), into a reformulated .us ccTLD.

The U.S. government will further explore and seek public input on these issues through a separate Request for Comment on the evolution of the .us name space. However, we welcome any preliminary comments at this time.

E. The Process

The U.S. government recognizes that its unique role in the Internet domain name system should end as soon as is practical. We also recognize an obligation to end this involvement in a responsible manner that preserves the stability of the Internet. We cannot cede authority to any particular commercial interest or any specific coalition of interest groups. We also have a responsibility to oppose any efforts to fragment the Internet, as this would destroy one of the key factors--interoperability--that has made the Internet so successful.

Our goal is to seek as strong a consensus as possible so that a new, open, and accountable system can emerge that is legitimate in the eyes of all Internet stakeholders. It is in this spirit that we present this paper for discussion.

VIII. Other Information

Executive Order 12866

This proposal has been determined not to be significant under section 3(f) of Executive Order 12866.

Executive Order 12612

This rule does not contain policies with Federalism implications sufficient to warrant preparation of a Federalism assessment under Executive Order 12612.

Regulatory Flexibility Act

The Assistant General Counsel for Legislation and Regulation of the Department of Commerce certified to the Chief Counsel for Advocacy, the Small Business Administration that this proposed rule, if adopted, would not have a significant economic impact on a substantial number of small entities as follows:

We believe that the overall effect of the proposal will be highly beneficial. No negative effects are envisioned at this time. In fact, businesses will enjoy a reduction in the cost of registering domain names as a result of this proposal. In 1995, the National Science Foundation authorized a registration fee of $50 per year for the first two years, 30 percent of which was to be deposited in a fund for the preservation and enhancement of the intellectual infrastructure of the Internet (the ``Intellectual Infrastructure Fund''). The proposal seeks to terminate the agreement to earmark a portion of the registration fee to the Intellectual Infrastructure Fund. We also believe that a competitive registration system will lead to reduced fees in registering domain names.

The proposal is pro-competitive because it transfers the current system of domain name registration to a market-driven registry system. Moreover, as the Internet becomes more important to commerce, particularly small businesses, it is crucial that a more formal and robust management structure be implemented. As the commercial value of Internet names increases, decisions regarding the addition of new top-level domains should be formal, certain, and accountable to the Internet community. For example, presently, mechanisms for resolving disputes between trademark holders and domain name holders are expensive and cumbersome. The proposal requires each name registry to establish an inexpensive and efficient dispute resolution system as well as other procedures related to trademark consideration.

The U.S. government would gradually transfer existing Internet Assigned Numbers Authority (IANA) functions, the root system and the appropriate databases to a new not-for-profit corporation by September 30, 1998. The U.S. government would, however, participate in policy oversight to assure stability until the new corporation is established and stable, phasing out completely no later than September 30, 2000. Accordingly, the transition period would afford the U.S. government an opportunity to determine if the structure of the new corporation negatively impacts small entities. Moreover, the corporation would be headquartered in the U.S. and incorporated under U.S. law. Accordingly, the corporation would be subject to antitrust scrutiny if dominated by

economically interested entities, or if its standards are established by a few leading competitors.
    As a result, no initial regulatory flexibility analysis has been prepared.

Paperwork Reduction Act

    This rule does not contain information collection requirements subject to the provisions of the Paperwork Reduction Act.
Kathy Smith,
Acting Deputy Assistant Secretary for Communications and Information.

Appendix 1--Recommended Registry and Registrar Requirements

    In order to ensure the stability of the Internet's domain name system, protect consumers, and preserve the intellectual property rights of trademark owners, all registries of generic top-level domain names must meet the set of technical, managerial, and site requirements outlined below. Only prospective registries that meet these criteria will be allowed by IANA to register their gTLD in the ``A'' server. If, after it begins operations, a registry no longer meets these requirements, IANA may transfer management of the domain names under that registry's gTLD to another organization.
    Independent testing, reviewing, and inspection called for in the requirements for registries should be done by appropriate certifying organizations or testing laboratories rather than IANA itself, although IANA will define the requirements and the procedures for tests and audits.
    These requirements apply only to generic TLDs. They will apply to both existing gTLDs (e.g., .com, .edu., .net, .org) and new gTLDs. Although they are not required to, we expect many ccTLD registries and registrars may wish to assure their customers that they meet these requirements or similar ones.
    Registries will be separate from registrars and have only registrars as their customers. If a registry wishes to act both as registry and registrar for the same TLD, it must do so through separate subsidiaries. Appropriate accounting and confidentiality safeguards shall be used to ensure that the registry subsidiary's business is not utilized in any manner to benefit the registrar subsidiary to the detriment of any other registrar.
    Each top-level domain (TLD) database will be maintained by only one registry and, at least initially, each new registry can host only one TLD.

Registry Requirements

    1. An independently-tested, functioning Database and Communications System that:
    a. Allows multiple competing registrars to have secure access (with encryption and authentication) to the database on an equal (first-come, first-served) basis.

[[Page 8833]]

    b. Is both robust (24 hours per day, 365 days per year) and scalable (i.e., capable of handling high volumes of entries and inquiries).
    c. Has multiple high-throughput (i.e., at least T1) connections to the Internet via at least two separate Internet Service Providers.
    d. Includes a daily data backup and archiving system.
    e. Incorporates a record management system that maintains copies of all transactions, correspondence, and communications with registrars for at least the length of a registration contract.
    f. Features a searchable, on-line database meeting the requirements of Appendix 2.
    g. Provides free access to the software and customer interface that a registrar would need to register new second-level domain names.
    h. An adequate number (perhaps two or three) of globally-positioned zone-file servers connected to the Internet for each TLD.
    2. Independently-reviewed Management Policies, Procedures, and Personnel including:
    a. Alternate (i.e., non-litigation) dispute resolution providing a timely and inexpensive forum for trademark-related complaints. (These procedures should be consistent with applicable national laws and compatible with any available judicial or administrative remedies.)
    b. A plan to ensure that the registry's obligations to its

customers will be fulfilled in the event that the registry goes out of business. This plan must indicate how the registry would ensure that domain name holders will continue to have use of their domain name and that operation of the Internet will not be adversely affected.

c. Procedures for assuring and maintaining the expertise and experience of technical staff.

d. Commonly-accepted procedures for information systems security to prevent malicious hackers and others from disrupting operations of the registry.

3. Independently inspected Physical Sites that feature:

a. A backup power system including a multi-day power source.

b. A high level of security due to twenty-four-hour guards and appropriate physical safeguards against intruders.

c. A remotely-located, fully redundant and staffed twin facility with ``hot switchover'' capability in the event of a main facility failure caused by either a natural disaster (e.g., earthquake or tornado) or an accidental (fire, burst pipe) or deliberate (arson, bomb) man-made event. (This might be provided at, or jointly supported with, another registry, which would encourage compatibility of hardware and commonality of interfaces.)

Registrar Requirements

Registries will set standards for registrars with which they wish to do business. The following are the minimal qualifications that IANA should mandate that each registry impose and test or inspect before allowing a registrar to access its database(s). Any additional requirements imposed by registries on registrars must be approved by IANA and should not affect the stability of the Internet or substantially reduce competition in the registrar business. Registries may refuse to accept registrations from registrars that fail to meet these requirements and may remove domain names from the registries if at a later time the registrar which registered them no longer meets the requirements for registrars.

1. A functioning Database and Communications System that supports:

a. Secure access (with encryption and authentication) to the registry.

b. Robust and scalable operations capable of handling moderate volumes.

c. Multiple connections to the Internet via at least two Internet Service Providers.

d. A daily data backup and archival system.

e. A record management system that maintains copies of all transactions, correspondence, and communications with all registries for at least the length of a registration contract.

2. Management Policies, Procedures, and Personnel including:

a. A plan to ensure that the registrar's obligations to its customers and to the registries will be fulfilled in the event that the registrar goes out of business. This plan must indicate how the registrar would ensure that domain name holders will continue to have use of their domain name and that operation of the Internet will not be adversely affected.

b. Commonly-accepted procedures for information systems security to prevent malicious hackers and others from disrupting operations.

3. Independently inspected Physical Sites that features:

a. A backup power system.

b. A high level of security due to twenty-four-hour guards and appropriate physical safeguards against intruders.

c. Remotely-stored backup files to permit recreation of customer records.

Appendix 2--Minimum Dispute Resolution and Other Procedures Related to Trademarks

1. Minimum Application Requirements.

a. Sufficient owner and contact information (e.g., names, mail address for service of process, e-mail address, telephone and fax numbers, etc.) to enable an interested party to contact either the owner/applicant or its designated representative; and a

b. Certification statement by the applicant that:

--It is entitled to register the domain name for which it is applying and knows of no entity with superior rights in the domain name; and
--It intends to use the domain name.

2. Searchable Database Requirements.

a. Utilizing a simple, easy-to-use, standardized search interface that features multiple field or string searching and the retrieval of similar names, the following information must be included in all registry databases, and available to anyone with access to the Internet:

--Up-to-date ownership and contact information;
--Up-to-date and historical chain of title information for the domain name;
--A mail address for service of process;
--The date of the domain name registration; and
--The date an objection to registration of the domain name was filed.

3. Updated Ownership, Contact and Use Information.
a. At any time there is a change in ownership, the domain name owner must submit the following information:

--Up-to-date contact and ownership information; and
--A description of how the owner is using the domain name, or, if the domain name is not in use, a statement to that effect.

4. Alternative Dispute Resolution of Domain Name Conflicts.
a. There must be a readily available and convenient dispute resolution process that requires no involvement by registrars.
b. Registries/Registrars will abide by the decisions resulting from an agreed upon dispute resolution process or by the decision of a court of competent jurisdiction.
If an objection to registration is raised within 30 days after registration of the domain name, a brief period of suspension during the pendency of the dispute will be provided by the registries.

[FR Doc. 98-4200 Filed 2-19-98; 8:45 am]
BILLING CODE 3510-60-P

National Telecommunications and Information Administration
1401 Constitution Ave., NW Washington, DC 20230

commerce.gov | Privacy Policy | Web Policies | FOIA | Accessibility | usa.gov

---

Source URL: https://www.ntia.doc.gov/federal-register-notice/1998/improvement-technical-management-internet-names-and-addresses-proposed-

EXHIBIT JMR-7

JMR-7

MEMORANDUM OF UNDERSTANDING BETWEEN
THE U.S. DEPARTMENT OF COMMERCE
AND
INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS

I. PARTIES

This document constitutes an agreement between the U.S. Department of Commerce (DOC or USG) and the Internet Corporation for Assigned Names and Numbers (ICANN), a not-for-profit corporation.

II. PURPOSE

A. Background

On July 1, 1997, as part of the Administration's Framework for Global Electronic Commerce, the President directed the Secretary of Commerce to privatize the management of the domain name system (DNS) in a manner that increases competition and facilitates international participation in its management.

On June 5, 1998, the DOC published its Statement of Policy, *Management of Internet Names and Addresses,* 63 *Fed. Reg.* 31741(1998) (Statement of Policy). The Statement of Policy addressed the privatization of the technical management of the DNS in a manner that allows for the development of robust competition in the management of Internet names and addresses. In the Statement of Policy, the DOC stated its intent to enter an agreement with a not-for-profit entity to establish a process to transition current U.S. Government management of the DNS to such an entity based on the principles of stability, competition, bottom-up coordination, and representation.

B. Purpose

Before making a transition to private sector DNS management, the DOC requires assurances that the private sector has the capability and resources to assume the important responsibilities related to the technical management of the DNS. To secure these assurances, the Parties will collaborate on this DNS Project (DNS Project). In the DNS Project, the Parties will jointly design, develop, and test the mechanisms, methods, and procedures that should be in place and the steps necessary to transition management responsibility for DNS functions now performed by, or on behalf of, the U.S. Government to a private-sector not-for-profit entity. Once testing is successfully completed, it is contemplated that management of the DNS will be transitioned to the mechanisms, methods, and procedures designed and developed in the DNS Project.

In the DNS Project, the parties will jointly design, develop, and test the mechanisms, methods, and procedures to carry out the following DNS management functions:

a. Establishment of policy for and direction of the allocation of IP number blocks;

b. Oversight of the operation of the authoritative root server system;

c. Oversight of the policy for determining the circumstances under which new top level domains would be added to the root system;

d. Coordination of the assignment of other Internet technical parameters as needed to maintain universal connectivity on the Internet; and

e. Other activities necessary to coordinate the specified DNS management functions, as agreed by the Parties.

The Parties will jointly design, develop, and test the mechanisms, methods, and procedures that will achieve the transition without disrupting the functional operation of the Internet. The Parties will also prepare a joint DNS Project Report that documents the conclusions of the design, development, and testing.

DOC has determined that this project can be done most effectively with the participation of ICANN. ICANN has a stated purpose to perform the described coordinating functions for Internet names and addresses and is the organization that best demonstrated that it can accommodate the broad and diverse interest groups that make up the Internet community.

C. The Principles

The Parties will abide by the following principles:

1. Stability

This Agreement promotes the stability of the Internet and allows the Parties to plan for a deliberate move from the existing structure to a private-sector structure without disruption to the functioning of the DNS. The Agreement calls for the design, development, and testing of a new management system that will not harm current functional operations.

2. Competition

This Agreement promotes the management of the DNS in a manner that will permit market mechanisms to support competition and consumer choice in the technical management of the DNS. This competition will lower costs, promote innovation, and enhance user choice and satisfaction.

3. Private, Bottom-Up Coordination

This Agreement is intended to result in the design, development, and testing of a private coordinating process that is flexible and able to move rapidly enough to meet the changing needs of the Internet and of Internet users. This Agreement is intended to foster the development of a private sector management system that, as far as possible, reflects a system of bottom-up management.

4. Representation.

This Agreement promotes the technical management of the DNS in a manner that reflects the global and functional diversity of Internet users and their needs. This Agreement is intended to promote the design, development, and testing of mechanisms to solicit public input, both domestic and international, into a private-sector decision making process. These mechanisms will promote the flexibility needed to adapt to changes in the composition of the Internet user community and their needs.

III. AUTHORITIES

A. DOC has authority to participate in the DNS Project with ICANN under the following authorities:

(1) 15 U.S.C. § 1525, the DOC's Joint Project Authority, which provides that the DOC may enter into joint projects with nonprofit, research, or public organizations on matters of mutual interest, the cost of which is equitably apportioned;

(2) 15 U.S.C. § 1512, the DOC's authority to foster, promote, and develop foreign and domestic commerce;

(3) 47 U.S.C. § 902, which specifically authorizes the National Telecommunications and Information Administration (NTIA) to coordinate the telecommunications activities of the Executive Branch and assist in the formulation of policies and standards for those activities including, but not limited to, considerations of interoperability, privacy, security, spectrum use, and emergency readiness;

(4) Presidential Memorandum on Electronic Commerce, 33 Weekly Comp. Presidential Documents 1006 (July 1, 1997), which directs the Secretary of Commerce to transition DNS management to the private sector; and

(5) Statement of Policy, *Management of Internet Names and Addresses*, (63 *Fed. Reg.* 31741(1998) (Attachment A), which describes the manner in which the Department of Commerce will transition DNS management to the private sector.

B. ICANN has the authority to participate in the DNS Project, as evidenced in its Articles of Incorporation (Attachment B) and Bylaws (Attachment C). Specifically, ICANN has stated that its business purpose is to:

(i) coordinate the assignment of Internet technical parameters as needed to maintain universal connectivity on the Internet;

(ii) perform and oversee functions related to the coordination of the Internet Protocol (IP) address space;

(iii) perform and oversee functions related to the coordination of the Internet domain name system, including the development of policies for determining the circumstances under which new top-level domains are added to the DNS root system;

(iv) oversee operation of the authoritative Internet DNS root server system; and

(v) engage in any other related lawful activity in furtherance of Items (i) through (iv).

IV. MUTUAL INTEREST OF THE PARTIES

Both DOC and ICANN have a mutual interest in a transition that ensures that future technical management of the DNS adheres to the principles of stability, competition, coordination, and representation as published in the Statement of Policy. ICANN has declared its commitment to these principles in its Bylaws. This Agreement is essential for the DOC to ensure continuity and stability in the performance of technical management of the DNS now performed by, or on behalf of, the U.S. Government. Together, the Parties will collaborate on the DNS Project to achieve the transition without disruption.

V. RESPONSIBILITIES OF THE PARTIES

A. General.

1. The Parties agree to jointly participate in the DNS Project for the design, development, and testing of the mechanisms, methods and procedures that should be in place for the private sector to manage the functions delineated in the Statement of Policy in a transparent, non-arbitrary, and reasonable manner.

2. The Parties agree that the mechanisms, methods, and procedures developed under the DNS Project will ensure that private-sector technical management of the DNS shall not apply standards, policies, procedures or practices inequitably or single out any particular party for disparate treatment unless justified by substantial and reasonable cause and will ensure sufficient appeal procedures for adversely affected members of the Internet community.

3. Before the termination of this Agreement, the Parties will collaborate on a DNS Project Report that will document ICANN's test of the policies and procedures designed and developed pursuant to this Agreement.

4. The Parties agree to execute the following responsibilities in accordance with the Principles and Purpose of this Agreement as set forth in section II.

B. DOC. The DOC agrees to perform the following activities and provide the following resources in support of the DNS Project:

1. Provide expertise and advice on existing DNS management functions.

2. Provide expertise and advice on methods and administrative procedures for conducting open, public proceedings concerning policies and procedures that address the technical management of the DNS.

3. Identify with ICANN the necessary software, databases, know-how, other equipment, and intellectual property necessary to design, develop, and test methods and procedures of the DNS Project.

4. Participate, as necessary, in the design, development, and testing of the methods and procedures of the DNS Project to ensure continuity including coordination between ICANN and Network Solutions, Inc.

5. Collaborate on a study on the design, development, and testing of a process for making the management of the root server system more robust and secure. This aspect of the DNS Project will address:

a. Operational requirements of root name servers, including host hardware capacities, operating system and name server software versions, network connectivity, and physical environment.

b. Examination of the security aspects of the root name server system and review of the number, location, and distribution of root name servers considering the total system performance, robustness, and reliability.

c. Development of operational procedures for the root server system, including formalization of contractual relationships under which root servers throughout the world are operated.

6. Consult with the international community on aspects of the DNS Project.

7. Provide general oversight of activities conducted pursuant to this Agreement.

8. Maintain oversight of the technical management of DNS functions currently performed either directly, or subject to agreements with the U.S. Government, until such time as further agreement(s) are arranged as necessary, for the private sector to undertake management of specific DNS technical management functions.

C. ICANN. ICANN agrees to perform the following activities and provide the following resources in support of the DNS Project and further agrees to undertake the following activities pursuant to its procedures as set forth in Attachment B (Articles of Incorporation) and Attachment C (By-Laws), as they may be revised from time to time in conformity with the DNS Project:

1. Provide expertise and advice on private sector functions related to technical management of the DNS such as the policy and direction of the allocation of IP number blocks and coordination of the assignment of other Internet technical parameters as needed to maintain universal connectivity on the Internet.

2. Collaborate on the design, development and testing of procedures by which members of the Internet community adversely affected by decisions that are in conflict with the bylaws of the organization can seek external review of such decisions by a neutral third party.

3. Collaborate on the design, development, and testing of a plan for introduction of competition in domain name registration services, including:

a. Development of procedures to designate third parties to participate in tests conducted pursuant to this Agreement.

b. Development of an accreditation procedure for registrars and procedures that subject registrars to consistent requirements designed to promote a stable and robustly competitive DNS, as set forth in the Statement of Policy.

c. Identification of the software, databases, know-how, intellectual property, and other equipment necessary to implement the plan for competition;

4. Collaborate on written technical procedures for operation of the primary root server including procedures that permit modifications, additions or deletions to the root zone file.

5. Collaborate on a study and process for making the management of the root server system more robust and secure. This aspect of the Project will address:

a. Operational requirements of root name servers, including host hardware capacities, operating system and name server software versions, network connectivity, and physical environment.

b. Examination of the security aspects of the root name server system and review of the number, location , and distribution of root name servers considering the total system performance; robustness, and reliability.

c. Development of operational procedures for the root system, including formalization of contractual relationships under which root servers throughout the world are operated.

6. Collaborate on the design, development and testing of a process for affected parties to participate in the formulation of policies and procedures that address the technical management of the Internet. This process will include methods for soliciting, evaluating and responding to comments in the adoption of policies and procedures.

7. Collaborate on the development of additional policies and procedures designed to provide information to the public.

8. Collaborate on the design, development, and testing of appropriate membership mechanisms that foster accountability to and representation of the global and functional diversity of the Internet and its users, within the structure of private-sector DNS management organization.

9. Collaborate on the design, development and testing of a plan for creating a process that will consider the possible expansion of the number of gTLDs. The designed process should consider and take into account the following:

a. The potential impact of new gTLDs on the Internet root server system and Internet stability.

b. The creation and implementation of minimum criteria for new and existing gTLD registries.

c. Potential consumer benefits/costs associated with establishing a competitive environment for gTLD registries.

d. Recommendations regarding trademark/domain name policies set forth in the Statement of Policy; recommendations made by the World Intellectual Property Organization (WIPO) concerning: (i) the development of a uniform approach to resolving trademark/domain name disputes involving cyberpiracy; (ii) a process for protecting famous trademarks in the generic top level domains; (iii) the effects of adding new gTLDs and related dispute resolution procedures on trademark and intellectual property holders; and recommendations made by other independent organizations concerning trademark/domain name issues.

10. Collaborate on other activities as appropriate to fulfill the purpose of this Agreement, as agreed by the Parties.

D. Prohibitions.

1. ICANN shall not act as a domain name Registry or Registrar or IP Address Registry in competition with entities affected by the plan developed under this Agreement. Nothing, however, in this Agreement is intended to prevent ICANN or the USG from taking reasonable steps that are necessary to protect the operational stability of the Internet in the event of the financial failure of a Registry or Registrar or other emergency.

2. Neither Party, either in the DNS Project or in any act related to the DNS Project, shall act unjustifiably or arbitrarily to injure particular persons or entities or particular categories of persons or entities.

3. Both Parties shall act in a non-arbitrary and reasonable manner with respect to design, development, and testing of the DNS Project and any other activity related to the DNS Project.

VI. EQUITABLE APPORTIONMENT OF COSTS

The costs of this activity are equitably apportioned, and each party shall bear the costs of its own activities under this Agreement. This Agreement contemplates no transfer of funds between the Parties. Each Party's estimated costs for the first six months of this Agreement are attached hereto. The Parties shall review these estimated costs in light of actual expenditures at the completion of the first six month period and will ensure costs will be equitably apportioned.

VII. PERIOD OF AGREEMENT AND MODIFICATION/TERMINATION

This Agreement will become effective when signed by all parties. The Agreement will terminate on September 30, 2000, but may be amended at any time by mutual agreement of the parties. Either party may terminate this Agreement by providing one hundred twenty (120) days written notice to the other party. In the event this Agreement is terminated, each party shall be solely responsible for the payment of any expenses it has incurred. This Agreement is subject to the availability of funds.

J. Beckw th Burr
Assoc ate Adm n strator, NTIA
U.S. Department of Commerce
Wash ngton, D.C. 20230

Joe S ms
Counse to ICANN
Jones, Day, Reav s & Pogue
1450 G Street N.W.
Wash ngton, D.C. 20005-2088

PARTIES ESTIMATED SIX MONTH COSTS

A. ICANN

Costs to be borne by ICANN over the first six months of this Agreement include: development of Accreditation Guidelines for Registries; review of Technical Specifications for Shared Registries; formation and operation of Government, Root Server, Membership and Independent Review Advisor Committees; advice on formation of and review of applications for recognition by Supporting Organizations; promulgation of conflicts of interest policies; review and adoption of At-Large membership and elections processes and independent review procedures, etc; quarterly regular Board meetings and associated costs (including open forums, travel, staff support and communications infrastructure); travel, administrative support and infrastructure for additional open forums to be determined; internal executive, technical and administrative costs; legal and other professional services; and related other costs. The estimated six month budget (subject to change and refinement over time) is $750,000 - 1 million.

B. DOC

Costs to be borne by DOC over the first six months of this Agreement include: maintenance of DNS technical management functions currently performed by, or subject to agreements with, the U.S. Government, expertise and advice on existing DNS management functions; expertise and advice on administrative procedures; examination and review of the security aspects of the Root Server System (including travel and technical expertise); consultations with the international community on aspects of the DNS Project (including travel and communications costs); general oversight of activities conducted pursuant to the Agreement; staff support equal to half-time dedication of 4-5 full time employees, travel, administrative support, communications and related other costs. The estimate six month budget (subject to change and refinement over time) is $250,000 - $350,000.

Comments concern ng the ayout, construct on and funct ona ty of th s s te
shou d be sent to webmaster@ cann.org.

Page Updated 31-December-99.

(c) 1999 The n erne Corpora ion for Assigned Names and Numbers All righ s reserved

EXHIBIT JMR-8

Resources

- About ICANN
- Board
- Accountability
- Governance
  - Governance Documents
    - Guidelines
    - Articles of Incorporation
      - Current
      - Archive
    - Bylaws
    - Board Code of Conduct
    - Board Conflicts of Interest Policy
    - Board Statements of Interest
    - Lobbying Disclosures & Contribution Reports
    - Summary of Conflicts of Interest and Ethics

ARTICLES OF INCORPORATION OF INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS

This page is available in:
English | العربية | Español | Français | Русский | 中文

As Revised November 21, 1998

1. The name of this corporation is Internet Corporation for Assigned Names and Numbers (the "Corporation").

2. The name of the Corporation's initial agent for service of process in the State of California, United States of America is C T Corporation System.

3. This Corporation is a nonprofit public benefit corporation and is not organized for the private gain of any person. It is organized under the California Nonprofit Public Benefit Corporation Law for charitable and public purposes. The Corporation is organized, and will be operated, exclusively for charitable, educational, and scientific purposes within the meaning of § 501 (c) (3) of the Internal Revenue Code of 1986, as amended (the "Code"), or the corresponding provision of any future United States tax code. Any reference in these Articles to the Code shall include the corresponding provisions of any further United States tax code. In furtherance of the foregoing purposes, and in recognition of the fact that the Internet is an international network of networks, owned by no single nation, individual or organization, the Corporation shall, except as limited by Article 5 hereof, pursue the charitable and public purposes of lessening the burdens of government and promoting the global public interest in the operational stability of the Internet by (i) coordinating the assignment of Internet technical parameters as needed to maintain universal connectivity on the Internet; (ii) performing and overseeing functions related to the coordination of the Internet Protocol ("IP") address space; (iii) performing and overseeing functions related to the coordination of the Internet domain name system ("DNS"), including the development of policies for determining the circumstances under which new top-level domains are added to the DNS root system; (iv) overseeing operation of the

Practices Review

- Agreements
- Annual Reports
- Financials
- Planning
- Presentations
- RFPs
- Litigation
- Newsletter
- Correspondence
- Quarterly Reports

- Groups
- Business
- Civil Society
- Complaints Office
- Contractual Compliance
- Registrars
- Registry Operators
- Domain Name Registrants
- GDD Metrics
- Identifier Systems Security, Stability and Resiliency (OCTO IS-SSR)

authoritative Internet DNS root server system; and (v) engaging in any other related lawful activity in furtherance of items (i) through (iv).

4. The Corporation shall operate for the benefit of the Internet community as a whole, carrying out its activities in conformity with relevant principles of international law and applicable international conventions and local law and, to the extent appropriate and consistent with these Articles and its Bylaws, through open and transparent processes that enable competition and open entry in Internet-related markets. To this effect, the Corporation shall cooperate as appropriate with relevant international organizations.

5. Notwithstanding any other provision (other than Article 8) of these Articles:

a. The Corporation shall not carry on any other activities not permitted to be carried on (i) by a corporation exempt from United States income tax under § 501 (c)(3) of the Code or (ii) by a corporation, contributions to which are deductible under § 170 (c)(2) of the Code.

b. No substantial part of the activities of the Corporation shall be the carrying on of propaganda, or otherwise attempting to influence legislation, and the Corporation shall be empowered to make the election under § 501 (h) of the Code.

c. The Corporation shall not participate in, or intervene in (including the publishing or distribution of statements) any political campaign on behalf of or in opposition to any candidate for public office.

d. No part of the net earnings of the Corporation shall inure to the benefit of or be distributable to its members, directors, trustees, officers, or other private persons, except that the Corporation shall be authorized and empowered to pay reasonable compensation for services rendered and to make payments and distributions in furtherance of the purposes set forth in Article 3 hereof.

e. In no event shall the Corporation be controlled directly or indirectly by one or more "disqualified persons" (as defined in § 4946 of the Code) other than foundation managers and other than one or more organizations described in paragraph (1) or (2) of § 509 (a) of the Code.

6. To the full extent permitted by the California Nonprofit Public Benefit Corporation Law or any other applicable laws presently or hereafter in effect, no director of the Corporation shall be personally liable to the Corporation or its members, should the Corporation elect to have members in the future, for or with respect to any acts or omissions in the performance of his or her duties as a director of the Corporation. Any repeal or modification of this Article 6

- ccTLDs
- Internationalized Domain Names
- Universal Acceptance Initiative
- Policy
- Public Comment
- Root Zone KSK Rollover
- Technical Functions
- Contact
- Help

shall not adversely affect any right or protection of a director of the Corporation existing immediately prior to such repeal or modification.

7. Upon the dissolution of the Corporation, the Corporation's assets shall be distributed for one or more of the exempt purposes set forth in Article 3 hereof and, if possible, to a § 501 (c)(3) organization organized and operated exclusively to lessen the burdens of government and promote the global public interest in the operational stability of the Internet, or shall be distributed to a governmental entity for such purposes, or for such other charitable and public purposes that lessen the burdens of government by providing for the operational stability of the Internet. Any assets not so disposed of shall be disposed of by a court of competent jurisdiction of the county in which the principal office of the Corporation is then located, exclusively for such purposes or to such organization or organizations, as such court shall determine, that are organized and operated exclusively for such purposes, unless no such corporation exists, and in such case any assets not disposed of shall be distributed to a § 501(c)(3) corporation chosen by such court.

8. Notwithstanding anything to the contrary in these Articles, if the Corporation determines that it will not be treated as a corporation exempt from federal income tax under § 501(c)(3) of the Code, all references herein to § 501(c)(3) of the Code shall be deemed to refer to § 501(c)(6) of the Code and Article 5(a)(ii), (b), (c) and (e) shall be deemed not to be a part of these Articles.

9. These Articles may be amended by the affirmative vote of at least two-thirds of the directors of the Corporation. When the Corporation has members, any such amendment must be ratified by a two-thirds (2/3) majority of the members voting on any proposed amendment.

Who We Are
- Get Started
- Learning
- Participate
- Groups
- Board
- President's Corner
- Staff
- Careers
- Public Responsibility

Contact Us
- Locations
- Global Support
- Report Security Issues
- PGP Keys
- Certificate Authority
- Registry Liaison
- Specific Reviews
- Organizational Reviews
- Complaints Office
- Request a Speaker
- For Journalists

Accountability & Transparency
- Accountability Mechanisms
- Independent Review Process
- Request for Reconsideration
- Ombudsman
- Empowered Community

Governance
- Documents
- Agreements
- Specific Reviews
- Annual Report
- Financials
- Document Disclosure
- Planning
- Accountability Indicators
- RFPs
- Litigation
- Correspondence

Help
- Dispute Resolution
- Domain Name Dispute Resolution
- Name Collision
- Registrar Problems
- WHOIS

Data Protection
- Data Privacy Practices
- Privacy Policy
- Terms of Service
- Cookies Policy

© 2018 Internet Corporation for Assigned Names and Numbers. Privacy Policy Terms of Service Cookies Policy

EXHIBIT JMR-9

JMR-9

Bylaws

Effective as of 15 December 2002

Note: this page is an archive of an old version of the bylaws. The current ICANN bylaws are always available at:
https://www.icann.org/resources/pages/governance/bylaws-en

BYLAWS FOR INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS
A California Nonprofit Public-Benefit Corporation
As adopted effective 15 December 2002 (the "New Bylaws")

TABLE OF CONTENTS

ARTICLE I: MISSION AND CORE VALUES

Section 1. MISSION

The mission of The Internet Corporation for Assigned Names and Numbers ("ICANN") is to coordinate, at the overall level, the global Internet's systems of

unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems. In particular, ICANN:

1. Coordinates the allocation and assignment of the three sets of unique identifiers for the Internet, which are

a. Domain names (forming a system referred to as "DNS");

b. Internet protocol ("IP") addresses and autonomous system ("AS") numbers; and

c. Protocol port and parameter numbers.

2. Coordinates the operation and evolution of the DNS root name server system.

3. Coordinates policy development reasonably and appropriately related to these technical functions.

Section 2. CORE VALUES

In performing its mission, the following core values should guide the decisions and actions of ICANN:

1. Preserving and enhancing the operational stability, reliability, security, and global interoperability of the Internet.

2. Respecting the creativity, innovation, and flow of information made possible by the Internet by limiting ICANN's activities to those matters within ICANN's mission requiring or significantly benefiting from global coordination.

3. To the extent feasible and appropriate, delegating coordination functions to or recognizing the policy role of other responsible entities that reflect the interests of affected parties.

4. Seeking and supporting broad, informed participation reflecting the functional, geographic, and cultural diversity of the Internet at all levels of policy development and decision-making.

5. Where feasible and appropriate, depending on market mechanisms to promote and sustain a competitive environment.

6. Introducing and promoting competition in the registration of domain names where practicable and beneficial in the public interest.

7. Employing open and transparent policy development mechanisms that (i) promote well-informed decisions based on expert advice, and (ii) ensure that those entities most affected can assist in the policy development process.

8. Making decisions by applying documented policies neutrally and objectively, with integrity and fairness.

9. Acting with a speed that is responsive to the needs of the Internet while, as part of the decision-making process, obtaining informed input from those entities most affected.

10. Remaining accountable to the Internet community through mechanisms that enhance ICANN's effectiveness.

11. While remaining rooted in the private sector, recognizing that governments and public authorities are responsible for public policy and duly taking into account governments' or public authorities' recommendations.

These core values are deliberately expressed in very general terms, so that they may provide useful and relevant guidance in the broadest possible range of circumstances. Because they are not narrowly prescriptive, the specific way in which they apply, individually and collectively, to each new situation will necessarily depend on many factors that cannot be fully anticipated or enumerated; and because they are statements of principle rather than practice, situations will inevitably arise in which perfect fidelity to all eleven core values simultaneously is not possible. Any ICANN body making a recommendation or decision shall exercise its judgment to determine which core values are most relevant and how they apply to the specific circumstances of the case at hand, and to determine, if necessary, an appropriate and defensible balance among competing values.

ARTICLE II: POWERS

Section 1. GENERAL POWERS

Except as otherwise provided in the Articles of Incorporation or these Bylaws, the powers of ICANN shall be exercised by, and its property controlled and its business and affairs conducted by or under the direction of, the Board. With respect to any matters that would fall within the provisions of Article III, Section 6, the Board may act only by a majority vote of all members of the Board. In all other matters, except as otherwise provided in these Bylaws or by law, the Board may act by majority vote of those present at any annual, regular, or special meeting of the Board. Any references in these Bylaws to a vote of the Board shall mean the vote of only those members present at the meeting where a quorum is present unless otherwise specifically provided in these Bylaws by reference to "all of the members of the Board."

Section 2. RESTRICTIONS

ICANN shall not act as a Domain Name System Registry or Registrar or Internet Protocol Address Registry in competition with entities affected by the policies of ICANN. Nothing in this Section is intended to prevent ICANN from taking whatever steps are necessary to protect the operational stability of the Internet in the event of financial failure of a Registry or Registrar or other emergency.

Section 3. NON-DISCRIMINATORY TREATMENT

ICANN shall not apply its standards, policies, procedures, or practices inequitably or single out any particular party for disparate treatment unless

justified by substantial and reasonable cause, such as the promotion of effective competition.

ARTICLE III: TRANSPARENCY

Section 1. PURPOSE

ICANN and its constituent bodies shall operate to the maximum extent feasible in an open and transparent manner and consistent with procedures designed to ensure fairness.

Section 2. WEBSITE

ICANN shall maintain a publicly-accessible Internet World Wide Web site (the "Website"), which may include, among other things, (i) a calendar of scheduled meetings of the Board, Supporting Organizations, and Advisory Committees; (ii) a docket of all pending policy development matters, including their schedule and current status; (iii) specific meeting notices and agendas as described below; (iv) information on ICANN's budget, annual audit, financial contributors and the amount of their contributions, and related matters; (v) information about the availability of accountability mechanisms, including reconsideration, independent review, and Ombudsman activities, as well as information about the outcome of specific requests and complaints invoking these mechanisms; (vi) announcements about ICANN activities of interest to significant segments of the ICANN community; (vii) comments received from the community on policies being developed and other matters; (viii) information about ICANN's physical meetings and public forums; and (ix) other information of interest to the ICANN community.

Section 3. MANAGER OF PUBLIC PARTICIPATION

There shall be a staff position designated as Manager of Public Participation, or such other title as shall be determined by the President, that shall be responsible, under the direction of the President, for coordinating the various aspects of public participation in ICANN, including the Website and various other means of communicating with and receiving input from the general community of Internet users.

Section 4. MEETING NOTICES AND AGENDAS

At least seven days in advance of each Board meeting (or if not practicable, as far in advance as is practicable), a notice of such meeting and, to the extent known, an agenda for the meeting shall be posted.

Section 5. MINUTES AND PRELIMINARY REPORTS

1. All minutes of meetings of the Board and Supporting Organizations (and any councils thereof) shall be approved promptly by the originating body and provided to the ICANN Secretary for posting on the Website.

2. No later than five (5) days after each meeting, any actions taken by the Board shall be made publicly available in a preliminary report on

the Website; provided, however, that any actions relating to personnel or employment matters, legal matters (to the extent the Board determines it is necessary or appropriate to protect the interests of ICANN), matters that ICANN is prohibited by law or contract from disclosing publicly, and other matters that the Board determines, by a three-quarters (3/4) vote of Directors present at the meeting and voting, are not appropriate for public distribution, shall not be included in the preliminary report made publicly available. For any matters that the Board determines not to disclose, the Board shall describe in general terms in the relevant preliminary report the reason for such nondisclosure.

3. No later than the day after the date on which they are formally approved by the Board, the minutes shall be made publicly available on the Website; provided, however, that any minutes relating to personnel or employment matters, legal matters (to the extent the Board determines it is necessary or appropriate to protect the interests of ICANN), matters that ICANN is prohibited by law or contract from disclosing publicly, and other matters that the Board determines, by a three-quarters (3/4) vote of Directors present at the meeting and voting, are not appropriate for public distribution, shall not be included in the minutes made publicly available. For any matters that the Board determines not to disclose, the Board shall describe in general terms in the relevant minutes the reason for such nondisclosure.

Section 6. NOTICE AND COMMENT ON POLICY ACTIONS

1. With respect to any policies that are being considered by the Board for adoption that substantially affect the operation of the Internet or third parties, including the imposition of any fees or charges, ICANN shall:

a. provide public notice on the Website explaining what policies are being considered for adoption and why, at least twenty-one days (and if practical, earlier) prior to any action by the Board;

b. provide a reasonable opportunity for parties to comment on the adoption of the proposed policies, to see the comments of others, and to reply to those comments, prior to any action by the Board; and

c. in those cases where the policy action affects public policy concerns, to request the opinion of the Governmental Advisory Committee and take duly into account any advice timely presented by the Governmental Advisory Committee on its own initiative or at the Board's request.

2. Where both practically feasible and consistent with the relevant policy development process, an in-person public forum shall also be

held for discussion of any proposed policies as described in Section 6 (1)(b) of this Article, prior to any final Board action.

3. After taking action on any policy subject to this Section, the Board shall publish in the meeting minutes the reasons for any action taken, the vote of each Director voting on the action, and the separate statement of any Director desiring publication of such a statement.

Section 7. TRANSLATION OF DOCUMENTS

As appropriate and to the extent provided in the ICANN budget, ICANN shall facilitate the translation of final published documents into various appropriate languages.

ARTICLE IV: ACCOUNTABILITY AND REVIEW

Section 1. PURPOSE

In carrying out its mission as set out in these Bylaws, ICANN should be accountable to the community for operating in a manner that is consistent with these Bylaws, and with due regard for the core values set forth in Article I of these Bylaws. The provisions of this Article, creating processes for reconsideration and independent review of ICANN actions and periodic review of ICANN's structure and procedures, are intended to reinforce the various accountability mechanisms otherwise set forth in these Bylaws, including the transparency provisions of Article III and the Board and other selection mechanisms set forth throughout these Bylaws.

Section 2. RECONSIDERATION

1. ICANN shall have in place a process by which any person or entity materially affected by an action of ICANN may request review or reconsideration of that action by the Board.

2. Any person or entity may submit a request for reconsideration or review of an ICANN action or inaction ("Reconsideration Request") to the extent that he, she, or it have been adversely affected by:

a. one or more staff actions or inactions that contradict established ICANN policy(ies); or

b. one or more actions or inactions of the ICANN Board that have been taken or refused to be taken without consideration of material information, except where the party submitting the request could have submitted, but did not submit, the information for the Board's consideration at the time of action or refusal to act.

3. There shall be a Committee of the Board consisting of not less than three directors to review and consider any such requests ("Reconsideration Committee"). The Reconsideration Committee shall have the authority to:

a. evaluate requests for review or reconsideration;

b. determine whether a stay of the contested action pending resolution of the request is appropriate;

c. conduct whatever factual investigation is deemed appropriate;

d. request additional written submissions from the affected party, or from other parties; and

e. make a recommendation to the Board of Directors on the merits of the request.

4. ICANN shall absorb the normal administrative costs of the reconsideration process. It reserves the right to recover from a party requesting review or reconsideration any costs which are deemed to be extraordinary in nature. When such extraordinary costs can be foreseen, that fact and the reasons why such costs are necessary and appropriate to evaluating the Reconsideration Request shall be communicated to the party seeking reconsideration, who shall then have the option of withdrawing the request or agreeing to bear such costs.

5. All Reconsideration Requests must be submitted to an e-mail address designated by the Board's Reconsideration Committee within thirty days after:

a. for requests challenging Board actions, the date on which information about the challenged Board action is first published in a preliminary report or minutes of the Board's meetings; or

b. for requests challenging staff actions, the date on which the party submitting the request became aware of, or reasonably should have become aware of, the challenged staff action; or

c. for requests challenging either Board or staff inaction, the date on which the affected person reasonably concluded, or reasonably should have concluded, that action would not be taken in a timely manner.

6. All Reconsideration Requests must include the information required by the Reconsideration Committee, which shall include at least the following information:

a. name, address, and contact information for the requesting party, including postal and e-mail addresses;

b. the specific action or inaction of ICANN for which review or reconsideration is sought;

c. the date of the action or inaction;

d. the manner by which the requesting party will be affected by the action or inaction;

e. the extent to which, in the opinion of the party submitting the Request for Reconsideration, the action or inaction complained of adversely affects others;

f. whether a temporary stay of any action complained of is requested, and if so, the harms that will result if the action is not stayed;

g. in the case of staff action or inaction, a detailed explanation of the facts as presented to the staff and the reasons why the staff's action or inaction was inconsistent with established ICANN policy(ies);

h. in the case of Board action or inaction, a detailed explanation of the material information not considered by the Board and, if the information was not presented to the Board, the reasons the party submitting the request did not submit it to the Board before it acted or failed to act;

i. what specific steps the requesting party asks ICANN to take-i.e., whether and how the action should be reversed, cancelled, or modified, or what specific action should be taken;

j. the grounds on which the requested action should be taken; and

k. any documents the requesting party wishes to submit in support of its request.

7. All Reconsideration Requests shall be posted on the Website.

8. The Reconsideration Committee shall have authority to consider Reconsideration Requests from different parties in the same proceeding so long as (i) the requests involve the same general action or inaction and (ii) the parties submitting Reconsideration Requests are similarly affected by such action or inaction.

9. The Reconsideration Committee shall review Reconsideration Requests promptly upon receipt and announce, within thirty days, its intention to either decline to consider or proceed to consider a Reconsideration Request after receipt of the Request. The announcement shall be posted on the Website.

10. The Reconsideration Committee announcement of a decision not to hear a Reconsideration Request must contain an explanation of the reasons for its decision.

11. The Reconsideration Committee may request additional information or clarifications from the party submitting the Request for Reconsideration.

12. The Reconsideration Committee may ask the ICANN staff for its views on the matter, which comments shall be made publicly available on the Website.

13. If the Reconsideration Committee requires additional information, it may elect to conduct a meeting with the party seeking Reconsideration by telephone, e-mail or, if acceptable to the party requesting reconsideration, in person. To the extent any information gathered in such a meeting is relevant to any recommendation by the Reconsideration Committee, it shall so state in its recommendation.

14. The Reconsideration Committee may also request information relevant to the request from third parties. To the extent any information gathered is relevant to any recommendation by the Reconsideration Committee, it shall so state in its recommendation.

15. The Reconsideration Committee shall act on a Reconsideration Request on the basis of the public written record, including information submitted by the party seeking reconsideration or review, by the ICANN staff, and by any third party.

16. To protect against abuse of the reconsideration process, a request for reconsideration may be dismissed by the Reconsideration Committee where it is repetitive, frivolous, non-substantive, or otherwise abusive, or where the affected party had notice and opportunity to, but did not, participate in the public comment period relating to the contested action, if applicable. Likewise, the Reconsideration Committee may dismiss a request when the requesting party does not show that it will be affected by ICANN's action.

17. The Reconsideration Committee shall make a final recommendation to the Board with respect to a Reconsideration Request within ninety days following its receipt of the request, unless impractical, in which case it shall report to the Board the circumstances that prevented it from making a final recommendation and its best estimate of the time required to produce such a final recommendation. The final recommendation shall be posted on the Website.

18. The Board shall not be bound to follow the recommendations of the Reconsideration Committee. The final decision of the Board shall be made public as part of the preliminary report and minutes of the Board meeting at which action is taken.

19. The Reconsideration Committee shall submit a report to the Board on an annual basis containing at least the following information for the preceding calendar year:

a. the number and general nature of Reconsideration Requests received;

b. the number of Reconsideration Requests on which the Committee has taken action;

c. the number of Reconsideration Requests that remained pending at the end of the calendar year and the average length of time for which such Reconsideration Requests have been pending;

d. a description of any Reconsideration Requests that were pending at the end of the calendar year for more than ninety (90) days and the reasons that the Committee has not taken action on them;

e. the number and nature of Reconsideration Requests that the Committee declined to consider on the basis that they did not meet the criteria established in this policy;

f. for Reconsideration Requests that were denied, an explanation of any other mechanisms available to ensure that ICANN is accountable to persons materially affected by its decisions; and

g. whether or not, in the Committee's view, the criteria for which reconsideration may be requested should be revised, or another process should be adopted or modified, to ensure that all persons materially affected by ICANN decisions have meaningful access to a review process that ensures fairness while limiting frivolous claims.

20. Each annual report shall also aggregate the information on the topics listed in paragraph 19(a)-(e) of this Section for the period beginning 1 January 2003.

Section 3. INDEPENDENT REVIEW OF BOARD ACTIONS

1. In addition to the reconsideration process described in Section 2 of this Article, ICANN shall have in place a separate process for independent third-party review of Board actions alleged by an affected party to be inconsistent with the Articles of Incorporation or Bylaws.

2. Any person materially affected by a decision or action by the Board that he or she asserts is inconsistent with the Articles of Incorporation or Bylaws may submit a request for independent review of that decision or action.

3. Requests for such independent review shall be referred to an Independent Review Panel ("IRP"), which shall be charged with comparing contested actions of the Board to the Articles of

Incorporation and Bylaws, and with declaring whether the Board has acted consistently with the provisions of those Articles of Incorporation and Bylaws.

4. The IRP shall be operated by an international arbitration provider appointed from time to time by ICANN ("the IRP Provider") using arbitrators under contract with or nominated by that provider.

5. Subject to the approval of the Board, the IRP Provider shall establish operating rules and procedures, which shall implement and be consistent with this Section 3.

6. Either party may elect that the request for independent review be considered by a three-member panel; in the absence of any such election, the issue shall be considered by a one-member panel.

7. The IRP Provider shall determine a procedure for assigning members to individual panels; provided that if ICANN so directs, the IRP Provider shall establish a standing panel to hear such claims.

8. The IRP shall have the authority to:

a. request additional written submissions from the party seeking review, the Board, the Supporting Organizations, or from other parties;

b. declare whether an action or inaction of the Board was inconsistent with the Articles of Incorporation or Bylaws; and

c. recommend that the Board stay any action or decision, or that the Board take any interim action, until such time as the Board reviews and acts upon the opinion of the IRP.

9. Individuals holding an official position or office within the ICANN structure are not eligible to serve on the IRP.

10. In order to keep the costs and burdens of independent review as low as possible, the IRP should conduct its proceedings by e-mail and otherwise via the Internet to the maximum extent feasible. Where necessary, the IRP may hold meetings by telephone.

11. The IRP shall adhere to conflicts-of-interest policy stated in the IRP Provider's operating rules and procedures, as approved by the Board.

12. Declarations of the IRP shall be in writing. The IRP shall make its declaration based solely on the documentation, supporting materials, and arguments submitted by the parties, and in its declaration shall specifically designate the prevailing party. The party not prevailing shall ordinarily be responsible for bearing all costs of the IRP Provider, but in an extraordinary case the IRP may in its declaration

allocate up to half of the costs of the IRP Provider to the prevailing party based upon the circumstances, including a consideration of the reasonableness of the parties' positions and their contribution to the public interest. Each party to the IRP proceedings shall bear its own expenses.

13. The IRP operating procedures, and all petitions, claims, and declarations, shall be posted on the Website when they become available.

14. The IRP may, in its discretion, grant a party's request to keep certain information confidential, such as trade secrets.

15. Where feasible, the Board shall consider the IRP declaration at the Board's next meeting.

Section 4. PERIODIC REVIEW OF ICANN STRUCTURE AND OPERATIONS

The Board shall cause a periodic review, if feasible no less frequently than every three years, of the performance and operation of each Supporting Organization, Supporting Organization Council, Advisory Committee (other than the Governmental Advisory Committee) and Nominating Committee by an entity or entities independent of the organization under review. The goal of the review, to be undertaken pursuant to such criteria and standards as the Board shall direct, shall be to determine (i) whether that organization has a continuing purpose in the ICANN structure, and (ii) if so, whether any change in structure or operations is desirable to improve its effectiveness. The results of such reviews shall be posted on the Website for public review and comment, and shall be considered by the Board no later than the second scheduled meeting of the Board after such results have been posted for 30 days. The first such reviews, to be initiated within one year following the adoption of these Bylaws, shall be of the GNSO Names Council and the ICANN Root Server System Advisory Committee. The Governmental Advisory Committee shall provide its own review mechanisms.

ARTICLE V: OMBUDSMAN

Section 1. OFFICE OF OMBUDSMAN

1. There shall be an Office of Ombudsman, to be managed by an Ombudsman and to include such staff support as the Board determines is appropriate and feasible. The Ombudsman shall be a full-time position, with salary and benefits appropriate to the function, as determined by the Board.

2. The Ombudsman shall be appointed by the Board for an initial term of two years, subject to renewal by the Board.

3. The Ombudsman shall be subject to dismissal by the Board only upon a three-fourths (3/4) vote of the entire Board.

4. The annual budget for the Office of Ombudsman shall be established by the Board as part of the annual ICANN budget process. The Ombudsman shall submit a proposed budget to the

President, and the President shall include that budget submission in its entirety and without change in the general ICANN budget recommended by the ICANN President to the Board. Nothing in this Article shall prevent the President from offering separate views on the substance, size, or other features of the Ombudsman's proposed budget to the Board.

Section 2. CHARTER

The charter of the Ombudsman shall be to act as a neutral dispute resolution practitioner for those matters for which the provisions of the Reconsideration Policy set forth in Section 2 of Article IV or the Independent Review Policy set forth in Section 3 of Article IV have not been invoked. The principal function of the Ombudsman shall be to provide an independent internal evaluation of complaints by members of the ICANN community who believe that the ICANN staff, Board or an ICANN constituent body has treated them unfairly. The Ombudsman shall serve as an objective advocate for fairness, and shall seek to evaluate and where possible resolve complaints about unfair or inappropriate treatment by ICANN staff, the Board, or ICANN constituent bodies, clarifying the issues and using conflict resolution tools such as negotiation, facilitation, and "shuttle diplomacy" to achieve these results.

Section 3. OPERATIONS

The Office of Ombudsman shall:

1. facilitate the fair, impartial, and timely resolution of problems and complaints that affected members of the ICANN community (excluding employees and vendors/suppliers of ICANN) may have with specific actions or failures to act by the Board or ICANN staff which have not otherwise become the subject of either the Reconsideration or Independent Review Policies;

2. exercise discretion to accept or decline to act on a complaint or question, including by the development of procedures to dispose of complaints that are insufficiently concrete, substantive, or related to ICANN's interactions with the community so as to be inappropriate subject matters for the Ombudsman to act on. In addition, and without limiting the foregoing, the Ombudsman shall have no authority to act in any way with respect to internal administrative matters, personnel matters, issues relating to membership on the Board, or issues related to vendor/supplier relations;

3. have the right to have access to (but not to publish if otherwise confidential) all necessary information and records from ICANN staff and constituent bodies to enable an informed evaluation of the complaint and to assist in dispute resolution where feasible (subject only to such confidentiality obligations as are imposed by the complainant or any generally applicable confidentiality policies adopted by ICANN);

4. heighten awareness of the Ombudsman program and functions through routine interaction with the ICANN community and online availability;

5. maintain neutrality and independence, and have no bias or personal stake in an outcome; and

6. comply with all ICANN conflicts-of-interest and confidentiality policies.

Section 4. INTERACTION WITH ICANN AND OUTSIDE ENTITIES

1. No ICANN employee, Board member, or other participant in Supporting Organizations or Advisory Committees shall prevent or impede the Ombudsman's contact with the ICANN community (including employees of ICANN). ICANN employees and Board members shall direct members of the ICANN community who voice problems, concerns, or complaints about ICANN to the Ombudsman, who shall advise complainants about the various options available for review of such problems, concerns, or complaints.

2. ICANN staff and other ICANN participants shall observe and respect determinations made by the Office of Ombudsman concerning confidentiality of any complaints received by that Office.

3. Contact with the Ombudsman shall not constitute notice to ICANN of any particular action or cause of action.

4. The Ombudsman shall be specifically authorized to make such reports to the Board as he or she deems appropriate with respect to any particular matter and its resolution or the inability to resolve it. Absent a determination by the Ombudsman, in his or her sole discretion, that it would be inappropriate, such reports shall be posted on the Website.

5. The Ombudsman shall not take any actions not authorized in these Bylaws, and in particular shall not institute, join, or support in any way any legal actions challenging ICANN structure, procedures, processes, or any conduct by the ICANN Board, staff, or constituent bodies.

Section 5. ANNUAL REPORT

The Office of Ombudsman shall publish on an annual basis a consolidated analysis of the year's complaints and resolutions, appropriately dealing with confidentiality obligations and concerns. Such annual report should include a description of any trends or common elements of complaints received during the period in question, as well as recommendations for steps that could be taken to minimize future complaints. The annual report shall be posted on the Website.

ARTICLE VI: BOARD OF DIRECTORS

Section 1. COMPOSITION OF THE BOARD

The ICANN Board of Directors ("Board") shall consist of fifteen voting members ("Directors"). In addition, six non-voting liaisons ("Liaisons") shall be designated for the purposes set forth in Section 9 of this Article. Only Directors shall be included in determining the existence of quorums, and in establishing the validity of votes taken by the ICANN Board.

Section 2. DIRECTORS AND THEIR SELECTION; ELECTION OF CHAIRMAN AND VICE-CHAIRMAN

1. The Directors shall consist of:

a. Eight voting members selected by the Nominating Committee established by Article VII of these Bylaws. These seats on the Board of Directors are referred to in these Bylaws as Seats 1 through 8.

b. Two voting members selected by the Address Supporting Organization according to the provisions of Article VIII of these Bylaws. These seats on the Board of Directors are referred to in these Bylaws as Seat 9 and Seat 10.

c. Two voting members selected by the Country-Code Names Supporting Organization according to the provisions of Article IX of these Bylaws. These seats on the Board of Directors are referred to in these Bylaws as Seat 11 and Seat 12.

d. Two voting members selected by the Generic Names Supporting Organization according to the provisions of Article X of these Bylaws. These seats on the Board of Directors are referred to in these Bylaws as Seat 13 and Seat 14.

e. The President ex officio, who shall be a voting member.

2. In carrying out its responsibilities to fill Seats 1 through 8, the Nominating Committee shall seek to ensure that the ICANN Board is composed of members who in the aggregate display diversity in geography, culture, skills, experience, and perspective, by applying the criteria set forth in Section 3 of this Article. At no time shall the Nominating Committee select a Director to fill any vacancy or expired term whose selection would cause the total number of Directors (not including the President) who are citizens of countries in any one Geographic Region (as defined in Section 5 of this Article) to exceed five; and the Nominating Committee shall ensure through its selections that at all times the Board includes at least one Director who is a citizen of a country in each ICANN Geographic Region.

3. In carrying out their responsibilities to fill Seats 9 through 14, the Supporting Organizations shall seek to ensure that the ICANN Board is composed of members that in the aggregate display diversity in geography, culture, skills, experience, and perspective, by applying

the criteria set forth in Section 3 of this Article. At any given time, no two Directors selected by a Supporting Organization shall be citizens of the same country or of countries located in the same Geographic Region.

4. The Board shall annually elect a Chairman and a Vice-Chairman from among the Directors, not including the President.

Section 3. CRITERIA FOR SELECTION OF DIRECTORS

ICANN Directors shall be:

1. Accomplished persons of integrity, objectivity, and intelligence, with reputations for sound judgment and open minds, and a demonstrated capacity for thoughtful group decision-making;

2. Persons with an understanding of ICANN's mission and the potential impact of ICANN decisions on the global Internet community, and committed to the success of ICANN;

3. Persons who will produce the broadest cultural and geographic diversity on the Board consistent with meeting the other criteria set forth in this Section;

4. Persons who, in the aggregate, have personal familiarity with the operation of gTLD registries and registrars; with ccTLD registries; with IP address registries; with Internet technical standards and protocols; with policy-development procedures, legal traditions, and the public interest; and with the broad range of business, individual, academic, and non-commercial users of the Internet;

5. Persons who are willing to serve as volunteers, without compensation other than the reimbursement of certain expenses; and

6. Persons who are able to work and communicate in written and spoken English.

Section 4. ADDITIONAL QUALIFICATIONS

Notwithstanding anything herein to the contrary, no official of a national government or a multinational entity established by treaty or other agreement between national governments may serve as a Director. As used herein, the term "official" means a person (i) who holds an elective governmental office or (ii) who is employed by such government or multinational entity and whose primary function with such government or entity is to develop or influence governmental or public policies.

Section 5. INTERNATIONAL REPRESENTATION

In order to ensure broad international representation on the Board, the selection of Directors by the Nominating Committee and each Supporting Organization shall comply with all applicable diversity provisions of these Bylaws or of any Memorandum of Understanding referred to in these Bylaws concerning the

Supporting Organization. One intent of these diversity provisions is to ensure that at all times each Geographic Region shall have at least one Director, and at all times no region shall have more than five Directors on the Board (not including the President). As used in these Bylaws, each of the following is considered to be a "Geographic Region": Europe; Asia/Australia/Pacific; Latin America/Caribbean islands; Africa; and North America. The specific countries included in each Geographic Region shall be determined by the Board, and this Section shall be reviewed by the Board from time to time (but at least every three years) to determine whether any change is appropriate, taking account of the evolution of the Internet.

Section 6. DIRECTORS' CONFLICTS OF INTEREST

The Board, through a committee designated for that purpose, shall require a statement from each Director not less frequently than once a year setting forth all business and other affiliations which relate in any way to the business and other affiliations of ICANN. Each Director shall be responsible for disclosing to ICANN any matter that could reasonably be considered to make such Director an "interested director" within the meaning of Section 5233 of the California Nonprofit Public Benefit Corporation Law ("CNPBCL"). In addition, each Director shall disclose to ICANN any relationship or other factor that could reasonably be considered to cause the Director to be considered to be an "interested person" within the meaning of Section 5227 of the CNPBCL. The Board shall adopt policies specifically addressing Director, Officer, and Supporting Organization conflicts of interest. No Director shall vote on any matter in which he or she has a material and direct financial interest that would be affected by the outcome of the vote.

Section 7. DUTIES OF DIRECTORS

Directors shall serve as individuals who have the duty to act in what they reasonably believe are the best interests of ICANN and not as representatives of the entity that selected them, their employers, or any other organizations or constituencies.

Section 8. TERMS OF DIRECTORS

1. Subject to the provisions of the Transition Article of these Bylaws, the regular term of office of Director Seats 1 through 14 shall begin as follows:

a. The regular terms of Seats 1 through 3 shall begin at the conclusion of ICANN's annual meeting in 2003 and each ICANN meeting every third year after 2003;

b. The regular terms of Seats 4 through 6 shall begin at the conclusion of ICANN's annual meeting in 2004 and each ICANN meeting every third year after 2004;

c. The regular terms of Seats 7 and 8 shall begin at the conclusion of ICANN's annual meeting in 2005 and each ICANN meeting every third year after 2005;

d. The regular terms of Seats 9 and 12 shall begin on the day six months after the conclusion of ICANN's annual meeting in 2002 and each ICANN meeting every third year after 2002;

e. The regular terms of Seats 10 and 13 shall begin on the day six months after the conclusion of ICANN's annual meeting in 2003 and each ICANN meeting every third year after 2003; and

f. The regular terms of Seats 11 and 14 shall begin on the day six months after the conclusion of ICANN's annual meeting in 2004 and each ICANN meeting every third year after 2004.

2. Each Director holding any of Seats 1 through 14, including a Director selected to fill a vacancy, shall hold office for a term that lasts until the next term for that Seat commences and until a successor has been selected and qualified or until that Director resigns or is removed in accordance with these Bylaws.

3. At least one month before the commencement of each annual meeting, the Nominating Committee shall give the Secretary of ICANN written notice of its selection of Directors for seats with terms beginning at the conclusion of the annual meeting.

4. No later than five months after the conclusion of each annual meeting, any Supporting Organization entitled to select a Director for a Seat with a term beginning on the day six months after the conclusion of the annual meeting shall give the Secretary of ICANN written notice of its selection.

5. No Director may serve more than three consecutive terms.

6. The term as Director of the person holding the office of President shall be for as long as, and only for as long as, such person holds the office of President.

Section 9. NON-VOTING LIAISONS

1. The non-voting liaisons shall include:

a. One appointed by the Governmental Advisory Committee;

b. One appointed by the Root Server System Advisory Committee established by Article XI of these Bylaws;

c. One appointed by the Security and Stability Advisory Committee established by Article XI of these Bylaws;

d. One appointed by the Technical Liaison Group established by Article XI-A of these Bylaws;

e. One appointed by the At-Large Advisory Committee established by Article XI of these Bylaws; and

f. One appointed by the Internet Engineering Task Force.

2. Subject to the provisions of the Transition Article of these Bylaws, the non-voting liaisons shall serve terms that begin at the conclusion of each annual meeting. At least one month before the commencement of each annual meeting, each body entitled to appoint a non-voting liaison shall give the Secretary of ICANN written notice of its appointment.

3. Non-voting liaisons shall serve as volunteers, without compensation other than the reimbursement of certain expenses.

4. Each non-voting liaison may be reappointed, and shall remain in that position until a successor has been appointed or until the liaison resigns or is removed in accordance with these Bylaws.

5. The non-voting liaisons shall be entitled to attend Board meetings, participate in Board discussions and deliberations, and have access (under conditions established by the Board) to materials provided to Directors for use in Board discussions, deliberations and meetings, but shall otherwise not have any of the rights and privileges of Directors. Non-voting liaisons shall be entitled (under conditions established by the Board) to use any materials provided to them pursuant to this Section for the purpose of consulting with their respective committee or organization.

Section 10. RESIGNATION OF A DIRECTOR OR NON-VOTING LIAISON

Subject to Section 5226 of the CNPBCL, any Director or non-voting liaison may resign at any time, either by oral tender of resignation at any meeting of the Board (followed by prompt written notice to the Secretary of ICANN) or by giving written notice thereof to the President or the Secretary of ICANN. Such resignation shall take effect at the time specified, and, unless otherwise specified, the acceptance of such resignation shall not be necessary to make it effective. The successor shall be selected pursuant to Section 12 of this Article.

Section 11. REMOVAL OF A DIRECTOR OR NON-VOTING LIAISON

1. Any Director may be removed, following notice to that Director and, if selected by a Supporting Organization, to that Supporting Organization, by a three-fourths (3/4) majority vote of all Directors; provided, however, that the Director who is the subject of the removal action shall not be entitled to vote on such an action or be counted as a voting member of the Board when calculating the required three-fourths (3/4) vote; and provided further, that each vote to remove a Director shall be a separate vote on the sole question of the removal of that particular Director.

2. With the exception of the non-voting liaison appointed by the Governmental Advisory Committee, any non-voting liaison may be

removed, following notice to that liaison and to the organization by which that liaison was selected, by a three-fourths (3/4) majority vote of all Directors if the selecting organization fails to promptly remove that liaison following such notice. The Board may request the Governmental Advisory Committee to consider the replacement of the non-voting liaison appointed by that Committee if the Board, by a three-fourths (3/4) majority vote of all Directors, determines that such an action is appropriate.

Section 12. VACANCIES

1. A vacancy or vacancies in the Board of Directors shall be deemed to exist in the case of the death, resignation, or removal of any Director; if the authorized number of Directors is increased; or if a Director has been declared of unsound mind by a final order of court or convicted of a felony or incarcerated for more than 90 days as a result of a criminal conviction or has been found by final order or judgment of any court to have breached a duty under Sections 5230 et seq. of the CNPBCL. Any vacancy occurring on the Board of Directors shall be filled by the Nominating Committee, unless (a) that Director was selected by a Supporting Organization, in which case that vacancy shall be filled by that Supporting Organization, or (b) that Director was the President, in which case the vacancy shall be filled in accordance with the provisions of Article XIII of these Bylaws. The selecting body shall give written notice to the Secretary of ICANN of their appointments to fill vacancies. A Director selected to fill a vacancy on the Board shall serve for the unexpired term of his or her predecessor in office and until a successor has been selected and qualified. No reduction of the authorized number of Directors shall have the effect of removing a Director prior to the expiration of the Director's term of office.

2. The organizations selecting the non-voting liaisons identified in Section 9 of this Article are responsible for determining the existence of, and filling, any vacancies in those positions. They shall give the Secretary of ICANN written notice of their appointments to fill vacancies.

Section 13. ANNUAL MEETINGS

Annual meetings of ICANN shall be held for the purpose of electing Officers and for the transaction of such other business as may come before the meeting. Each annual meeting shall be held during the fourth quarter of the calendar year. The annual meeting shall be held at the principal office of ICANN. The annual meeting shall be open to the public. If the Board determines that it is practical, the annual meeting should be distributed in real-time and archived video and audio formats on the Internet.

Section 14. REGULAR MEETINGS

Regular meetings of the Board shall be held on dates to be determined by the Board. In the absence of other designation, regular meetings shall be held at the principal office of ICANN.

Section 15. SPECIAL MEETINGS

Special meetings of the Board may be called by or at the request of one-quarter (1/4) of the members of the Board or by the Chairman of the Board or the President. A call for a special meeting shall be made by the Secretary of ICANN. In the absence of designation, special meetings shall be held at the principal office of ICANN.

Section 16. NOTICE OF MEETINGS

Notice of time and place of all meetings shall be delivered personally or by telephone or by electronic mail to each Director and non-voting liaison, or sent by first-class mail (air mail for addresses outside the United States) or facsimile, charges prepaid, addressed to each Director and non-voting liaison at the Director's or non-voting liaison's address as it is shown on the records of ICANN. In case the notice is mailed, it shall be deposited in the United States mail at least fourteen (14) days before the time of the holding of the meeting. In case the notice is delivered personally or by telephone or facsimile or electronic mail it shall be delivered personally or by telephone or facsimile or electronic mail at least forty-eight (48) hours before the time of the holding of the meeting. Notwithstanding anything in this Section to the contrary, notice of a meeting need not be given to any Director who signed a waiver of notice or a written consent to holding the meeting or an approval of the minutes thereof, whether before or after the meeting, or who attends the meeting without protesting, prior thereto or at its commencement, the lack of notice to such Director. All such waivers, consents and approvals shall be filed with the corporate records or made a part of the minutes of the meetings.

Section 17. QUORUM

At all annual, regular, and special meetings of the Board, a majority of the total number of Directors then in office shall constitute a quorum for the transaction of business, and the act of a majority of the Directors present at any meeting at which there is a quorum shall be the act of the Board, unless otherwise provided herein or by law. If a quorum shall not be present at any meeting of the Board, the Directors present thereat may adjourn the meeting from time to time to another place, time, or date. If the meeting is adjourned for more than twenty-four (24) hours, notice shall be given to those Directors not at the meeting at the time of the adjournment.

Section 18. ACTION BY TELEPHONE MEETING OR BY OTHER COMMUNICATIONS EQUIPMENT

Members of the Board or any Committee of the Board may participate in a meeting of the Board or Committee of the Board through use of (i) conference telephone or similar communications equipment, provided that all Directors participating in such a meeting can speak to and hear one another or (ii) electronic video screen communication or other communication equipment; provided that (a) all Directors participating in such a meeting can speak to and hear one another, (b) all Directors are provided the means of fully participating in all matters before the Board or Committee of the Board, and (c) ICANN adopts and implements means of verifying that (x) a person participating in such a meeting is a Director or other person entitled to participate in the meeting and (y)

all actions of, or votes by, the Board or Committee of the Board are taken or cast only by the members of the Board or Committee and not persons who are not members. Participation in a meeting pursuant to this Section constitutes presence in person at such meeting. ICANN shall make available at the place of any meeting of the Board the telecommunications equipment necessary to permit members of the Board to participate by telephone.

Section 19. ACTION WITHOUT MEETING

Any action required or permitted to be taken by the Board or a Committee of the Board may be taken without a meeting if all of the Directors entitled to vote thereat shall individually or collectively consent in writing to such action. Such written consent shall have the same force and effect as the unanimous vote of such Directors. Such written consent or consents shall be filed with the minutes of the proceedings of the Board.

Section 20. ELECTRONIC MAIL

If permitted under applicable law, communication by electronic mail shall be considered equivalent to any communication otherwise required to be in writing. ICANN shall take such steps as it deems appropriate under the circumstances to assure itself that communications by electronic mail are authentic.

Section 21. RIGHTS OF INSPECTION

Every Director shall have the right at any reasonable time to inspect and copy all books, records and documents of every kind, and to inspect the physical properties of ICANN. ICANN shall establish reasonable procedures to protect against the inappropriate disclosure of confidential information.

Section 22. COMPENSATION

The Directors shall receive no compensation for their services as Directors. The Board may, however, authorize the reimbursement of actual and necessary reasonable expenses incurred by Directors and non-voting liaisons performing their duties as Directors or non-voting liaisons.

Section 23. PRESUMPTION OF ASSENT

A Director present at a Board meeting at which action on any corporate matter is taken shall be presumed to have assented to the action taken unless his or her dissent or abstention is entered in the minutes of the meeting, or unless such Director files a written dissent or abstention to such action with the person acting as the secretary of the meeting before the adjournment thereof, or forwards such dissent or abstention by registered mail to the Secretary of ICANN immediately after the adjournment of the meeting. Such right to dissent or abstain shall not apply to a Director who voted in favor of such action.

ARTICLE VII: NOMINATING COMMITTEE

Section 1. DESCRIPTION

There shall be a Nominating Committee of ICANN, responsible for the selection of all ICANN Directors except the President and those Directors selected by ICANN's Supporting Organizations, and for such other selections as are set forth in these Bylaws.

Section 2. COMPOSITION

The Nominating Committee shall be composed of the following delegates:

1. A non-voting Chair, appointed by the ICANN Board;

2. The immediately previous Nominating Committee Chair, as a non-voting advisor;

3. A non-voting liaison appointed by the ICANN Root Server System Advisory Committee established by Article XI of these Bylaws;

4. A non-voting liaison appointed by the ICANN Security and Stability Advisory Committee established by Article XI of these Bylaws;

5. A non-voting liaison appointed by the Governmental Advisory Committee;

6. Subject to the provisions of the Transition Article of these Bylaws, five voting delegates selected by the At-Large Advisory Committee established by Article XI of these Bylaws;

7. Two voting delegates, one representing small business users and one representing large business users, selected by the Business Users Constituency of the Generic Names Supporting Organization established by Article X of these Bylaws; and

8. One voting delegate each selected by the following entities:

   a. The gTLD Registry Constituency of the Generic Names Supporting Organization established by Article X of these Bylaws;

   b. The gTLD Registrars Constituency of the Generic Names Supporting Organization established by Article X of these Bylaws;

   c. The Council of the Country Code Names Supporting Organization established by Article IX of these Bylaws;

   d. The Internet Service Providers Constituency of the Generic Names Supporting Organization established by Article X of these Bylaws;

   e. The Intellectual Property Constituency of the Generic Names Supporting Organization established by Article X of these Bylaws;

f. The Council of the Address Supporting Organization established by Article VIII of these Bylaws;

g. An entity designated by the Board to represent academic and similar organizations;

h. Consumer and civil society groups, selected by the Non-commercial Users Constituency of the Generic Names Supporting Organization established by Article X of these Bylaws;

i. The Internet Engineering Task Force; and

j. The ICANN Technical Liaison Group established by Article XI-A of these Bylaws.

Section 3. TERMS

Subject to the provisions of the Transition Article of these Bylaws:

1. Each voting delegate shall serve a one-year term. A delegate may serve at most two successive one-year terms, after which at least two years must elapse before the individual is eligible to serve another term.

2. The regular term of each voting delegate shall begin at the conclusion of an ICANN annual meeting and shall end at the conclusion of the immediately following ICANN annual meeting.

3. Non-voting liaisons shall serve during the term designated by the entity that appoints them.

4. Vacancies on the Nominating Committee shall be filled by the entity entitled to select the delegate, non-voting liaison, or Chair involved.

5. The existence of any vacancies shall not affect the obligation of the Nominating Committee to carry out the responsibilities assigned to it in these Bylaws.

Section 4. CRITERIA FOR SELECTION OF NOMINATING COMMITTEE DELEGATES

Delegates to the ICANN Nominating Committee shall be:

1. Accomplished persons of integrity, objectivity, and intelligence, with reputations for sound judgment and open minds, and with experience and competence with collegial large group decision-making;

2. Persons with wide contacts, broad experience in the Internet community, and a commitment to the success of ICANN;

3. Persons whom the selecting body is confident will consult widely and accept input in carrying out their responsibilities;

4. Persons who are neutral and objective, without any fixed personal commitments to particular individuals, organizations, or commercial objectives in carrying out their Nominating Committee responsibilities;

5. Persons with an understanding of ICANN's mission and the potential impact of ICANN's activities on the broader Internet community who are willing to serve as volunteers, without compensation other than the reimbursement of certain expenses; and

6. Persons who are able to work and communicate in written and spoken English.

Section 5. DIVERSITY

In carrying out its responsibilities to select members of the ICANN Board (and selections to any other ICANN bodies as the Nominating Committee is responsible for under these Bylaws), the Nominating Committee shall take into account the continuing membership of the ICANN Board (and such other bodies), and seek to ensure that the persons selected to fill vacancies on the ICANN Board (and each such other body) shall, to the extent feasible and consistent with the other criteria required to be applied by Section 4 of this Article, make selections guided by Core Value 4 in Article I, Section 2 .

Section 6. ADMINISTRATIVE AND OPERATIONAL SUPPORT

ICANN shall provide administrative and operational support necessary for the Nominating Committee to carry out its responsibilities.

Section 7. PROCEDURES

The Nominating Committee shall adopt such operating procedures as it deems necessary, which shall be published on the Website.

ARTICLE VIII: ADDRESS SUPPORTING ORGANIZATION [Note: This article is subject to amendment as a result of continuing discussion and the Regional Internet Registries.]

Section 1. DESCRIPTION

1. The Address Supporting Organization (ASO) shall advise the Board with respect to policy issues relating to the operation, assignment, and management of Internet addresses.

2. The ASO shall be the entity established by the Memorandum of Understanding originally entered on 18 October 1999 between ICANN and a group of regional Internet registries (RIRs), and amended in October 2000.

Section 2. ADDRESS COUNCIL

1. The ASO shall have an Address Council, consisting of representatives of the RIRs that are signatories to the Memorandum of Understanding.

2. The Address Council shall, at least annually, host a meeting (the "General Assembly") open to participation by all interested individuals.

3. The Address Council shall select Directors to those seats on the Board designated to be filled by the ASO.

ARTICLE IX: COUNTRY CODE NAMES SUPPORTING ORGANIZATION

[Note: This article is still under development within the community and is expected to be added at a later date. See Article XX, Section 4 for transition details.]

ARTICLE X: GENERIC NAMES SUPPORTING ORGANIZATION

Section 1. DESCRIPTION

There shall be a policy-development body known as the Generic Names Supporting Organization (GNSO), which shall be responsible for developing and recommending to the ICANN Board substantive policies relating to generic top-level domains.

Section 2. ORGANIZATION

The GNSO shall consist of (i) various Constituencies representing particular groups of stakeholders, as described in Section 5 of this Article and (ii) a GNSO Council responsible for managing the policy development process of the GNSO.

Section 3. GNSO COUNCIL

1. Subject to the provisions of the Transition Article of these Bylaws, the GNSO Council shall consist of two representatives selected by each of the Constituencies described in Section 5 of this Article, and three persons selected by the ICANN Nominating Committee. There may also be two liaisons to the GNSO Council, one appointed by each of the Governmental Advisory Committee and the At-Large Advisory Committee from time to time, who shall not be members of or entitled to vote on the GNSO Council, but otherwise shall be entitled to participate on equal footing with members of the GNSO Council.

2. Subject to the provisions of the Transition Article of these Bylaws: (a) the regular term of each GNSO Council member shall begin at the conclusion of an ICANN annual meeting and shall end at the conclusion of the second ICANN annual meeting thereafter; (b) the regular term of one representative selected by each Constituency shall begin in an even-numbered year and the regular term of the other representative selected by the Constituency shall begin in an odd-numbered year; and (c) the regular term of one of the three members selected by the Nominating Committee shall begin in even-numbered years and the regular term of the other two of the three members selected by the Nominating Committee shall begin in odd-numbered years. Each GNSO Council member shall hold office

during his or her regular term and until a successor has been selected and qualified or until that member resigns or is removed in accordance with these Bylaws.

3. A GNSO Council member may resign at any time by giving written notice to the ICANN Secretary. A GNSO Council member selected by a Constituency may be removed by that Constituency according to its published procedures. A GNSO Council member selected by the Nominating Committee may be removed for cause stated by a three-fourths (3/4) vote of all members of the GNSO Council (excluding the member to be removed), subject to approval by the ICANN Board. A vacancy on the GNSO Council shall be deemed to exist in the case of the death, resignation, or removal of any member. Vacancies shall be filled for the unexpired term involved by the Nominating Committee giving the ICANN Secretary written notice of its selection, unless the member holding the position before the vacancy occurred was selected by a Constituency, in which case that Constituency shall fill the unexpired term by giving the ICANN Secretary written notice of its selection.

4. The GNSO Council is responsible for managing the policy development process of the GNSO. It shall adopt such procedures as it sees fit to carry out that responsibility, provided that such procedures are approved by the Board, and further provided that, until any modifications are recommended by the GNSO Council and approved by the Board, the applicable procedures shall be as set forth in Section 6 of this Article. In addition, the GNSO Council is responsible for managing open forums, in the form of mailing lists or otherwise, for the participation of all who are willing to contribute to the work of the GNSO; such forums shall be appropriately moderated to ensure maximum focus on the business of the GNSO and to minimize non-substantive and abusive postings.

5. No more than one officer, director or employee of any particular corporation or other organization (including its subsidiaries and affiliates) shall serve on the GNSO Council at any given time.

6. The GNSO Council shall make selections to fill Seats 13 and 14 on the ICANN Board by written ballot or by action at a meeting; any such selection must have the affirmative votes of a majority of all the members of the GNSO Council. Notification of the GNSO Council's selections shall be given by the GNSO Chair in writing to the ICANN Secretary, consistent with Article VI, Sections 8(4) and 12(1).

7. The GNSO Council shall select the GNSO Chair, for a term the GNSO Council specifies but not longer than one year, by written ballot or by action at a meeting. Any such selection must have the affirmative votes of a majority of all the members of the GNSO Council.

8. Except as provided by paragraph 6 of this Section, the GNSO Council shall act at meetings. Members of the GNSO Council may

participate in a meeting of the GNSO Council through use of (i) conference telephone or similar communications equipment, provided that all members participating in such a meeting can speak to and hear one another or (ii) electronic video screen communication or other communication equipment; provided that (a) all members participating in such a meeting can speak to and hear one another, (b) all members are provided the means of fully participating in all matters before the GNSO Council, and (c) ICANN adopts and implements means of verifying that (x) a person participating in such a meeting is a member of the GNSO Council or other person entitled to participate in the meeting and (y) all actions of, or votes by, the GNSO Council are taken or cast only by the members of the GNSO Council and not persons who are not members. A majority of the total number of GNSO Council members then in office shall constitute a quorum for the transaction of business, and the act of a majority of the GNSO Council members present at any meeting at which there is a quorum shall be the act of the GNSO Council, unless otherwise provided herein. Advance notice of such meetings shall be posted on the Website, if reasonably practicable, at least 7 days in advance of the meeting. Except where determined by a majority vote of members of the GNSO Council present that a closed session is appropriate, meetings shall be open to physical or electronic attendance by all interested persons. The GNSO Council shall transmit minutes of its meetings to the ICANN Secretary, who shall cause those minutes to be posted to the Website as soon as practicable following the meeting, and no later than 21 days following the meeting.

Section 4. STAFF SUPPORT AND FUNDING

1. A member of the ICANN staff shall be assigned to support the GNSO, whose work on substantive matters shall be assigned by the Chair of the GNSO Council, and shall be designated as the GNSO Staff Manager (Staff Manager).

2. ICANN shall provide administrative and operational support necessary for the GNSO to carry out its responsibilities. Such support shall not include an obligation for ICANN to fund travel expenses incurred by GNSO participants for travel to any meeting of the GNSO or for any other purpose.

Section 5. CONSTITUENCIES

1. The following self-organized Constituencies are hereby recognized as representative of a specific and significant group of stakeholders and, subject to the provisions of the Transition Article of these Bylaws, shall each select two representatives to the GNSO Council:

a. gTLD Registries (representing all gTLD registries under contract to ICANN);

b. Registrars (representing all registrars accredited by and under contract to ICANN);

c. Internet Service and Connectivity Providers (representing all entities providing Internet service and connectivity to Internet users);

d. Commercial and Business Users (representing both large and small commercial entity users of the Internet);

e. Non-Commercial Users (representing the full range of non-commercial entity users of the Internet); and

f. Intellectual Property Interests (representing the full range of trademark and other intellectual property interests relating to the DNS).

2. The number of votes that members of the GNSO Council may cast shall be equalized so that the aggregate number of votes of representatives selected by the Constituencies (currently the gTLD Registries and Registrars) that are under contract with ICANN obligating them to implement ICANN-adopted policies is equal to the number of votes of representatives selected by other Constituencies. Initially, each member of the GNSO Council selected by the gTLD Registries Constituency or the Registrars Constituency shall be entitled to cast two votes and all other members (including those selected by the Nominating Committee) shall be entitled to cast one vote. In the event that there is a change in the Constituencies that are entitled to select voting members of the Names Council, the Board shall review the change in circumstances and by resolution revise the procedure for equalization of votes in a manner consistent with this paragraph 2.

3. Each Constituency identified in paragraph 1 of this Section shall maintain its recognition, and thus its ability to select GNSO Council representatives, only so long as it in fact represents the interests globally of the stakeholder communities it purports to represent, and shall operate to the maximum extent feasible in an open and transparent manner and consistent with procedures designed to ensure fairness. No individual or entity shall be excluded from participation in a Constituency merely because of participation in another Constituency.

4. Any group of individuals or entities may petition the Board for recognition as a new or separate Constituency. Any such petition shall contain a detailed explanation of:

a. Why the addition of such a Constituency will improve the ability of the GNSO to carry out its policy-development responsibilities; and

b. Why the proposed new Constituency would adequately represent, on a global basis, the stakeholders it seeks to represent.

Any petition for the recognition of a new Constituency shall be posted for public comment.

5. The Board may create new Constituencies in response to such a petition, or on its own motion, if it determines that such action would serve the purposes of ICANN. In the event the Board is considering acting on its own motion it shall post a detailed explanation of why such action is necessary or desirable, set a reasonable time for public comment, and not make a final decision on whether to create such new Constituency until after reviewing all comments received. Whenever the Board posts a petition or recommendation for a new Constituency for public comment, it shall notify the GNSO Council and shall consider any response to that notification prior to taking action.

Section 6. POLICY DEVELOPMENT PROCESS

Initially, the policy-development procedures to be followed by the GNSO shall be as stated in Annex A to these Bylaws. These procedures may be supplemented or revised in the manner stated in Section 3(4) of this Article.

ARTICLE XI: ADVISORY COMMITTEES

Section 1. GENERAL

The Board may create one or more Advisory Committees in addition to those set forth in this Article. Advisory Committee membership may consist of Directors only, Directors and non-directors, or non-directors only, and may also include non-voting or alternate members. Advisory Committees shall have no legal authority to act for ICANN, but shall report their findings and recommendations to the Board.

Section 2. SPECIFIC ADVISORY COMMITTEES

There shall be at least the following Advisory Committees:

1. Governmental Advisory Committee

a. The Governmental Advisory Committee should consider and provide advice on the activities of ICANN as they relate to concerns of governments, particularly matters where there may be an interaction between ICANN's policies and various laws and international agreements or where they may affect public policy issues.

b. Membership in the Governmental Advisory Committee shall be open to all national governments. Membership shall also be open to Distinct Economies as recognized in international fora, and multinational governmental organizations and treaty organizations, on the invitation of the Governmental Advisory Committee through its Chair.

c. The Governmental Advisory Committee may adopt its own charter and internal operating principles or procedures to guide its operations, to be published on the Website.

d. The chair of the Governmental Advisory Committee shall be elected by the members of the Governmental Advisory Committee pursuant to procedures adopted by such members.

e. Each member of the Governmental Advisory Committee shall appoint one accredited representative to the Committee. The accredited representative of a member must hold a formal official position with the member's public administration. The term "official" includes a holder of an elected governmental office, or a person who is employed by such government, public authority, or multinational governmental or treaty organization and whose primary function with such government, public authority, or organization is to develop or influence governmental or public policies.

f. The Governmental Advisory Committee shall annually appoint one non-voting liaison to the ICANN Board of Directors, without limitation on reappointment, and shall annually appoint one delegate to the ICANN Nominating Committee.

g. The Governmental Advisory Committee may designate a non-voting liaison to each of the Supporting Organization Councils and Advisory Committees, to the extent the Governmental Advisory Committee deems it appropriate and useful to do so.

h. The Board shall notify the Chair of the Governmental Advisory Committee in a timely manner of any proposal raising public policy issues on which it or any of ICANN's supporting organizations or advisory committees seeks public comment, and shall take duly into account any timely response to that notification prior to taking action.

i. The Governmental Advisory Committee may put issues to the Board directly, either by way of comment or prior advice, or by way of specifically recommending action or new policy development or revision to existing policies.

j. The advice of the Governmental Advisory Committee on public policy matters shall be duly taken into account, both in the formulation and adoption of policies. In the event that the ICANN Board determines to take an action that is not consistent with the Governmental Advisory Committee advice, it shall so inform the Committee and state the reasons why it decided not to follow that advice. The

Governmental Advisory Committee and the ICANN Board will then try, in good faith and in a timely and efficient manner, to find a mutually acceptable solution.

k. If no such solution can be found, the ICANN Board will state in its final decision the reasons why the Governmental Advisory Committee advice was not followed, and such statement will be without prejudice to the rights or obligations of Governmental Advisory Committee members with regard to public policy issues falling within their responsibilities.

2. Security and Stability Advisory Committee

a. The role of the Security and Stability Advisory Committee ("SAC") is to advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. It shall have the following responsibilities:

1. To develop a security framework for Internet naming and address allocation services that defines the key focus areas, and identifies where the responsibilities for each area lie. The committee shall focus on the operational considerations of critical naming infrastructure.

2. To communicate on security matters with the Internet technical community and the operators and managers of critical DNS infrastructure services, to include the root name server operator community, the top-level domain registries and registrars, the operators of the reverse delegation trees such as in-addr.arpa and ip6.arpa, and others as events and developments dictate. The Committee shall gather and articulate requirements to offer to those engaged in technical revision of the protocols related to DNS and address allocation and those engaged in operations planning.

3. To engage in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and to advise the ICANN community accordingly. The Committee shall recommend any necessary audit activity to assess the current status of DNS and address allocation security in relation to identified risks and threats.

4. To communicate with those who have direct responsibility for Internet naming and address allocation security matters (IETF, RSSAC, RIRs, name registries, etc.), to ensure that its advice on security risks, issues, and priorities is properly synchronized with existing standardization, deployment, operational, and coordination activities. The Committee shall monitor these activities and inform the ICANN community and Board on their progress, as appropriate.

5. To report periodically to the Board on its activities.

6. To make policy recommendations to the ICANN community and Board.

b. The SAC's chair and members shall be appointed by the Board.

c. The SAC shall annually appoint a non-voting liaison to the ICANN Board according to Section 9 of Article VI.

3. Root Server System Advisory Committee

a. The role of the Root Server System Advisory Committee ("RSSAC") shall be to advise the Board about the operation of the root name servers of the domain name system. The RSSAC shall consider and provide advice on the operational requirements of root name servers, including host hardware capacities, operating systems and name server software versions, network connectivity and physical environment. The RSSAC shall examine and advise on the security aspects of the root name server system. Further, the RSSAC shall review the number, location, and distribution of root name servers considering the total system performance, robustness, and reliability.

b. Membership in the RSSAC shall consist of (i) each operator of an authoritative root name server (as listed at <ftp://ftp.internic.net/domain/named.root>), and (ii) such other persons as are appointed by the ICANN Board.

c. The initial chairman of the DNS Root Server System Advisory Committee shall be appointed by the Board; subsequent chairs shall be elected by the members of the DNS Root Server System Advisory Committee pursuant to procedures adopted by the members.

d. The Root Server System Advisory Committee shall annually appoint one non-voting liaison to the ICANN

Board of Directors, without limitation on re-appointment, and shall annually appoint one non-voting liaison to the ICANN Nominating Committee.

4. At-Large Advisory Committee

a. The role of the At-Large Advisory Committee ("ALAC") shall be to consider and provide advice on the activities of ICANN, insofar as they relate to the interests of individual Internet users.

b. The ALAC shall consist of (i) two members selected by each of the Regional At-Large Organizations ("RALOs") established according to paragraph 4(g) of this Section, and (ii) five members selected by the Nominating Committee. The five members selected by the Nominating Committee shall include one citizen of a country within each of the five Geographic Regions established according to Section 5 of Article VI.

c. Subject to the provisions of the Transition Article of these Bylaws, the regular terms of members of the ALAC shall be as follows:

1. The term of one member selected by each RALO shall begin at the conclusion of an ICANN annual meeting in an even-numbered year.

2. The term of the other member selected by each RALO shall begin at the conclusion of an ICANN annual meeting in an odd-numbered year.

3. The terms of three of the members selected by the Nominating Committee shall begin at the conclusion of an annual meeting in an odd-numbered year and the terms of the other two members selected by the Nominating Committee shall begin at the conclusion of an annual meeting in an even-numbered year.

4. The regular term of each member shall end at the conclusion of the second ICANN annual meeting after the term began.

d. The Chair of the ALAC shall be elected by the members of the ALAC pursuant to procedures adopted by the Committee.

e. The ALAC shall annually appoint one non-voting liaison to the ICANN Board of Directors, without limitation on re-appointment, and shall, after consultation with each

RALO, annually appoint five voting delegates (no two of whom shall be citizens of countries in the same Geographic Region, as defined according to Section 5 of Article VI) to the Nominating Committee.

f. Subject to the provisions of the Transition Article of these Bylaws, the At-Large Advisory Committee may designate a non-voting liaison to the GNSO Council.

g. There shall be one RALO for each Geographic Region established according to Section 5 of Article VI. Each RALO shall serve as the main forum and coordination point for public input to ICANN in its Geographic Region and shall be a non-profit organization certified by ICANN according to criteria and standards established by the Board based on recommendations of the At-Large Advisory Committee. An organization shall become the recognized RALO for its Geographic Region upon entering a Memorandum of Understanding with ICANN addressing the respective roles and responsibilities of ICANN and the RALO regarding the process for selecting ALAC members and requirements of openness, participatory opportunities, transparency, accountability, and diversity in the RALO's structure and procedures, as well as criteria and standards for the RALO's constituent At-Large Structures.

h. Each RALO shall be comprised of self-supporting At-Large Structures within its Geographic Region, certified according to paragraph 4(i) of this Section, that involve individual Internet users at the local or issue level and that, in the aggregate, are open to participation by all (but only) individual Internet users who are citizens and residents of the RALO's Geographic Region (as defined in Section 5 of Article VI). If so provided by its Memorandum of Understanding with ICANN, a RALO may also have as its members individual Internet users who are citizens and residents of the RALO's Geographic Region.

i. The ALAC is responsible for certifying organizations as meeting the criteria and standards for At-Large Structures. The criteria and standards for certification of At-Large Structures within a each Geographic Region shall be established by the Board based on recommendations of the ALAC and shall be stated in the Memorandum of Understanding between ICANN and the RALO for that Geographic Region, so that each RALO is afforded the type of structure that best fits its Geographic Region's customs and characteristics. Decisions to certify or de-certify an At-Large Structure as meeting the applicable criteria and standards shall require a 2/3 vote of all the members of the ALAC and shall be subject to review

according to procedures the Board may establish. The ALAC may also give advice as to whether a prospective At-Large Structure meets the applicable criteria and standards.

j. The ALAC is also responsible, working in conjunction with the RALOs, for coordinating the following activities:

1. Keeping the community of individual Internet users informed about the significant news from ICANN;

2. Distributing (through posting or otherwise) an updated agenda, news about ICANN, and information about items in the ICANN policy-development process;

3. Promoting outreach activities in the community of individual Internet users;

4. Developing and maintaining on-going information and education programs, regarding ICANN and its work;

5 Establishing an outreach strategy about ICANN issues in each RALO's Region;

6. Making public, and analyzing, ICANN's proposed policies and its decisions and their (potential) regional impact and (potential) effect on individuals in the region;

7. Offering Internet-based mechanisms that enable discussions among members of At-Large structures; and

8. Establishing mechanisms and processes that enable two-way communication between members of At-Large Structures and those involved in ICANN decision-making, so interested individuals can share their views on pending ICANN issues.

Section 3. PROCEDURES

Each Advisory Committee shall determine its own rules of procedure and quorum requirements.

Section 4. TERM OF OFFICE

The chair and each member of a committee shall serve until his or her successor is appointed, or until such committee is sooner terminated, or until he or she is removed, resigns, or otherwise ceases to qualify as a member of the committee.

Section 5. VACANCIES

Vacancies on any committee shall be filled in the same manner as provided in the case of original appointments.

Section 6. COMPENSATION

Committee members shall receive no compensation for their services as a member of a committee. The Board may, however, authorize the reimbursement of actual and necessary expenses incurred by committee members, including Directors, performing their duties as committee members.

ARTICLE XI-A: OTHER ADVISORY MECHANISMS

Section 1. EXTERNAL EXPERT ADVICE

1. Purpose. The purpose of seeking external expert advice is to allow the policy-development process within ICANN to take advantage of existing expertise that resides in the public or private sector but outside of ICANN. In those cases where there are relevant public bodies with expertise, or where access to private expertise could be helpful, the Board and constituent bodies should be encouraged to seek advice from such expert bodies or individuals.

2. Types of Expert Advisory Panels.

a. On its own initiative or at the suggestion of any ICANN body, the Board may appoint, or authorize the President to appoint, Expert Advisory Panels consisting of public or private sector individuals or entities. If the advice sought from such Panels concerns issues of public policy, the provisions of Section 1(3)(b) of this Article shall apply.

b. In addition, in accordance with Section 1(3) of this Article, the Board may refer issues of public policy pertinent to matters within ICANN's mission to a multinational governmental or treaty organization.

3. Process for Seeking Advice-Public Policy Matters.

a. The Governmental Advisory Committee may at any time recommend that the Board seek advice concerning one or more issues of public policy from an external source, as set out above.

b. In the event that the Board determines, upon such a recommendation or otherwise, that external advice should be sought concerning one or more issues of public policy, the Board shall, as appropriate, consult with the Governmental Advisory Committee regarding the appropriate source from which to seek the advice and the arrangements, including definition of scope and process, for requesting and obtaining that advice.

c. The Board shall, as appropriate, transmit any request for advice from a multinational governmental or treaty organization, including specific terms of reference, to the Governmental Advisory Committee, with the suggestion that the request be transmitted by the Governmental Advisory Committee to the multinational governmental or treaty organization.

4. Process for Seeking and Advice-Other Matters. Any reference of issues not concerning public policy to an Expert Advisory Panel by the Board or President in accordance with Section 1(2)(a) of this Article shall be made pursuant to terms of reference describing the issues on which input and advice is sought and the procedures and schedule to be followed.

5. Receipt of Expert Advice and its Effect. External advice pursuant to this Section shall be provided in written form. Such advice is advisory and not binding, and is intended to augment the information available to the Board or other ICANN body in carrying out its responsibilities.

6. Opportunity to Comment. The Governmental Advisory Committee, in addition to the Supporting Organizations and other Advisory Committees, shall have an opportunity to comment upon any external advice received prior to any decision by the Board.

Section 2. TECHNICAL LIAISON GROUP

1. Purpose. The quality of ICANN's work depends on access to complete and authoritative information concerning the technical standards that underlie ICANN's activities. ICANN's relationship to the organizations that produce these standards is therefore particularly important. The Technical Liaison Group (TLG) shall connect the Board with appropriate sources of technical advice on specific matters pertinent to ICANN's activities.

2. TLG Organizations. The TLG shall consist of four organizations: the European Telecommunications Standards Institute (ETSI), the International Telecommunications Union's Telecommunication Standardization Sector (ITU-T), the World Wide Web Consortium (W3C), and the Internet Architecture Board (IAB).

3. Role. The role of the TLG organizations shall be to channel technical information and guidance to the Board and to other ICANN entities. This role has both a responsive component and an active "watchdog" component, which involve the following responsibilities:

a. In response to a request for information, to connect the Board or other ICANN body with appropriate sources of technical expertise. This component of the TLG role covers circumstances in which ICANN seeks an authoritative answer to a specific technical question. Where information is requested regarding a particular technical standard for which a TLG organization is

responsible, that request shall be directed to that TLG organization.

b. As an ongoing "watchdog" activity, to advise the Board of the relevance and progress of technical developments in the areas covered by each organization's scope that could affect Board decisions or other ICANN actions, and to draw attention to global technical standards issues that affect policy development within the scope of ICANN's mission. This component of the TLG role covers circumstances in which ICANN is unaware of a new development, and would therefore otherwise not realize that a question should be asked.

4. TLG Procedures. The TLG shall not have officers or hold meetings, nor shall it provide policy advice to the Board as a committee (although TLG organizations may individually be asked by the Board to do so as the need arises in areas relevant to their individual charters). Neither shall the TLG debate or otherwise coordinate technical issues across the TLG organizations; establish or attempt to establish unified positions; or create or attempt to create additional layers or structures within the TLG for the development of technical standards or for any other purpose.

5. Technical Work of the IANA. The TLG shall have no involvement with the IANA's work for the Internet Engineering Task Force, Internet Research Task Force, or the Internet Architecture Board, as described in the Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority ratified by the Board on 10 March 2000.

6. Individual Technical Experts. Each TLG organization shall designate two individual technical experts who are familiar with the technical standards issues that are relevant to ICANN's activities. These 8 experts shall be available as necessary to determine, through an exchange of e-mail messages, where to direct a technical question from ICANN when ICANN does not ask a specific TLG organization directly.

7. Board Liaison and Nominating Committee Delegate. Annually, in rotation, one TLG organization shall appoint one non-voting liaison to the Board according to Article VI, Section 9(1)(d). Annually, in rotation, one TLG organization shall select one voting delegate to the ICANN Nominating Committee according to Article VII, Section 2(8)(j). The rotation order for the appointment of the non-voting liaison to the Board shall be ETSI, ITU-T, and W3C. The rotation order for the selection of the Nominating Committee delegate shall be W3C, ETSI, and ITU-T. (IAB does not participate in these rotations because the IETF otherwise appoints a non-voting liaison to the Board and selects a delegate to the ICANN Nominating Committee.)

ARTICLE XII: BOARD AND TEMPORARY COMMITTEES

Section 1. BOARD COMMITTEES

The Board may establish one or more committees of the Board, which shall continue to exist until otherwise determined by the Board. Only Directors may be appointed to a Committee of the Board. If a person appointed to a Committee of the Board ceases to be a Director, such person shall also cease to be a member of any Committee of the Board. Each Committee of the Board shall consist of two or more Directors. The Board may designate one or more Directors as alternate members of any such committee, who may replace any absent member at any meeting of the committee. Committee members may be removed from a committee at any time by a two-thirds (2/3) majority vote of all members of the Board; provided, however, that any Director or Directors which are the subject of the removal action shall not be entitled to vote on such an action or be counted as a member of the Board when calculating the required two-thirds (2/3) vote; and, provided further, however, that in no event shall a Director be removed from a committee unless such removal is approved by not less than a majority of all members of the Board.

Section 2. POWERS OF BOARD COMMITTEES

1. The Board may delegate to Committees of the Board all legal authority of the Board except with respect to:

   a. The filling of vacancies on the Board or on any committee;

   b. The amendment or repeal of Bylaws or the Articles of Incorporation or the adoption of new Bylaws or Articles of Incorporation;

   c. The amendment or repeal of any resolution of the Board which by its express terms is not so amendable or repealable;

   d. The appointment of committees of the Board or the members thereof;

   e. The approval of any self-dealing transaction, as such transactions are defined in Section 5233(a) of the CNPBCL;

   f. The approval of the annual budget required by Article XVI; or

   g. The compensation of any officer described in Article XIII.

2. The Board shall have the power to prescribe the manner in which proceedings of any Committee of the Board shall be conducted. In the absence of any such prescription, such committee shall have the power to prescribe the manner in which its proceedings shall be conducted. Unless these Bylaws, the Board or such committee shall otherwise provide, the regular and special meetings shall be

governed by the provisions of Article VI applicable to meetings and actions of the Board. Each committee shall keep regular minutes of its proceedings and shall report the same to the Board from time to time, as the Board may require.

Section 3. TEMPORARY COMMITTEES

The Board may establish such temporary committees as it sees fit, with membership, duties, and responsibilities as set forth in the resolutions or charters adopted by the Board in establishing such committees.

ARTICLE XIII: OFFICERS

Section 1. OFFICERS

The officers of ICANN shall be a President (who shall serve as Chief Executive Officer), a Secretary, and a Chief Financial Officer. ICANN may also have, at the discretion of the Board, any additional officers that it deems appropriate. Any person, other than the President, may hold more than one office, except that no member of the Board (other than the President) shall simultaneously serve as an officer of ICANN.

Section 2. ELECTION OF OFFICERS

The officers of ICANN shall be elected annually by the Board, pursuant to the recommendation of the President or, in the case of the President, of the Chairman of the ICANN Board. Each such officer shall hold his or her office until he or she resigns, is removed, is otherwise disqualified to serve, or his or her successor is elected.

Section 3. REMOVAL OF OFFICERS

Any Officer may be removed, either with or without cause, by a two-thirds (2/3) majority vote of all the members of the Board. Should any vacancy occur in any office as a result of death, resignation, removal, disqualification, or any other cause, the Board may delegate the powers and duties of such office to any Officer or to any Director until such time as a successor for the office has been elected.

Section 4. PRESIDENT

The President shall be the Chief Executive Officer (CEO) of ICANN in charge of all of its activities and business. All other officers and staff shall report to the President or his or her delegate, unless stated otherwise in these Bylaws. The President shall serve as an ex officio member of the Board, and shall have all the same rights and privileges of any Board member. The President shall be empowered to call special meetings of the Board as set forth herein, and shall discharge all other duties as may be required by these Bylaws and from time to time may be assigned by the Board.

Section 5. SECRETARY

The Secretary shall keep or cause to be kept the minutes of the Board in one or more books provided for that purpose, shall see that all notices are duly given in accordance with the provisions of these Bylaws or as required by law, and in general shall perform all duties as from time to time may be prescribed by the President or the Board.

Section 6. CHIEF FINANCIAL OFFICER

The Chief Financial Officer ("CFO") shall be the chief financial officer of ICANN. If required by the Board, the CFO shall give a bond for the faithful discharge of his or her duties in such form and with such surety or sureties as the Board shall determine. The CFO shall have charge and custody of all the funds of ICANN and shall keep or cause to be kept, in books belonging to ICANN, full and accurate amounts of all receipts and disbursements, and shall deposit all money and other valuable effects in the name of ICANN in such depositories as may be designated for that purpose by the Board. The CFO shall disburse the funds of ICANN as may be ordered by the Board or the President and, whenever requested by them, shall deliver to the Board and the President an account of all his or her transactions as CFO and of the financial condition of ICANN. The CFO shall be responsible for ICANN's financial planning and forecasting and shall assist the President in the preparation of ICANN's annual budget. The CFO shall coordinate and oversee ICANN's funding, including any audits or other reviews of ICANN or its Supporting Organizations. The CFO shall be responsible for all other matters relating to the financial operation of ICANN.

Section 7. ADDITIONAL OFFICERS

In addition to the officers described above, any additional or assistant officers who are elected or appointed by the Board shall perform such duties as may be assigned to them by the President or the Board.

Section 8. COMPENSATION AND EXPENSES

The compensation of any Officer of ICANN shall be approved by the Board. Expenses incurred in connection with performance of their officer duties may be reimbursed to Officers upon approval of the President (in the case of Officers other than the President), by another Officer designated by the Board (in the case of the President), or the Board.

Section 9. CONFLICTS OF INTEREST

The Board, through a committee designated for that purpose, shall establish a policy requiring a statement from each Officer not less frequently than once a year setting forth all business and other affiliations which relate in any way to the business and other affiliations of ICANN.

ARTICLE XIV: INDEMNIFICATION OF DIRECTORS, OFFICERS, EMPLOYEES, AND OTHER AGENTS

ICANN shall, to maximum extent permitted by the CNPBCL, indemnify each of its agents against expenses, judgments, fines, settlements, and other amounts actually and reasonably incurred in connection with any proceeding arising by reason of the fact that any such person is or was an agent of ICANN. For

purposes of this Article, an "agent" of ICANN includes any person who is or was a Director, Officer, employee, or any other agent of ICANN, including a member of any Supporting Organization acting within the scope of his or her responsibility and on behalf of the best interests of ICANN; or is or was serving at the request of ICANN as a Director, Officer, employee, or agent of another corporation, partnership, joint venture, trust or other enterprise. The Board may adopt a resolution authorizing the purchase and maintenance of insurance on behalf of any agent of ICANN against any liability asserted against or incurred by the agent in such capacity or arising out of the agent's status as such, whether or not ICANN would have the power to indemnify the agent against that liability under the provisions of this Article.

ARTICLE XV: GENERAL PROVISIONS

Section 1. CONTRACTS

The Board may authorize any Officer or Officers, agent or agents, to enter into any contract or execute or deliver any instrument in the name of and on behalf of ICANN, and such authority may be general or confined to specific instances. In the absence of a contrary Board authorization, contracts and instruments may only be executed by the following Officers: President, any Vice President, or the CFO. Unless authorized or ratified by the Board, no other Officer, agent, or employee shall have any power or authority to bind ICANN or to render it liable for any debts or obligations.

Section 2. DEPOSITS

All funds of ICANN not otherwise employed shall be deposited from time to time to the credit of ICANN in such banks, trust companies, or other depositories as the Board, or the President under its delegation, may select.

Section 3. CHECKS

All checks, drafts, or other orders for the payment of money, notes, or other evidences of indebtedness issued in the name of ICANN shall be signed by such Officer or Officers, agent or agents, of ICANN and in such a manner as shall from time to time be determined by resolution of the Board.

Section 4. LOANS

No loans shall be made by or to ICANN and no evidences of indebtedness shall be issued in its name unless authorized by a resolution of the Board. Such authority may be general or confined to specific instances; provided, however, that no loans shall be made by ICANN to its Directors or Officers.

ARTICLE XVI: FISCAL MATTERS

Section 1. ACCOUNTING

The fiscal year end of ICANN shall be determined by the Board.

Section 2. AUDIT

At the end of the fiscal year, the books of ICANN shall be closed and audited by certified public accountants. The appointment of the fiscal auditors shall be the responsibility of the Board.

Section 3. ANNUAL REPORT AND ANNUAL STATEMENT

The Board shall publish, at least annually, a report describing its activities, including an audited financial statement and a description of any payments made by ICANN to Directors (including reimbursements of expenses). ICANN shall cause the annual report and the annual statement of certain transactions as required by the CNPBCL to be prepared and sent to each member of the Board and to such other persons as the Board may designate, no later than one hundred twenty (120) days after the close of ICANN's fiscal year.

Section 4. ANNUAL BUDGET

At least forty-five (45) days prior to the commencement of each fiscal year, the President shall prepare and submit to the Board, a proposed annual budget of ICANN for the next fiscal year, which shall be posted on the Website. The proposed budget shall identify anticipated revenue sources and levels and shall, to the extent practical, identify anticipated material expense items by line item. The Board shall adopt an annual budget and shall publish the adopted Budget on the Website.

Section 5. FEES AND CHARGES

The Board may set fees and charges for the services and benefits provided by ICANN, with the goal of fully recovering the reasonable costs of the operation of ICANN and establishing reasonable reserves for future expenses and contingencies reasonably related to the legitimate activities of ICANN. Such fees and charges shall be fair and equitable, shall be published for public comment prior to adoption, and once adopted shall be published on the Website in a sufficiently detailed manner so as to be readily accessible.

ARTICLE XVII: MEMBERS

ICANN shall not have members, as defined in the California Nonprofit Public Benefit Corporation Law ("CNPBCL"), notwithstanding the use of the term "Member" in these Bylaws, in any ICANN document, or in any action of the ICANN Board or staff.

ARTICLE XVIII: OFFICES AND SEAL

Section 1. OFFICES

The principal office for the transaction of the business of ICANN shall be in the County of Los Angeles, State of California, United States of America. ICANN may also have an additional office or offices within or outside the United States of America as it may from time to time establish.

Section 2. SEAL

The Board may adopt a corporate seal and use the same by causing it or a facsimile thereof to be impressed or affixed or reproduced or otherwise.

ARTICLE XIX: AMENDMENTS

Except as otherwise provided in the Articles of Incorporation or these Bylaws, the Articles of Incorporation or Bylaws of ICANN may be altered, amended, or repealed and new Articles of Incorporation or Bylaws adopted only upon action by a two-thirds (2/3) vote of all members of the Board.

ARTICLE XX: TRANSITION ARTICLE

Section 1. PURPOSE

This Transition Article sets forth the provisions for the transition from the processes and structures defined by the ICANN Bylaws, as amended and restated on 29 October 1999 and amended through 12 February 2002 (the "Old Bylaws"), to the processes and structures defined by the Bylaws of which this Article is a part (the "New Bylaws").

Section 2. BOARD OF DIRECTORS

1. For the period beginning on the adoption of this Transition Article and ending on the Effective Date and Time of the New Board, as defined in paragraph 5 of this Section 2, the Board of Directors of the Corporation ("Transition Board") shall consist of the members of the Board who would have been Directors under the Old Bylaws immediately after the conclusion of the annual meeting in 2002, except that those At-Large members of the Board under the Old Bylaws who elect to do so by notifying the Secretary of the Board on 15 December 2002 or in writing or by e-mail no later than 23 December 2002 shall also serve as members of the Transition Board. Notwithstanding the provisions of Article VI, Section 12 of the New Bylaws, vacancies on the Transition Board shall not be filled. The Transition Board shall not have liaisons as provided by Article VI, Section 9 of the New Bylaws. The Board Committees existing on the date of adoption of this Transition Article shall continue in existence, subject to any change in Board Committees or their membership that the Transition Board may adopt by resolution.

2. The Transition Board shall elect a Chair and Vice-Chair to serve until the Effective Date and Time of the New Board.

3. The "New Board" is that Board described in Article VI, Section 2(1) of the New Bylaws.

4. Promptly after the adoption of this Transition Article, a Nominating Committee shall be formed including, to the extent feasible, the delegates and liaisons described in Article VII, Section 2 of the New Bylaws, with terms to end at the conclusion of the ICANN annual meeting in 2003. The Nominating Committee shall proceed without delay to select Directors to fill Seats 1 through 8 on the New Board, with terms to conclude upon the commencement of the first regular

terms specified for those Seats in Article VI, Section 8(1)(a)-(c) of the New Bylaws, and shall give the ICANN Secretary written notice of that selection.

5. The Effective Date and Time of the New Board shall be a time, as designated by the Transition Board, during the first regular meeting of ICANN in 2003 that begins not less than seven calendar days after the ICANN Secretary has received written notice of the selection of Directors to fill at least ten of Seats 1 through 14 on the New Board. As of the Effective Date and Time of the New Board, it shall assume from the Transition Board all the rights, duties, and obligations of the ICANN Board of Directors. Subject to Section 4 of this Article, the Directors (Article VI, Section 2(1)(a)-(d)) and non-voting liaisons (Article VI, Section 9) as to which the ICANN Secretary has received notice of selection shall, along with the President (Article VI, Section 2(1)(e)), be seated upon the Effective Date and Time of the New Board, and thereafter any additional Directors and non-voting liaisons shall be seated upon the ICANN Secretary's receipt of notice of their selection.

6. The New Board shall elect a Chairman and Vice-Chairman as its first order of business. The terms of those Board offices shall expire at the end of the annual meeting in 2003.

7. Committees of the Board in existence as of the Effective Date and Time of the New Board shall continue in existence according to their existing charters, but the terms of all members of those committees shall conclude at the Effective Date and Time of the New Board. Temporary committees in existence as of the Effective Date and Time of the New Board shall continue in existence with their existing charters and membership, subject to any change the New Board may adopt by resolution.

Section 3. ADDRESS SUPPORTING ORGANIZATION

The Address Supporting Organization shall continue in operation according to the provisions of the Memorandum of Understanding originally entered on 18 October 1999 between ICANN and a group of regional Internet registries (RIRs), and amended in October 2000, until a replacement Memorandum of Understanding becomes effective. Promptly after the adoption of this Transition Article, the Address Supporting Organization shall make selections, and give the ICANN Secretary written notice of those selections, of:

1. Directors to fill Seats 9 and 10 on the New Board, with terms to conclude upon the commencement of the first regular terms specified for each of those Seats in Article VI, Section 8(1)(d) and (e) of the New Bylaws; and

2. the delegate to the Nominating Committee selected by the Council of the Address Supporting Organization, as called for in Article VII, Section 2(8)(f) of the New Bylaws.

With respect to the ICANN Directors that it is entitled to select, and taking into account the need for rapid selection to ensure that the New Board becomes effective as soon as possible, the Address Supporting Organization may select those Directors from among the persons it previously selected as ICANN Directors pursuant to the Old Bylaws. To the extent the Address Supporting Organization does not provide the ICANN Secretary written notice, on or before 31 March 2003, of its selections for Seat 9 and Seat 10, the Address Supporting Organization shall be deemed to have selected for Seat 9 the person it selected as an ICANN Director pursuant to the Old Bylaws for a term beginning in 2001 and for Seat 10 the person it selected as an ICANN Director pursuant to the Old Bylaws for a term beginning in 2002.

Section 4. COUNTRY-CODE NAMES SUPPORTING ORGANIZATION

Until such time as a Country-Code Names Supporting Organization is established, Seats 11 and 12 on the New Board shall remain vacant, and the delegate to the Nominating Committee established by the New Bylaws designated to be selected by such an organization shall be appointed by the Transition or New Board, depending on which is in existence at the time any particular appointment is required, after due consultation with members of the ccTLD community. Upon the organization and recognition by the ICANN Board of a Country-Code Names Supporting Organization, that Supporting Organization shall promptly select persons to fill Seats 11 and 12 on the New Board, and give written notice of those selections to the ICANN Secretary. Any delegate to the Nominating Committee appointed by the Transition or New Board according to this Section 4 then serving shall remain in office, but subsequent appointments of the Nominating Committee delegate described in Article VII, Section 2(8)(c) shall be made by the Council of the Country Code Names Supporting Organization.

Section 5. GENERIC NAMES SUPPORTING ORGANIZATION

1. The Domain Name Supporting Organization shall cease operations upon the adoption of this Transition Article, except that the Names Council of the Domain Name Supporting Organization may act for the limited purpose of authorizing the transfer of any funds it has collected to the benefit of the Generic Names Supporting Organization.

2. The Generic Names Supporting Organization ("GNSO") shall commence operations upon the adoption of this Transition Article, and the following six DNSO constituencies shall automatically become constituencies of the GNSO, initially under their existing charter:

a. The commercial and business entities constituency of the DNSO shall become the Commercial and Business Users constituency of the GNSO.

b. The gTLD registries constituency of the DNSO shall become the gTLD Registries constituency of the GNSO.

c. The ISP and connectivity providers constituency of the DNSO shall become the Internet Service and Connectivity Providers constituency of the GNSO.

d. The non-commercial domain name holders constituency of the DNSO shall become the Non-Commercial Users constituency of the GNSO.

e. The registrars constituency of the DNSO shall become the Registrars constituency of the GNSO.

f. The trademark, other intellectual property and anti-counterfeiting interests constituency of the DNSO shall become the Intellectual Property Interests constituency of the GNSO.

3. Notwithstanding the adoption or effectiveness of the New Bylaws, each GNSO constituency described in paragraph 2 of this Section 5 shall continue operating as before and no constituency official, task force, or other activity shall be changed until further action of the constituency, provided that each GNSO constituency shall submit to the ICANN Secretary a new charter and statement of operating procedures, adopted according to the constituency's processes and consistent with the New Bylaws, no later than 15 July 2003.

4. Until the conclusion of the ICANN annual meeting in 2003, the GNSO Council shall consist of three representatives of each constituency of the GNSO plus, upon their selection by the Nominating Committee, three persons selected by that committee. It may also have liaisons appointed by the Governmental Advisory Committee and (Interim) At-Large Advisory Committee, as provided in Article X, Section 3(1) of the New Bylaws. Thereafter, the composition of the GNSO Council shall be as provided in the New Bylaws, as they may be amended from time to time, without regard to this Transition Article. All committees, task forces, working groups, drafting committees, and similar groups established by the DNSO Names Council and in existence immediately before the adoption of this Transition Article shall continue in existence as groups of the GNSO Council with the same charters, membership, and activities, subject to any change by action of the GNSO Council.

5. Upon the adoption of this Transition Article, the three representatives on the Domain Name Supporting Organization ("DNSO") Names Council from each of six DNSO constituencies shall be seated as representatives of constituencies on the GNSO Council, as follows:

a. The three representatives of the commercial and business entities constituency of the DNSO shall be seated as representatives of the Commercial and Business Users constituency of the GNSO.

b. The three representatives of the gTLD registries constituency of the DNSO shall be seated as representatives of the gTLD Registries constituency of the GNSO.

c. The three representatives of the ISP and connectivity providers constituency of the DNSO shall be seated as representatives of the Internet Service and Connectivity Providers constituency of the GNSO.

d. The three representatives of the non-commercial domain name holders constituency of the DNSO shall be seated as representatives of the Non-Commercial Users constituency of the GNSO.

e. The three representatives of the registrars constituency of the DNSO shall be seated as representatives of the Registrars constituency of the GNSO.

f. The three representatives of the trademark, other intellectual property and anti-counterfeiting interests constituency of the DNSO shall be seated as representatives of the Intellectual Property Interests constituency of the GNSO.

6. The terms of the GNSO Council members described in paragraph 5 of this Section 5 shall last for the remainder of their terms under the Old Bylaws, except that all terms of GNSO Council members shall conclude at the conclusion of the ICANN annual meeting in 2003. Any vacancy occurring in a position on the GNSO Council before that time shall be filled by the constituency which the vacant position represents for the remainder of the term lasting until the conclusion of the ICANN annual meeting in 2003.

7. Promptly after the adoption of this Transition Article, the Generic Names Supporting Organization shall, through the GNSO Council, make selections of Directors to fill Seats 13 and 14 on the New Board, with terms to conclude upon the commencement of the first regular terms specified for each of those Seats in Article VI, Section 8 (1)(d) and (e) of the New Bylaws, and shall give the ICANN Secretary written notice of its selections.

8. In the absence of further action on the topic by the New Board, each of the GNSO constituencies shall select two representatives to the GNSO Council no later than 1 October 2003, and shall provide the ICANN Secretary written notice of its selections. Each constituency shall designate one of those representatives to serve a one-year term, and one to serve a two year-term. Each successor to those representatives shall serve a two-year term.

9. Upon the adoption of this Transition Article, and until further action by the ICANN Board, the GNSO Council shall assume responsibility

for the DNSO General Assembly e-mail announcement and discussion lists.

10. Each of the constituencies identified in paragraph 5 of this Section 5 that are designated to select a delegate to the Nominating Committee under Article VII, Section 2 of the New Bylaws shall promptly, upon adoption of this Transition Article, notify the ICANN Secretary of the person(s) selected to serve as delegates.

Section 6. PROTOCOL SUPPORTING ORGANIZATION

The Protocol Supporting Organization referred to in the Old Bylaws is discontinued.

Section 7. ADVISORY COMMITTEES AND TECHNICAL LIAISON GROUP

1. Upon the adoption of the New Bylaws, the Governmental Advisory Committee shall continue in operation according to its existing operating principles and practices, until further action of the committee. The Governmental Advisory Committee may designate liaisons to serve with other ICANN bodies as contemplated by the New Bylaws by providing written notice to the ICANN Secretary. Promptly upon the adoption of this Transition Article, the Governmental Advisory Committee shall notify the ICANN Secretary of the person selected as its delegate to the Nominating Committee, as set forth in Article VII, Section 2 of the New Bylaws.

2. The organizations designated as members of the Technical Liaison Group under Article XI-A, Section 2(2) of the New Bylaws shall each designate the two individual technical experts described in Article XI-A, Section 2(6) of the New Bylaws, by providing written notice to the ICANN Secretary. As soon as feasible, the delegate from the Technical Liaison Group to the Nominating Committee shall be selected according to Article XI-A, Section 2(7) of the New Bylaws.

3. Upon the adoption of the New Bylaws, the Security and Stability Advisory Committee shall continue in operation according to its existing operating principles and practices, until further action of the committee. Promptly upon the adoption of this Transition Article, the Security and Stability Advisory Committee shall notify the ICANN Secretary of the person selected as its delegate to the Nominating Committee, as set forth in Article VII, Section 2(4) of the New Bylaws.

4. Upon the adoption of the New Bylaws, the Root Server System Advisory Committee shall continue in operation according to its existing operating principles and practices, until further action of the committee. Promptly upon the adoption of this Transition Article, the Root Server Advisory Committee shall notify the ICANN Secretary of the person selected as its delegate to the Nominating Committee, as set forth in Article VII, Section 2(3) of the New Bylaws.

5. At-Large Advisory Committee

a. Until such time as ICANN recognizes, through the entry of a Memorandum of Understanding, the Regional At-Large Organizations (RALOs) identified in Article XI, Section 2(4) of the New Bylaws, there shall exist an Interim At-Large Advisory Committee composed of ten individuals (two from each ICANN region) selected by the ICANN Board following nominations by the At-Large Organizing Committee. The Nominating Committee shall select five more individuals, one from each region, as soon as feasible, to serve terms on the (Interim) At-Large Advisory Committee as specified by Article XI, Section (2)(4)(c)(3) of the New Bylaws in accordance with the principles established in Article VII, Section 5 of the New Bylaws.

b. Upon the entry of each RALO into such a Memorandum of Understanding, that entity shall be entitled to select two persons who are citizens and residents of that Region to be members of the At-Large Advisory Committee established by Article XI, Section 2(4) of the New Bylaws. Upon the entity's written notification to the ICANN Secretary of such selections, those persons shall immediately assume the seats held until that notification by the Interim At-Large Advisory Committee members previously selected by the Board from the RALO's region.

c. Upon the seating of persons selected by all five RALOs, the Interim At-Large Advisory Committee shall become the At-Large Advisory Committee, as established by Article XI, Section 2(4) of the New Bylaws. The five individuals selected to the Interim At-Large Advisory Committee by the Nominating Committee shall become members of the At-Large Advisory Committee for the remainder of the terms for which they were selected.

d. Promptly upon its creation, the Interim At-Large Advisory Committee shall notify the ICANN Secretary of the persons selected as its delegates to the Nominating Committee, as set forth in Article VII, Section 2(6) of the New Bylaws.

Section 8. OFFICERS

ICANN officers (as defined in Article XIII of the New Bylaws) shall be elected by the then-existing Board of ICANN at the annual meeting in 2002 to serve until the annual meeting in 2003.

Section 9. GROUPS APPOINTED BY THE PRESIDENT

Notwithstanding the adoption or effectiveness of the New Bylaws, task forces and other groups appointed by the ICANN President shall continue unchanged in membership, scope, and operation until changes are made by the President.

Section 10. CONTRACTS WITH ICANN

Notwithstanding the adoption or effectiveness of the New Bylaws, all agreements, including employment and consulting agreements, entered by ICANN shall continue in effect according to their terms.

Annex A: GNSO Policy Development Process

The following process shall govern the GNSO policy development process ("PDP") until such time as modifications are recommended to and approved by the ICANN Board of Directors ("Board").

1. Raising an Issue

An issue may be raised for consideration as part of the PDP by any of the following:

a. *Board Initiation.* The Board may initiate the PDP by instructing the GNSO Council ("Council") to begin the process outlined in this Annex.

b. *Council Initiation.* The GNSO Council may initiate the PDP by a vote of at least twenty-five percent (25%) of the members of the Council present at any meeting in which a motion to initiate the PDP is made.

c. *Advisory Committee Initiation.* An Advisory Committee may raise an issue for policy development by action of such committee to commence the PDP, and transmission of that request to the GNSO Council.

2. Creation of the Issue Report

Within fifteen (15) calendar days after receiving either (i) an instruction from the Board; (ii) a properly supported motion from a Council member; or (iii) a properly supported motion from an Advisory Committee, the Staff Manager will create a report (an "Issue Report"). Each Issue Report shall contain at least the following:

a. The proposed issue raised for consideration;

b. The identity of the party submitting the issue;

c. How that party is affected by the issue;

d. Support for the issue to initiate the PDP;

e. A recommendation from the Staff Manager as to whether the Council should initiate the PDP for this issue (the "Staff Recommendation"). Each Staff Recommendation shall include the opinion of the ICANN General Counsel regarding whether the issue proposed to initiate the PDP is properly within the scope of the ICANN policy process and within the scope of the GNSO. In

determining whether the issue is properly within the scope of the ICANN policy process, the General Counsel shall examine whether such issue:

1. is within the scope of ICANN's mission statement;

2. is broadly applicable to multiple situations or organizations;

3. is likely to have lasting value or applicability, albeit with the need for occasional updates;

4. will establish a guide or framework for future decision-making; or

5. implicates or affects an existing ICANN policy.

f. On or before the fifteen (15) day deadline, the Staff Manager shall distribute the Issue Report to the full Council for a vote on whether to initiate the PDP, as discussed below.

3. Initiation of PDP

The Council shall initiate the PDP as follows:

a. *Issue Raised by the Board.* If the Board directs the Council to initiate the PDP, then the Council shall meet and do so within fifteen (15) calendar days after receipt of the Issue Report, with no intermediate vote of the Council.

b. *Issue Raised by Other than by the Board.* If a policy issue is presented to the Council for consideration via an Issue Report, then the Council shall meet within fifteen (15) calendar days after receipt of such Report to vote on whether to initiate the PDP. Such meeting may be convened in any manner deemed appropriate by the Council, including in person, via conference call or via electronic mail.

c. *Vote of the Council.* A vote of more than 33% of the Council members present in favor of initiating the PDP will suffice to initiate the PDP; unless the Staff Recommendation stated that the issue is not properly within the scope of the ICANN policy process or the GNSO, in which case a Supermajority Vote of the Council members present in favor of initiating the PDP will be required to initiate the PDP.

4. Commencement of the PDP

At the meeting of the Council initiating the PDP, the Council shall decide, by a majority vote of members present at the meeting, whether to appoint a task force to address the issue. If the Council votes:

a. In favor of convening a task force, it shall do so in accordance with the provisions of Item 7 below.

b. Against convening a task force, then it will collect information on the policy issue in accordance with the provisions of Item 8 below.

5. Composition and Selection of Task Forces

a. Upon voting to appoint a task force, the Council shall invite each of the constituencies of the GNSO to appoint one individual to participate in the task force. Additionally, the Council may appoint up to three outside advisors to sit on the task force. (Each task force member is referred to in this Annex as a "Representative" and collectively, the "Representatives"). The Council may increase the number of Representatives per constituency that may sit on a task force in its discretion in circumstances that it deems necessary or appropriate.

b. Any constituency wishing to appoint a Representative to the task force must submit the name of the constituency designee to the Staff Manager within ten (10) calendar days after such request in order to be included on the task force. Such designee need not be a member of the Council, but must be an individual who has an interest, and ideally knowledge and expertise, in the area to be developed, coupled with the ability to devote a substantial amount of time to task force activities.

c. The Council may also pursue other options that it deems appropriate to assist in the PDP, including appointing a particular individual or organization to gather information on the issue or scheduling meetings for deliberation or briefing. All such information shall be submitted to the Staff Manager within thirty-five (35) calendar days after initiation of the PDP.

6. Public Notification of Initiation of the PDP

After initiation of the PDP, ICANN shall post a notification of such action to the Website. A public comment period shall be commenced for the issue for a period of twenty (20) calendar days after initiation of the PDP. The Staff Manager, or some other designated representative of ICANN shall review the public comments and incorporate them into a report (the "Public Comment Report") to be included in either the Preliminary Task Force Report or the Initial Report, as applicable.

7. Task Forces

a. *Role of Task Force.* If a task force is created, its role will generally be to (i) gather information detailing the positions of formal constituencies and provisional constituencies, if any, within the GNSO; and (ii) otherwise obtain relevant information that will enable the Task Force Report to be as complete and informative as possible.

The task force shall not have any formal decision-making authority. Rather, the role of the task force shall be to gather information that will document the positions of various parties or groups as specifically

and comprehensively as possible, thereby enabling the Council to have a meaningful and informed deliberation on the issue.

b. *Task Force Charter or Terms of Reference.* The Council, with the assistance of the Staff Manager, shall develop a charter or terms of reference for the task force (the "Charter") within ten (10) calendar days after initiation of the PDP. Such Charter will include:

1. the issue to be addressed by the task force, as such issue was articulated for the vote before the Council that commenced the PDP;

2. the specific timeline that the task force must adhere to, as set forth below, unless the Board determines that there is a compelling reason to extend the timeline; and

3. any specific instructions from the Council for the task force, including whether or not the task force should solicit the advice of outside advisors on the issue.

The task force shall prepare its report and otherwise conduct its activities in accordance with the Charter. Any request to deviate from the Charter must be formally presented to the Council and may only be undertaken by the task force upon a vote of a majority of the Council members present.

c. *Appointment of Task Force Chair.* The Staff Manager shall convene the first meeting of the task force within five (5) calendar days after receipt of the Charter. At the initial meeting, the task force members will, among other things, vote to appoint a task force chair. The chair shall be responsible for organizing the activities of the task force, including compiling the Task Force Report. The chair of a task force need not be a member of the Council.

d. *Collection of Information.*

1. *Constituency Statements.* The Representatives will each be responsible for soliciting the position of their constituencies, at a minimum, and other comments as each Representative deems appropriate, regarding the issue under consideration. This position and other comments, as applicable, should be submitted in a formal statement to the task force chair (each, a "Constituency Statement") within thirty-five (35) calendar days after initiation of the PDP. Every Constituency Statement shall include at least the following:

(i) If a Supermajority Vote was reached, a clear statement of the constituency's position on the issue;

(ii) If a Supermajority Vote was not reached, a clear statement of all positions espoused by constituency members;

(iii) A clear statement of how the constituency arrived at its position(s). Specifically, the statement should detail specific constituency meetings, teleconferences, or other means of deliberating an issue, and a list of all members who participated or otherwise submitted their views;

(iv) An analysis of how the issue would affect the constituency, including any financial impact on the constituency; and

(v) An analysis of the period of time that would likely be necessary to implement the policy.

2. *Outside Advisors.* The task force, should it deem it appropriate or helpful, may solicit the opinions of outside advisors, experts, or other members of the public, in addition to those of constituency members. Such opinions should be set forth in a report prepared by such outside advisors, and (i) clearly labeled as coming from outside advisors; (ii) accompanied by a detailed statement of the advisors' (A) qualifications and relevant experience; and (B) potential conflicts of interest. These reports should be submitted in a formal statement to the task force chair within thirty-five (35) calendar days after initiation of the PDP.

e. *Task Force Report.* The chair of the task force, working with the Staff Manager, shall compile the Constituency Statements, Public Comment Report, and other information or reports, as applicable, into a single document ("Preliminary Task Force Report") and distribute the Preliminary Task Force Report to the full task force within forty (40) calendar days after initiation of the PDP. The task force shall have a final task force meeting within five (5) days after the date of distribution of the Preliminary Task Force Report to deliberate the issues and try and reach a Supermajority Vote. Within five (5) calendar days after the final task force meeting, the chair of the task force and the Staff Manager shall create the final task force report (the "Task Force Report") and post it on the Comment Site. Each Task Force Report must include:

1. A clear statement of any Supermajority Vote position of the task force on the issue;

2. If a Supermajority Vote was not reached, a clear statement of all positions espoused by task force members submitted within the twenty-day timeline for submission of constituency reports. Each statement

should clearly indicate (i) the reasons underlying the position and (ii) the constituency(ies) that held the position;

3. An analysis of how the issue would affect each constituency of the task force, including any financial impact on the constituency;

4. An analysis of the period of time that would likely be necessary to implement the policy; and

5. The advice of any outside advisors appointed to the task force by the Council, accompanied by a detailed statement of the advisors' (i) qualifications and relevant experience; and (ii) potential conflicts of interest.

8. Procedure if No Task Force is Formed

a. If the Council decides not to convene a task force, the Council will request that, within ten (10) calendar days thereafter, each constituency appoint a representative to solicit the constituency's views on the issue. Each such representative shall be asked to submit a Constituency Statement to the Staff Manager within thirty-five (35) calendar days after initiation of the PDP.

b. The Council may also pursue other options that it deems appropriate to assist in the PDP, including appointing a particular individual or organization to gather information on the issue or scheduling meetings for deliberation or briefing. All such information shall be submitted to the Staff Manager within thirty-five (35) calendar days after initiation of the PDP.

c. The Staff Manager will take all Constituency Statements, Public Comment Statements, and other information and compile (and post on the Comment Site) an Initial Report within fifty (50) calendar days after initiation of the PDP. Thereafter, the PDP shall follow the provisions of Item 9 below in creating a Final Report.

9. Public Comments to the Task Force Report or Initial Report

a. The public comment period will last for twenty (20) calendar days after posting of the Task Force Report or Initial Report. Any individual or organization may submit comments during the public comment period, including any constituency that did not participate in the task force. All comments shall be accompanied by the name of the author of the comments, the author's relevant experience, and the author's interest in the issue.

b. At the end of the twenty (20) day period, the Staff Manager will be responsible for reviewing the comments received and adding those deemed appropriate for inclusion in the Staff Manager's reasonable discretion to the Task Force Report or Initial Report (collectively, the "Final Report"). The Staff Manager shall not be obligated to include

all comments made during the comment period, including each comment made by any one individual or organization.

c. The Staff Manager shall prepare the Final Report and submit it to the Council chair within ten (10) calendar days after the end of the public comment period.

10. Council Deliberation

a. Upon receipt of a Final Report, whether as the result of a task force or otherwise, the Council chair will (i) distribute the Final Report to all Council members; and (ii) call for a Council meeting within ten (10) calendar days thereafter. The Council may commence its deliberation on the issue prior to the formal meeting, including via in-person meetings, conference calls, e-mail discussions or any other means the Council may choose. The deliberation process shall culminate in a formal Council meeting either in person or via teleconference, wherein the Council will work towards achieving a Supermajority Vote to present to the Board.

b. The Council may, if it so chooses, solicit the opinions of outside advisors at its final meeting. The opinions of these advisors, if relied upon by the Council, shall be (i) embodied in the Council's report to the Board, (ii) specifically identified as coming from an outside advisor; and (iii) be accompanied by a detailed statement of the advisor's (x) qualifications and relevant experience; and (y) potential conflicts of interest.

11. Council Report to the Board

The Staff Manager will be present at the final meeting of the Council, and will have five (5) calendar days after the meeting to incorporate the views of the Council into a report to be submitted to the Board (the "Board Report"). The Board Report must contain at least the following:

a. A clear statement of any Supermajority Vote recommendation of the Council;

b. If a Supermajority Vote was not reached, a clear statement of all positions held by Council members. Each statement should clearly indicate (i) the reasons underlying each position and (ii) the constituency(ies) that held the position;

c. An analysis of how the issue would affect each constituency, including any financial impact on the constituency;

d. An analysis of the period of time that would likely be necessary to implement the policy;

e. The advice of any outside advisors relied upon, which should be accompanied by a detailed statement of the advisor's (i) qualifications and relevant experience; and (ii) potential conflicts of interest;

f. The Final Report submitted to the Council; and

g. A copy of the minutes of the Council deliberation on the policy issue, including the all opinions expressed during such deliberation, accompanied by a description of who expressed such opinions.

12. Agreement of the Council

A Supermajority Vote of the Council members will be deemed to reflect the view of the Council, and may be conveyed to the Board as the Council's recommendation. Abstentions shall not be permitted; thus all Council members must cast a vote unless they identify a financial interest in the outcome of the policy issue. Notwithstanding the foregoing, as set forth above, all viewpoints expressed by Council members during the PDP must be included in the Board Report.

13. Board Vote

a. The Board will meet to discuss the GNSO Council recommendation as soon as feasible after receipt of the Board Report from the Staff Manager.

b. In the event that the Council reached a Supermajority Vote, the Board shall adopt the policy according to the Council Supermajority Vote recommendation unless by a vote of more than sixty-six (66%) percent of the Board determines that such policy is not in the best interests of the ICANN community or ICANN.

c. In the event that the Board determines not to act in accordance with the Council Supermajority Vote recommendation, the Board shall (i) articulate the reasons for its determination in a report to the Council (the "Board Statement"); and (ii) submit the Board Statement to the Council.

d. The Council shall review the Board Statement for discussion with the Board within twenty (20) calendar days after the Council's receipt of the Board Statement. The Board shall determine the method (e.g., by teleconference, e-mail, or otherwise) by which the Council and Board will discuss the Board Statement.

e. At the conclusion of the Council and Board discussions, the Council shall meet to affirm or modify its recommendation, and communicate that conclusion (the "Supplemental Recommendation") to the Board, including an explanation for its current recommendation. In the event that the Council is able to reach a Supermajority Vote on the Supplemental Recommendation, the Board shall adopt the recommendation unless more than sixty-six (66%) percent of the Board determines that such policy is not in the interests of the ICANN community or ICANN.

f. In any case in which the Council is not able to reach Supermajority, a majority vote of the Board will be sufficient to act.

g. When a final decision on a GNSO Council Recommendation or Supplemental Recommendation is timely, the Board shall take a preliminary vote and, where practicable, will publish a tentative decision that allows for a ten (10) day period of public comment prior to a final decision by the Board.

14. Implementation of the Policy

Upon a final decision of the Board, the Board shall, as appropriate, give authorization or direction to the ICANN staff to take all necessary steps to implement the policy.

15. Maintenance of Records

Throughout the PDP, from policy suggestion to a final decision by the Board, ICANN will maintain on the Website, a status web page detailing the progress of each PDP issue, which will describe:

a. The initial suggestion for a policy;

b. A list of all suggestions that do not result in the creation of an Issue Report;

c. The timeline to be followed for each policy;

d. All discussions among the Council regarding the policy;

e. All reports from task forces, the Staff Manager, the Council and the Board; and

f. All public comments submitted.

16. Additional Definitions

"Comment Site" and "Website" refer to one or more web sites designated by ICANN on which notifications and comments regarding the PDP will be posted.

"Staff Manager" means an ICANN staff person(s) who manages the PDP.

"Supermajority Vote" means a vote of more than sixty-six (66) percent of the members present at a meeting of the applicable body.

Comments concerning the layout, construction and functionality of this site should be sent to webmaster@icann.org.

Page Updated 15-Mar-2003

©1998 2002 The nternet Corporation for Assigned Names and Numbers All rights reserved

EXHIBIT JMR-10

JMR-10

ICANN-NSI Registry Agreement

(Approved November 4, 1999)

(Signed November 10, 1999)

(Posted November 10, 1999)

On September 28, 1999, ICANN announced tentative agreement with the United States Department of Commerce and Network Solutions, Inc. on a series of agreements that will put the newly introduced competition among registrars in the .com, .net, and .org TLDs on a permanant and firmer footing. After written and oral public comments, these agreements were revised in several respects and were adopted by the ICANN Board on November 4, 1999.

One of these agreements is a registry agreement under which NSI will operate the registry for the .com, .net, and .org top-level domains according to requirements stated in the agreement and developed in the future through the ICANN consensus-based process. All ICANN-accredited registrars will have equal access to this registry.

The text of the registry agreement appears below.

REGISTRY AGREEMENT

This REGISTRY AGREEMENT ("Agreement") is by and between the Internet Corporation for Assigned Names and Numbers, a not-for-profit corporation, and Network Solutions, Inc., a Delaware corporation.

Definitions

For purposes of this Agreement, the following definitions shall apply:

1. A "Consensus Policy" is one adopted by ICANN as follows:

> (a) "Consensus Policies" are those adopted based on a consensus among Internet stakeholders represented in the ICANN process, as demonstrated by (1) the adoption of the policy by the ICANN Board of Directors, (2) a recommendation that the policy should be adopted by at least a two-thirds vote of the council of the ICANN Supporting Organization to which the matter is delegated, and (3) a written report and supporting materials (which must include all substantive submissions to the Supporting Organization relating to the proposal) that (i) documents the extent of agreement and disagreement among impacted groups, (ii) documents the outreach process used to seek to achieve adequate representation of the views of groups that are likely to be impacted, and (iii) documents the nature and intensity of reasoned support and opposition to the proposed policy.

(b) In the event that NSI disputes the presence of such a consensus, it shall seek review of that issue from an Independent Review Panel established under ICANN's bylaws. Such review must be sought within fifteen working days of the publication of the Board's action adopting the policy. The decision of the panel shall be based on the report and supporting materials required by subsection (a) above. In the event that NSI seeks review and the Panel sustains the Board's determination that the policy is based on a consensus among Internet stakeholders represented in the ICANN process, then NSI must implement such policy unless it promptly seeks and obtains injunctive relief under Section 13 below.

(c) If, following a decision by the Independent Review Panel convened under subsection (b) above, NSI still disputes the presence of such a consensus, it may seek further review of that issue within fifteen working days of publication of the decision in accordance with the dispute resolution procedures set forth in Section 13 below; provided, however, that NSI must continue to implement the policy unless it has obtained injunctive relief under Section 13 below or a final decision is rendered in accordance with the provisions of Section 13 that relieves NSI of such obligation. The decision in any such further review shall be based on the report and supporting materials required by subsection (a) above.

(d) A policy adopted by the ICANN Board of Directors on a temporary basis, without a prior recommendation by the council of an ICANN Supporting Organization, shall also be considered to be a Consensus Policy if adopted by the ICANN Board of Directors by a vote of at least two-thirds of its members, and if immediate temporary adoption of a policy on the subject is necessary to maintain the stability of the Internet or the operation of the domain name system, and if the proposed policy is as narrowly tailored as feasible to achieve those objectives. In adopting any policy under this provision, the ICANN Board of Directors shall state the period of time for which the policy is temporarily adopted and shall immediately refer the matter to the appropriate Supporting Organization for its evaluation and review with a detailed explanation of its reasons for adopting the temporary policy and why the Board believes the policy should receive the consensus support of Internet stakeholders. If the period of time for which the policy is adopted exceeds 45 days, the Board shall reaffirm its temporary adoption every 45 days for a total period not to exceed 180 days, in order to maintain such policy in effect until such time as it meets the standard set forth in subsection (a) above. If the standard set forth in subsection (a) above is not met within the temporary period set by the Board, or the council of the Supporting Organization to which it has been referred votes to reject the temporary policy, it will no longer be a "Consensus Policy."

(e) For all purposes under this Agreement, the policies identified in Appendix A adopted by the ICANN Board of Directors before the effective date of this Agreement shall be treated in the same manner and have the same effect as "Consensus Policies."

(f) In the event that, at the time the ICANN Board adopts a policy under subsection (a) above during the term of this Agreement, ICANN does not have in place an Independent Review Panel established under ICANN's bylaws, the fifteen working day period allowed under subsection (b) above to seek review shall be extended until fifteen working days after ICANN does have such an Independent Review Panel in place and NSI shall not be obligated to comply with the policy in the interim.

2. The "Effective Date" is the date on which the Agreement is signed by ICANN and NSI.

3. The "Expiration Date" is the date specified in Section 23 below.

4. "gTLDs" means the .com, .net, and .org TLDs, and any new gTLDs established by ICANN.

5. "ICANN" refers to the Internet Corporation for Assigned Names and Numbers, a party to this Agreement.

6. "NSI" refers to Network Solutions, Inc., in its capacity as a domain name registry for the Registry TLDs, a party to this Agreement.

7. "Personal Data" refers to data about any identified or identifiable natural person.

8. "Registry Data" means all data maintained in electronic form in the registry database, and shall include Zone File Data, all data submitted by registrars in electronic form, and all other data concerning particular registrations or nameservers maintained in electronic form in the registry database.

9. "Registry Services" means operation of the registry for the Registry TLDs and shall include receipt of data concerning registrations and nameservers from registrars, provision of status information to registrars, operation of the registry TLD zone servers, and dissemination of TLD zone files.

10. "Registry TLDs" refers to the .com, .net, and .org TLDs.

11. "SLD" refers to a second-level domain in the Internet domain name system.

12. "Term of this Agreement" begins on the Effective Date and runs through the earliest of (a) the Expiration Date, (b) termination of this Agreement under Section 14 or Section 16(B), or (c) termination of this Agreement pursuant to withdrawal of the Department of Commerce's recognition of ICANN under Section 24.

13. "TLD" refers to a top-level domain in the Internet domain name system.

14. "Zone File Data" means all data contained in domain name system zone files for the Registry TLDs as provided to TLD nameservers on the Internet.

Agreements

NSI and ICANN agree as follows:

1. Designation of Registry. ICANN acknowledges and agrees that NSI is and will remain the registry for the Registry TLD(s) throughout the Term of this Agreement.

2. Recognition in Authoritative Root Server System. In the event and to the extent that ICANN is authorized to set policy with regard to an authoritative root server system, it will ensure that (A) the authoritative root will point to the TLD zone servers designated by NSI for the Registry TLDs throughout the Term of this Agreement and (B) any changes to TLD zone server designation submitted to ICANN by NSI will be implemented by ICANN within five business days of submission. In the event that this Agreement is terminated (A) under Section 14 or 16(B) by NSI or (B) under Section 24 due to the withdrawal of recognition of ICANN by the United States Department of Commerce, ICANN's obligations concerning TLD zone server designations for the .com, .net, and .org TLDs in the authoritative root server system shall be as stated in a separate agreement between ICANN and the Department of Commerce.

3. General Obligations of NSI.

(A) During the Term of this Agreement:

(i) NSI agrees that it will operate the registry for the Registry TLDs in accordance with this Agreement;

(ii) NSI shall comply, in its operation of the registry, with all Consensus Policies insofar as they:

(a) are adopted by ICANN in compliance with Section 4 below,

(b) relate to one or more of the following: (1) issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, technical reliability and/or stable operation of the Internet or domain-name system, (2) registry policies reasonably necessary to implement Consensus Policies relating to registrars, or (3) resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names), and

(c) do not unreasonably restrain competition.

(B) NSI acknowledges and agrees that upon the earlier of (i) the Expiration Date or (ii) termination of this Agreement by ICANN pursuant to Section 14, it will cease to be the registry for the Registry TLDs, unless prior to the end of the term of this Agreement NSI is chosen as the Successor Registry in accordance with the provisions of this Agreement.

(C) To the extent that Consensus Policies are adopted in conformance with Section 4 of this Agreement, the measures permissible under Section 3(A)(ii)(b) shall include, without limitation:

(i) principles for allocation of SLD names (e.g., first-come/first-served, timely renewal, holding period after expiration);

(ii) prohibitions on warehousing of or speculation in domain names by registries or registrars;

(iii) reservation of SLD names that may not be registered initially or that may not be renewed due to reasons reasonably related to (a) avoidance of confusion among or misleading of users, (b) intellectual property, or (c) the technical management of the DNS or the Internet (e.g., "example.com" and single-letter/digit names);

(iv) the allocation among continuing registrars of the SLD names sponsored in the registry by a registrar losing accreditation; and

(v) dispute resolution policies that take into account the use of a domain name.

Nothing in this Section 3 shall limit or otherwise affect NSI's obligations as set forth elsewhere in this Agreement.

4. General Obligations of ICANN. With respect to all matters that impact the rights, obligations, or role of NSI, ICANN shall during the Term of this Agreement:

(A) exercise its responsibilities in an open and transparent manner;

(B) not unreasonably restrain competition and, to the extent feasible, promote and encourage robust competition;

(C) not apply standards, policies, procedures or practices arbitrarily, unjustifiably, or inequitably and not single out NSI for disparate treatment unless justified by substantial and reasonable cause; and

(D) ensure, through its reconsideration and independent review policies, adequate appeal procedures for NSI, to the extent it is adversely affected by ICANN standards, policies, procedures or practices.

5. Protection from Burdens of Compliance With ICANN Policies. ICANN hereby agrees to indemnify and hold harmless NSI, and its directors, officers, employees and agents from and against any and all claims, damages or liabilities arising solely from NSI's compliance as required by this Agreement with an ICANN policy adopted after both parties have entered into this Agreement, except that NSI shall not be indemnified or held harmless hereunder to the extent that the claims, damages or liabilities arise from the particular manner in which NSI has chosen to comply with the policy. In addition, NSI shall be given a reasonable period after receiving notice of adoption of an ICANN Consensus Policy in which to comply with that policy.

6. NSI Registry-Level Financial Support of ICANN. NSI, in its role as operator of the registry for the Registry TLDs, shall pay the gTLD registry-level fees adopted by ICANN in conformance with Section 4 of this Agreement, provided such fees are reasonably allocated among all gTLD registries that contract with ICANN and provided further that, if NSI's share of the total gTLD registry-level fees are or are budgeted to be in excess of $250,000 in any given year, any such excess must be expressly approved by gTLD registries accounting, in aggregate, for payment of two-thirds of all gTLD registry-level fees. NSI shall pay such fees in a timely manner throughout the Term of this Agreement, and notwithstanding the pendency of any dispute between NSI and ICANN. NSI agrees to prepay $250,000 toward its share of gTLD registry-level fees at the time of signing of this Agreement.

7. Data Escrow. NSI shall deposit into escrow all Registry Data on a schedule (not more frequently than weekly for a complete set of Registry Data, and daily for incremental updates) and in an electronic format mutually approved from time to time by NSI and ICANN, such approval not to be unreasonably withheld by either party. The escrow shall be maintained, at NSI's expense, by a reputable escrow agent mutually approved by NSI and ICANN, such approval also not to be unreasonably withheld by either party. The escrow shall be held under an agreement among ICANN, NSI, the United States Department of Commerce, and the escrow agent providing that (A) the data shall be received and held in escrow, with no use other than verification that the deposited data is complete and in proper format, until released to ICANN or to the United States Department of Commerce; (B) the data shall be released to ICANN upon termination of this Agreement by ICANN under Section 14 or upon the Expiration Date if (1) this Agreement has not sooner been terminated and (2) it has been finally determined by the ICANN Board (and no injunction obtained pursuant to Section 13 has been obtained) that NSI will not be designated as the successor registry under Section 22 of this Agreement; and (C), in the alternative, the data shall be released to the United States Department of Commerce according to the terms of the cooperative agreement between NSI and the United States Government.

8. NSI Handling of Personal Data. NSI agrees to notify registrars sponsoring registrations in the registry of the purposes for which Personal Data submitted to the registry by registrars is collected, the recipients (or categories of recipients) of such Personal Data, and the mechanism for access to and correction of such Personal Data. NSI shall take reasonable steps to protect Personal Data from loss, misuse, unauthorized disclosure, alteration or destruction. NSI shall not use or authorize the use of Personal Data in a way that is incompatible with the notice provided to registrars.

9. Publication by NSI of Registry Data.

(A) NSI shall provide an interactive web page and a port 43 Whois service providing free public query-based access to up-to-date (i.e. updated at least daily) registry database data which, in response to input of an SLD name, shall report at least the following data elements in response to queries: (a) the SLD name registered, (b) the TLD in which the SLD is registered;

(c) the IP addresses and corresponding names of the primary nameserver and secondary nameserver(s) for such SLD, (d) the identity of the sponsoring Registrar, and (e) the date of the most recent modification to the domain name record in the registry database; provided, however, that if ICANN adopts a Consensus Policy that adds to or subtracts from these elements, NSI will implement that policy.

(B) To ensure operational stability of the registry, NSI may temporarily limit access under subsection (A), in which case NSI shall immediately notify ICANN of the nature of and reason for the limitation. NSI shall not continue the limitation longer than three business days if ICANN objects in writing, which objection shall not be unreasonably made. Such temporary limitations shall be applied in a nonarbitrary manner and shall apply fairly to any registrar similarly situated, including NSI.

(C) NSI as registry shall comply with Consensus Policies providing for development and operation of a capability that provides distributed free public query-based (web and command-line) access to current registration data implemented by registrars providing for capabilities comparable to WHOIS, including (if called for by the Consensus Policy) registry database lookup capabilities according to a specified format. If such a service implemented by registrars on a distributed basis does not within a reasonable time provide reasonably robust, reliable and convenient access to accurate and up-to-date registration data, NSI as registry shall cooperate and, if reasonably determined to be necessary by ICANN (considering such possibilities as remedial action by specific registrars), provide data from the registry database to facilitate the development of a centralized service providing equivalent functionality in a manner established by a Consensus Policy.

10. Rights in Data. Except as permitted by the Registrar License and Agreement, NSI shall not be entitled to claim any intellectual property rights in data in the registry supplied by or through registrars other than NSI. In the event that Registry Data is released from escrow under Section 7 or transferred to a Successor Registry under Section 22(D), any rights held by NSI as registry in the data shall automatically be licensed on a non-exclusive, irrevocable, royalty-free, paid-up basis to the recipient of the data.

11. Limitation of Liability. Neither party shall be liable to the other under this Agreement for any special, indirect, incidental, punitive, exemplary or consequential damages.

12. Specific Performance. During the Term of this Agreement, either party may seek specific performance of any provision of this Agreement as provided by Section 13, provided the party seeking such performance is not in material breach of its obligations.

13. Resolution of Disputes Under This Agreement. Disputes arising under or in connection with this Agreement, including requests for specific performance, shall be resolved in a court of competent jurisdiction or, at the election of both parties (except for any dispute over whether a policy adopted by the Board is a Consensus Policy, in which case at the election of either party), by an arbitration conducted as provided in this Section pursuant to the International Arbitration Rules of the American Arbitration Association ("AAA"). The arbitration shall be conducted in English and shall occur in Los Angeles County, California, USA. There shall be three arbitrators: each party shall choose one arbitrator and, if the two arbitrators are not able to agree on a third arbitrator, the third shall be chosen by the AAA. The parties shall bear the costs of the arbitration in equal shares, subject to the right of the arbitrators to reallocate the costs in their award as provided in the AAA rules. The parties shall bear their own attorneys' fees in connection with the arbitration, and the arbitrators may not reallocate the attorneys' fees in conjunction with their award. The arbitrators shall render their decision within ninety days of the initiation of arbitration. In all litigation involving ICANN concerning this Agreement (whether in a case where arbitration has not been elected or to enforce an arbitration award), jurisdiction and exclusive venue for such litigation shall

be in a court located in Los Angeles, California, USA; however, the parties shall also have the right to enforce a judgment of such a court in any court of competent jurisdiction. For the purpose of aiding the arbitration and/or preserving the rights of the parties during the pendency of an arbitration, the parties shall have the right to seek temporary or preliminary injunctive relief from the arbitration panel or a court located in Los Angeles, California, USA, which shall not be a waiver of this arbitration agreement.

14. Termination.

(A) In the event an arbitration award or court judgment is rendered specifically enforcing any provision of this Agreement or declaring a party's rights or obligations under this Agreement, either party may, by giving written notice, demand that the other party comply with the award or judgment. In the event that the other party fails to comply with the order or judgment within ninety days after the giving of notice (unless relieved of the obligation to comply by a court or arbitration order before the end of that ninety-day period), the first party may terminate this Agreement immediately by giving the other party written notice of termination.

(B) In the event of termination by DOC of its Cooperative Agreement with NSI pursuant to Section I.B.8 of Amendment 19 to that Agreement, ICANN shall, after receiving express notification of that fact from DOC and a request from DOC to terminate NSI as the operator of the registry database for the Registry TLDs, terminate NSI's rights under this Agreement, and shall cooperate with DOC to facilitate the transfer of the operation of the registry database to a successor registry.

15. Assignment. Neither party may assign this Agreement without the prior written approval of the other party, such approval not to be unreasonably withheld. Notwithstanding the foregoing sentence, a party may assign this Agreement by giving written notice to the other party in the following circumstances, provided the assignee agrees in writing with the other party to assume the assigning party's obligations under this Agreement: (a) NSI may assign this Agreement as part of the transfer of its registry business approved under Section 25 and (b) ICANN may, in conjunction with a reorganization or reincorporation of ICANN and with the written approval of the Department of Commerce, assign this Agreement to another non-profit corporation organized for the same or substantially the same purposes as ICANN.

16. Relationship to Cooperative Agreement Between NSI and U.S. Government.

(A) NSI's obligations under this Agreement are conditioned on the agreement by NSI and the Department of Commerce to Amendment 19 to the Cooperative Agreement in the form attached to this Agreement as Appendix C.

(B) If within a reasonable period of time ICANN has not made substantial progress towards having entered into agreements with competing registries and NSI is adversely affected from a competitive perspective, NSI may terminate this Agreement with the approval of the U.S. Department of Commerce. In such event, as provided in Section 16(A) above, the Cooperative Agreement shall replace this Agreement.

(C) In the case of conflict while they are both in effect, and to the extent that they address the same subject in an inconsistent manner, the term(s) of the Cooperative Agreement shall take precedence over this Agreement.

17. NSI Agreements with Registrars. NSI shall make access to the Shared Registration System available to all ICANN-accredited registrars subject to the terms of the NSI/Registrar License and Agreement (attached as Appendix B). Such agreement may be revised by NSI, provided however, that any such changes must be approved in advance by ICANN. Such agreement shall also be revised to incorporate any Registry Service Level Agreement implemented under Section 18.

18. Performance and Functional Specifications for Registry Services. Unless and until ICANN adopts different standards as a Consensus Policy pursuant to Section 4, NSI shall provide registry services to ICANN-accredited registrars meeting the performance and functional specifications set forth in SRS specification version 1.0.6 dated September 10, 1999, as supplemented by Appendix E and any Registry Service Level Agreement established according to this Section 18. In the event ICANN adopts different performance and functional standards for the registry as a Consensus Policy in compliance with Section 4, NSI shall comply with those standards to the extent practicable, provided that compensation pursuant to the provisions of Section 20 has been resolved prior to implementation and provided further that NSI is given a reasonable time for implementation. In no event shall NSI be required to implement any different functional standards before 3 years from the Effective Date of this Agreement.

Within 45 days after the Effective Date, (i) representatives designated by ICANN of registrars accredited by ICANN for the Registry TLDs and (ii) NSI will establish a Registry Service Level Agreement for the registry system that shall include, at least:

(A) identified service level parameters and measurements regarding performance of the registry system, including, for example, system availability;

(B) responsibilities of registrars using the registry system and NSI (e.g., the obligation of the registrars to notify NSI of any experienced registry system outages and the obligation of NSI to respond in a timely manner to registry system outages);

(C) an appropriate service-level dispute-resolution process; and

(D) remedies for failure to comply with the Registry Service Level Agreement.

Unless the Registry Service Level Agreement requires fundamental architecture changes to the registry system or extraordinary increases in costs to NSI beyond what is generally required to implement a service level agreement (which is not the intent of the parties) the creation and implementation of the Registry Service Level Agreement shall not result in a price increase under Section 20.

The 45-day drafting process for the Registry Service Level Agreement shall be structured as follows: (E) the designated representatives and NSI (the "SLA Working Group") shall promptly meet and shall within 20 days after the Effective Date complete a draft of the Registry Service Level Agreement; (F) all registrars accredited by ICANN for the Registry TLDs shall have 10 days after distribution of that draft to submit comments to the SLA Working Group; and (G) the SLA Working Group shall meet again to finalize the Registry Service Level Agreement, taking into account the comments of the registrars. The 45-day period shall be subject to extension by mutual agreement of the members of the SLA Working Group. The SLA shall be implemented as soon as reasonably feasible after its completion and approval by ICANN, including by implementation in stages if appropriate.

After it is approved by the SLA Working Group and ICANN, the Registry Service Level Agreement shall be incorporated in the NSI/Registrar License and Agreement referred to in Section 17.

19. Bulk Access to Zone Files. NSI shall provide third parties bulk access to the zone files for .com, .net, and .org TLDs on the terms set forth in the zone file access agreement (attached as Appendix D). Such agreement may be revised by NSI, provided however, that any such changes must be approved in advance by ICANN.

20. Price for Registry Services. The price(s) to accredited registrars for entering initial and renewal SLD registrations into the registry database and for transferring a SLD registration from one accredited registrar to another will be as set forth in Section 5 of the Registrar License and Agreement (attached as Appendix B). These prices shall be increased through an amendment to this Agreement as approved by

ICANN and NSI, such approval not to be unreasonably withheld, to reflect demonstrated increases in the net costs of operating the registry arising from (1) ICANN policies adopted after the date of this Agreement, or (2) legislation specifically applicable to the provision of Registry Services adopted after the date of this Agreement, to ensure that NSI recovers such costs and a reasonable profit thereon; provided that such increases exceed any reductions in costs arising from (1) or (2) above.

21. Additional NSI Obligations.

(A) NSI shall provide all licensed Accredited Registrars (including NSI acting as registrar) with equivalent access to the Shared Registration System. NSI further agrees that it will make a certification to ICANN every six months, using the objective criteria set forth in Appendix F that NSI is providing all licensed Accredited Registrars with equivalent access to its registry services.

(B) NSI will ensure, in a form and through ways described in Appendix F that the revenues and assets of the registry are not utilized to advantage NSI's registrar activities to the detriment of other registrars.

22. Designation of Successor Registry.

(A) Not later than one year prior to the end of the term of this Agreement, ICANN shall, in accordance with Section 4, adopt an open, transparent procedure for designating a Successor Registry. The requirement that this procedure be opened one year prior to the end of the Agreement shall be waived in the event that the Agreement is terminated prior to its expiration.

(B) NSI or its assignee shall be eligible to serve as the Successor Registry and neither the procedure established in accordance with subsection (A) nor the fact that NSI is the incumbent shall disadvantage NSI in comparison to other entities seeking to serve as the Successor Registry.

(C) If NSI or its assignee is not designated as the Successor Registry, NSI or its assignee shall cooperate with ICANN and with the Successor Registry in order to facilitate the smooth transition of operation of the registry to Successor Registry. Such cooperation shall include the timely transfer to the Successor Registry of an electronic copy of the registry database and of a full specification of the format of the data.

(D) ICANN shall select as the Successor Registry the eligible party that it reasonably determines is best qualified to perform the registry function under terms and conditions developed as a Consensus Policy, taking into account all factors relevant to the stability of the Internet, promotion of competition, and maximization of consumer choice, including without limitation: functional capabilities and performance specifications proposed by the eligible party for its operation of the registry, the price at which registry services are proposed to be provided by the party, relevant experience of the party, and demonstrated ability of the party to handle operations at the required scale. ICANN shall not charge any additional fee to the Successor Registry.

(E) In the event that a party other than NSI or its assignee is designated as the Successor Registry, NSI shall have the right to challenge the reasonableness of ICANN's failure to designate NSI or its assignee as the Successor Registry under the provisions of Section 13 of this Agreement.

23. Expiration of this Agreement. The Expiration Date shall be four years after the Effective Date, unless extended as provided below. In the event that NSI completes the legal separation of ownership of its

Registry Services business from its registrar business by divesting all the assets and operations of one of those businesses within 18 months after Effective Date to an unaffiliated third party that enters an agreement enforceable by ICANN and the Department of Commerce (i) not to be both a registry and a registrar in the Registry TLDs, and (ii) not to control, own or have as an affiliate any individual(s) or entity (ies) that, collectively, act as both a registry and a registrar in the Registry TLDs, the Expiration Date shall be extended for an additional four years, resulting in a total term of eight years. For the purposes of this Section, "unaffiliated third party" means any entity in which NSI (including its successors and assigns, subsidiaries and divisions, and their respective directors, officers, employees, agents and representatives) does not have majority equity ownership or the ability to exercise managerial or operational control, either directly or indirectly through one or more intermediaries. "Control," as used in this Section 23, means any of the following: (1) ownership, directly or indirectly, or other interest entitling NSI to exercise in the aggregate 25% or more of the voting power of an entity; (2) the power, directly or indirectly, to elect 25% or more of the board of directors (or equivalent governing body) of an entity; or (3) the ability, directly or indirectly, to direct or cause the direction of the management, operations, or policies of an entity.

24. Withdrawal of Recognition of ICANN by the Department of Commerce. In the event that, prior to the expiration or termination of this Agreement under Section 14 or 16(B), the United States Department of Commerce withdraws its recognition of ICANN as NewCo under the Statement of Policy pursuant to the procedures set forth in Section 5 of Amendment 1 (dated November 10, 1999) to the Memorandum of Understanding between ICANN and the Department of Commerce, this Agreement shall terminate.

25. Assignment of Registry Assets. NSI may assign and transfer its registry assets in connection with the sale of its registry business only with the approval of the Department of Commerce.

26. Option to Substitute Generic Agreement. At NSI's option, it may substitute any generic ICANN/Registry agreement that may be adopted by ICANN for this Agreement; provided, however, that Sections 16, 19, 20, 21, 23, 24, and 25 of this Agreement will remain in effect following any such election by NSI.

27. Notices, Designations, and Specifications. All notices to be given under this Agreement shall be given in writing at the address of the appropriate party as set forth below, unless that party has given a notice of change of address in writing. Any notice required by this Agreement shall be deemed to have been properly given when delivered in person, when sent by electronic facsimile, or when scheduled for delivery by internationally recognized courier service. Designations and specifications by ICANN under this Agreement shall be effective when written notice of them is deemed given to Registry.

If to ICANN, addressed to:

Internet Corporation for Assigned Names and Numbers
4676 Admiralty Way, Suite 330
Marina Del Rey, California 90292
Telephone: 1/310/823-9358
Facsimile: 1/310/823-8649
Attention: Chief Executive Officer

If to Registry, addressed to:

1. Network Solutions, Inc.
Contact Information Redacted

Telephone: Con ac nforma ion Redac ed
Facsimile: Con ac nforma ion Redac ed
Attention: General Counsel

2.Network Solutions, Inc.
Contact Information Redacted

Telephone: Con ac nforma ion Redac ed
Facsimile: Con ac nforma ion Redac ed
Attention: Registry General Manager

28. Dates and Times. All dates and times relevant to this Agreement or its performance shall be computed based on the date and time observed in Los Angeles, California, USA.

29. Language. All notices, designations, and specifications made under this Agreement shall be in the English language.

30. Entire Agreement. This Agreement constitutes the entire agreement of the parties hereto pertaining to the registry for the Registry TLDs and supersedes all prior agreements, understandings, negotiations and discussions, whether oral or written, between the parties on that subject. This Agreement is intended to coexist with any Registrar Accreditation Agreement between the parties.

31. Amendments and Waivers. No amendment, supplement, or modification of this Agreement or any provision hereof shall be binding unless executed in writing by both parties. No waiver of any provision of this Agreement shall be binding unless evidenced by a writing signed by the party waiving compliance with such provision. No waiver of any of the provisions of this Agreement shall be deemed or shall constitute a waiver of any other provision hereof, nor shall any such waiver constitute a continuing waiver unless otherwise expressly provided.

32. Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed in duplicate by their duly authorized representatives.

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS

By:_____

Michael M. Roberts

President and CEO

Date: November 10, 1999

NETWORK SOLUTIONS, INC.

By:_____

Jonathan W. Emery

Senior Vice President, General

Counsel & Secretary

Date: November 10, 1999

Page modified 10-November-1999

EXHIBIT JMR-11

Published on *National Telecommunications and Information Administration* (https://www.ntia.doc.gov)

Statement of Policy on the Management of Internet Names and Addresses

Topics:

- Domain Name System [1]

Date:
June 05, 1998
Docket Number:
980212036-8146-02

UNITED STATES DEPARTMENT OF COMMERCE

Management of Internet Names and Addresses

Docket Number: 980212036-8146-02

AGENCY: National Telecommunications and Information Administration

ACTION: Statement of Policy

SUMMARY: On July 1, 1997, as part of the Clinton Administration's *Framework for Global Electronic Commerce*,(1) the President directed the Secretary of Commerce to privatize the domain name system (DNS) in a manner that increases competition and facilitates international participation in its management.

Accordingly, on July 2, 1997, the Department of Commerce issued a Request for Comments (RFC) on DNS administration. The RFC solicited public input on issues relating to the overall framework of the DNS administration, the creation of new top-level domains, policies for domain name registrars, and trademark issues. During the comment period, more than 430 comments were received, amounting to some 1500 pages.(2)

On January 30, 1998, the National Telecommunications and Information Administration (NTIA), an agency of the Department of Commerce, issued for comment, *A Proposal to Improve the Technical Management of Internet Names and Addresses.* The proposed rulemaking, or "Green Paper," was published in the Federal Register on February 20, 1998,

providing opportunity for public comment. NTIA received more than 650 comments, as of March 23, 1998, when the comment period closed.[3]

The Green Paper proposed certain actions designed to privatize the management of Internet names and addresses in a manner that allows for the development of robust competition and facilitates global participation in Internet management. The Green Paper proposed for discussion a variety of issues relating to DNS management including private sector creation of a new not-for-profit corporation (the "new corporation") managed by a globally and functionally representative Board of Directors.

EFFECTIVE DATE: This general statement of policy is not subject to the delay in effective date required of substantive rules under 5 U.S.C. § 553(d). It does not contain mandatory provisions and does not itself have the force and effect of law.[4] Therefore, the effective date of this policy statement is [insert date of publication in the Federal Register].

FOR FURTHER INFORMATION CONTACT: Karen Rose, Office of International Affairs (OIA), Rm 4701, National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce, Contact Information Redacted. Telephone: Contact nformation Redacted. E-mail: Contact Information Redacted [2]

AUTHORITY: 15 U.S.C. § 1512; 15 U.S.C. § 1525; 47 U.S.C. § 902(b)(2)(H); 47 U.S.C. § 902(b)(2)(I); 47 U.S.C. § 902(b)(2)(M); 47 U.S.C. § 904(c)(1).

SUPPLEMENTARY INFORMATION:

Background:

Domain names are the familiar and easy-to-remember names for Internet computers (e.g., "www.ecommerce.gov"). They map to unique Internet Protocol (IP) numbers (e.g., 98.37.241.30) that serve as routing addresses on the Internet. The domain name system (DNS) translates Internet names into the IP numbers needed for transmission of information across the network.

U.S. Role in DNS Development:

More than 25 years ago, the U.S. Government began funding research necessary to develop packet-switching technology and communications networks, starting with the "ARPANET" network established by the Department of Defense's Advanced Research Projects Agency (DARPA) in the 1960s. ARPANET was later linked to other networks established by other government agencies, universities and research facilities. During the 1970s, DARPA also funded the development of a "network of networks;" this became known as the Internet, and the protocols that allowed the networks to intercommunicate became known as Internet protocols (IP).

As part of the ARPANET development work contracted to the University of California at Los Angeles (UCLA), Dr. Jon Postel, then a graduate student at the university, undertook the maintenance of a list of host names and addresses and also a list of documents prepared by ARPANET researchers, called Requests for Comments (RFCs). The lists and the RFCs were made available to the network community through the auspices of SRI International, under contract to DARPA and later the Defense Communication Agency (DCA) (now the Defense Information Systems Agency (DISA)) for performing the functions of the Network Information Center (the NIC).

After Dr. Postel moved from UCLA to the Information Sciences Institute (ISI) at the University of Southern California (USC), he continued to maintain the list of assigned Internet numbers and names under contracts with DARPA. SRI International continued to publish the lists. As the lists grew, DARPA permitted Dr. Postel to delegate additional administrative aspects of the list maintenance to SRI, under continuing technical oversight. Dr. Postel, under the DARPA contracts, also published a list of technical parameters that had been assigned for use by protocol developers. Eventually these functions collectively became known as the Internet Assigned Numbers Authority (IANA).

Until the early 1980s, the Internet was managed by DARPA, and used primarily for research purposes. Nonetheless, the task of maintaining the name list became onerous, and the Domain Name System (DNS) was developed to improve the process. Dr. Postel and SRI participated in DARPA's development and establishment of the technology and practices used by the DNS. By 1990, ARPANET was completely phased out.

The National Science Foundation (NSF) has statutory authority for supporting and strengthening basic scientific research, engineering, and educational activities in the United States, including the maintenance of computer networks to connect research and educational institutions. Beginning in 1987, IBM, MCI and Merit developed NSFNET, a national high-speed network based on Internet protocols, under an award from NSF. NSFNET, the largest of the governmental networks, provided a "backbone" to connect other networks serving more than 4,000 research and educational institutions throughout the country. The National Aeronautics and Space Administration (NASA) and the U.S. Department of Energy also contributed backbone facilities.

In 1991-92, NSF assumed responsibility for coordinating and funding the management of the non-military portion of the Internet infrastructure. NSF solicited competitive proposals to provide a variety of infrastructure services, including domain name registration services. On December 31, 1992, NSF entered into a cooperative agreement with Network Solutions, Inc. (NSI) for some of these services, including the domain name registration services. Since that time, NSI has managed key registration, coordination, and maintenance functions of the Internet domain name system. NSI registers domain names in the generic top level domains (gTLDs) on a first come, first served basis and also maintains a directory linking domain names with the IP numbers of domain name servers. NSI also currently maintains the authoritative database of Internet registrations.

In 1992, the U.S. Congress gave NSF statutory authority to allow commercial activity on the NSFNET.[(5)] This facilitated connections between NSFNET and newly forming commercial network service providers, paving the way for today's Internet. Thus, the U.S. Government has

played a pivotal role in creating the Internet as we know it today. The U.S. Government consistently encouraged bottom-up development of networking technologies, and throughout the course of its development, computer scientists from around the world have enriched the Internet and facilitated exploitation of its true potential. For example, scientists at CERN, in Switzerland, developed software, protocols and conventions that formed the basis of today's vibrant World Wide Web. This type of pioneering Internet research and development continues in cooperative organizations and consortia throughout the world.

DNS Management Today:

In recent years, commercial use of the Internet has expanded rapidly. As a legacy, however, major components of the domain name system are still performed by, or subject to, agreements with agencies of the U.S. Government.

Every Internet computer has a unique IP number. IANA, headed by Dr. Jon Postel, coordinates this system by allocating blocks of numerical addresses to regional IP registries (ARIN in North America, RIPE in Europe, and APNIC in the Asia/Pacific region), under contract with DARPA. In turn, larger Internet service providers apply to the regional IP registries for blocks of IP addresses. The recipients of those address blocks then reassign addresses to smaller Internet service providers and to end users.

- 1) Assignment of numerical addresses to Internet users.

The domain name space is constructed as a hierarchy. It is divided into top-level domains (TLDs), with each TLD then divided into second-level domains (SLDs), and so on. More than 200 national, or country-code, TLDs (ccTLDs) are administered by their corresponding governments or by private entities with the appropriate national government's acquiescence. A small set of gTLDs do not carry any national identifier, but denote the intended function of that portion of the domain space. For example, .com was established for commercial users, .org for not-for-profit organizations, and .net for network service providers. The registration and propagation of these key gTLDs are performed by NSI, under a five-year cooperative agreement with NSF. This agreement expires on September 30, 1998.

- 2) Management of the system of registering names for Internet users.

The root server system is a set of thirteen file servers, which together contain authoritative databases listing all TLDs. Currently, NSI operates the "A" root server, which maintains the authoritative root database and replicates changes to the other root servers on a daily basis. Different organizations, including NSI, operate the other 12 root servers.[(6)] The U.S. Government plays a role in the operation of about half of the Internet's root servers. Universal name consistency on the Internet cannot be guaranteed without a set of authoritative and consistent roots. Without such consistency messages could not be routed with any certainty to

the intended addresses.

- 3) Operation of the root server system.

The Internet protocol suite, as defined by the Internet Engineering Task Force (IETF), contains many technical parameters, including protocol numbers, port numbers, autonomous system numbers, management information base object identifiers and others. The common use of these protocols by the Internet community requires that the particular values used in these fields be assigned uniquely. Currently, IANA, under contract with DARPA, makes these assignments and maintains a registry of the assigned values.

- 4) Protocol Assignment.

The Need for Change:

From its origins as a U.S.-based research vehicle, the Internet is rapidly becoming an international medium for commerce, education and communication. The traditional means of organizing its technical functions need to evolve as well. The pressures for change are coming from many different quarters:

_ There is widespread dissatisfaction about the absence of competition in domain name registration.

_ Conflicts between trademark holders and domain name holders are becoming more common. Mechanisms for resolving these conflicts are expensive and cumbersome.

_ Many commercial interests, staking their future on the successful growth of the Internet, are calling for a more formal and robust management structure.

_ An increasing percentage of Internet users reside outside of the U.S., and those stakeholders want to participate in Internet coordination.

_ As Internet names increasingly have commercial value, the decision to add new top-level domains cannot be made on an *ad hoc* basis by entities or individuals that are not formally accountable to the Internet community.

_ As the Internet becomes commercial, it becomes less appropriate for U.S. research agencies to direct and fund these functions.

-

The Internet technical community has been actively debating DNS management policy for several years. Experimental registry systems offering name registration services in an

alternative set of exclusive domains developed as early as January 1996. Although visible to only a fraction of Internet users, alternative systems such as the name.space, AlterNIC, and eDNS affiliated registries(7) contributed to the community's dialogue on the evolution of DNS administration.

In May of 1996, Dr. Postel proposed the creation of multiple, exclusive, competing top-level domain name registries. This proposal called for the introduction of up to 50 new competing domain name registries, each with the exclusive right to register names in up to three new top-level domains, for a total of 150 new TLDs. While some supported the proposal, the plan drew much criticism from the Internet technical community.(8) The paper was revised and reissued.(9) The Internet Society's (ISOC) board of trustees endorsed, in principle, the slightly revised but substantively similar version of the draft in June of 1996.

After considerable debate and redrafting failed to produce a consensus on DNS change, IANA and the Internet Society (ISOC) organized the International Ad Hoc Committee(10) (IAHC or the Ad Hoc Committee) in September 1996, to resolve DNS management issues. The World Intellectual Property Organization (WIPO) and the International Telecommunications Union (ITU) participated in the IAHC. The Federal Networking Council (FNC) participated in the early deliberations of the Ad Hoc Committee.

The IAHC issued a draft plan in December 1996 that introduced unique and thoughtful concepts for the evolution of DNS administration.(11) The final report proposed a memorandum of understanding (MoU) that would have established, initially, seven new gTLDs to be operated on a nonexclusive basis by a consortium of new private domain name registrars called the Council of Registrars (CORE).(12) Policy oversight would have been undertaken in a separate council called the Policy Oversight Committee (POC) with seats allocated to specified stakeholder groups. Further, the plan formally introduced mechanisms for resolving trademark/domain name disputes. Under the MoU, registrants for second-level domains would have been required to submit to mediation and arbitration, facilitated by WIPO, in the event of conflict with trademark holders.

Although the IAHC proposal gained support in many quarters of the Internet community, the IAHC process was criticized for its aggressive technology development and implementation schedule, for being dominated by the Internet engineering community, and for lacking participation by and input from business interests and others in the Internet community.(13) Others criticized the plan for failing to solve the competitive problems that were such a source of dissatisfaction among Internet users and for imposing unnecessary burdens on trademark holders. Although the POC responded by revising the original plan, demonstrating a commendable degree of flexibility, the proposal was not able to overcome initial criticism of both the plan and the process by which the plan was developed.(14) Important segments of the Internet community remained outside the IAHC process, criticizing it as insufficiently representative.(15)

As a result of the pressure to change DNS management, and in order to facilitate its withdrawal from DNS management, the U.S. Government, through the Department of Commerce and NTIA, sought public comment on the direction of U.S. policy with respect to DNS, issuing the Green Paper on January 30, 1998.(16) The approach outlined in the Green

Paper adopted elements of other proposals, such as the early Postel drafts and the IAHC gTLD- MoU.

Comments and Response: The following are summaries of and responses to the major comments that were received in response to NTIA's issuance of *A Proposal to Improve the Technical Management of Internet Names and Addresses*. As used herein, quantitative terms such as "some," "many," and "the majority of," reflect, roughly speaking, the proportion of comments addressing a particular issue but are not intended to summarize all comments received or the complete substance of all such comments.

1. Principles for a New System. The Green Paper set out four principles to guide the evolution of the domain name system: stability, competition, private bottom-up coordination, and representation.

Comments: In general, commenters supported these principles, in some cases highlighting the importance of one or more of the principles. For example, a number of commenters emphasized the importance of establishing a body that fully reflects the broad diversity of the Internet community. Others stressed the need to preserve the bottom-up tradition of Internet governance. A limited number of commenters proposed additional principles for the new system, including principles related to the protection of human rights, free speech, open communication, and the preservation of the Internet as a public trust. Finally, some commenters who agreed that Internet stability is an important principle, nonetheless objected to the U.S. Government's assertion of any participatory role in ensuring such stability.

Response: The U.S. Government policy applies only to management of Internet names and addresses and does not set out a system of Internet "governance." Existing human rights and free speech protections will not be disturbed and, therefore, need not be specifically included in the core principles for DNS management. In addition, this policy is not intended to displace other legal regimes (international law, competition law, tax law and principles of international taxation, intellectual property law, etc.) that may already apply. The continued applicability of these systems as well as the principle of representation should ensure that DNS management proceeds in the interest of the Internet community as a whole. Finally, the U.S. Government believes that it would be irresponsible to withdraw from its existing management role without taking steps to ensure the stability of the Internet during its transition to private sector management. On balance, the comments did not present any consensus for amending the principles outlined in the Green Paper.

2. The Coordinated Functions. The Green Paper identified four DNS functions to be performed on a coordinated, centralized basis in order to ensure that the Internet runs smoothly:

2. To oversee the operation of the Internet root server system;

3. To oversee policy for determining the circumstances under which new top level domains would be added to the root system; and

4. To coordinate the development of other technical protocol parameters as needed to maintain universal connectivity on the Internet.

- 1. To set policy for and direct the allocation of IP number blocks;

Comments: Most commenters agreed that these functions should be coordinated centrally, although a few argued that a system of authoritative roots is not technically necessary to ensure DNS stability. A number of commenters, however, noted that the fourth function, as delineated in the Green Paper, overstated the functions currently performed by IANA, attributing to it central management over an expanded set of functions, some of which are now carried out by the IETF.

Response: In order to preserve universal connectivity and the smooth operation of the Internet, the U.S. Government continues to believe, along with most commenters, that these four functions should be coordinated. In the absence of an authoritative root system, the potential for name collisions among competing sources for the same domain name could undermine the smooth functioning and stability of the Internet.

The Green Paper was not, however, intended to expand the responsibilities associated with Internet protocols beyond those currently performed by IANA. Specifically, management of DNS by the new corporation does not encompass the development of Internet technical parameters for other purposes by other organizations such as IETF. The fourth function should be restated accordingly:

- · to coordinate the assignment of other Internet technical parameters as needed to maintain universal connectivity on the Internet.

3. Separation of Name and Number Authority.

Comments: A number of commenters suggested that management of the domain name system should be separated from management of the IP number system. These commenters expressed the view that the numbering system is relatively technical and straightforward. They feared that tight linkage of domain name and IP number policy development would embroil the IP numbering system in the kind of controversy that has surrounded domain name issuance in recent months. These commenters also expressed concern that the development of alternative name and number systems could be inhibited by this controversy or delayed by those with vested interests in the existing system.

Response: The concerns expressed by the commenters are legitimate, but domain names and IP numbers must ultimately be coordinated to preserve universal connectivity on the Internet. Also, there are significant costs associated with establishing and operating two separate management entities.

However, there are organizational structures that could minimize the risks identified by commenters. For example, separate name and number councils could be formed within a single organization. Policy could be determined within the appropriate council that would submit its recommendations to the new corporation's Board of Directors for ratification.

4. Creation of the New Corporation and Management of the DNS. The Green Paper called for the creation of a new private, not-for-profit corporation(17) responsible for coordinating specific DNS functions for the benefit of the Internet as a whole. Under the Green Paper proposal, the U.S. Government(18) would gradually transfer these functions to the new corporation beginning as soon as possible, with the goal of having the new corporation carry out operational responsibility by October 1998. Under the Green Paper proposal, the U.S. Government would continue to participate in policy oversight until such time as the new corporation was established and stable, phasing out as soon as possible, but in no event later than September 30, 2000. The Green Paper suggested that the new corporation be incorporated in the United States in order to promote stability and facilitate the continued reliance on technical expertise residing in the United States, including IANA staff at USC/ISI.

Comments: Almost all commenters supported the creation of a new, private not-for-profit corporation to manage DNS. Many suggested that IANA should evolve into the new corporation. A small number of commenters asserted that the U.S. Government should continue to manage Internet names and addresses. Another small number of commenters suggested that DNS should be managed by international governmental institutions such as the United Nations or the International Telecommunications Union. Many commenters urged the U.S. Government to commit to a more aggressive timeline for the new corporation's assumption of management responsibility. Some commenters also suggested that the proposal to headquarter the new corporation in the United States represented an inappropriate attempt to impose U.S. law on the Internet as a whole.

Response: The U.S. Government is committed to a transition that will allow the private sector to take leadership for DNS management. Most commenters shared this goal. While international organizations may provide specific expertise or act as advisors to the new corporation, the U.S. continues to believe, as do most commenters, that neither national governments acting as sovereigns nor intergovernmental organizations acting as representatives of governments should participate in management of Internet names and addresses. Of course, national governments now have, and will continue to have, authority to manage or establish policy for their own ccTLDs.

The U.S. Government would prefer that this transition be complete before the year 2000. To the extent that the new corporation is established and operationally stable, September 30, 2000 is intended to be, and remains, an "outside" date.

IANA has functioned as a government contractor, albeit with considerable latitude, for some time now. Moreover, IANA is not formally organized or constituted. It describes a function more than an entity, and as such does not currently provide a legal foundation for the new corporation. This is not to say, however, that IANA could not be reconstituted by a broad-based, representative group of Internet stakeholders or that individuals associated with IANA should not themselves play important foundation roles in the formation of the new corporation. We believe, and many commenters also suggested, that the private sector

organizers will want Dr. Postel and other IANA staff to be involved in the creation of the new corporation.

Because of the significant U.S.-based DNS expertise and in order to preserve stability, it makes sense to headquarter the new corporation in the United States. Further, the mere fact that the new corporation would be incorporated in the United States would not remove it from the jurisdiction of other nations. Finally, we note that the new corporation must be headquartered somewhere, and similar objections would inevitably arise if it were incorporated in another location.

5. Structure of the New Corporation. The Green Paper proposed a 15-member Board, consisting of three representatives of regional number registries, two members designated by the Internet Architecture Board (IAB), two members representing domain name registries and domain name registrars, seven members representing Internet users, and the Chief Executive Officer of the new corporation.

Comments: Commenters expressed a variety of positions on the composition of the Board of Directors for the new corporation. In general, however, most commenters supported the establishment of a Board of Directors that would be representative of the functional and geographic diversity of the Internet. For the most part, commenters agreed that the groups listed in the Green Paper included individuals and entities likely to be materially affected by changes in DNS. Most of those who criticized the proposed allocation of Board seats called for increased representation of their particular interest group on the Board of Directors. Specifically, a number of commenters suggested that the allocation set forth in the Green Paper did not adequately reflect the special interests of (1) trademark holders, (2) Internet service providers, or (3) the not-for-profit community. Others commented that the Green Paper did not adequately ensure that the Board would be globally representative.

Response: The Green Paper attempted to describe a manageably sized Board of Directors that reflected the diversity of the Internet. It is probably impossible to allocate Board seats in a way that satisfies all parties concerned. On balance, we believe the concerns raised about the representation of specific groups are best addressed by a thoughtful allocation of the "user" seats as determined by the organizers of the new corporation and its Board of Directors, as discussed below.

The Green Paper identified several international membership associations and organizations to designate Board members such as APNIC, ARIN, RIPE, and the Internet Architecture Board. We continue to believe that as use of the Internet expands outside the United States, it is increasingly likely that a properly open and transparent DNS management entity will have board members from around the world. Although we do not set any mandatory minimums for global representation, this policy statement is designed to identify global representativeness as an important priority.

6. Registrars and Registries. The Green Paper proposed moving the system for registering second level domains and the management of generic top-level domains into a competitive environment by creating two market-driven businesses, registration of second level domain names and the management of gTLD registries.

a. Competitive Registrars. Comments: Commenters strongly supported establishment of a

competitive registrar system whereby registrars would obtain domain names for customers in any gTLD. Few disagreed with this position. The Green Paper proposed a set of requirements to be imposed by the new corporation on all would-be registrars. Commenters for the most part did not take exception to the proposed criteria, but a number of commenters suggested that it was inappropriate for the United States government to establish them.

Response: In response to the comments received, the U.S. Government believes that the new corporation, rather than the U.S. Government, should establish minimum criteria for registrars that are pro-competitive and provide some measure of stability for Internet users without being so onerous as to prevent entry by would-be domain name registrars from around the world. Accordingly, the proposed criteria are not part of this policy statement.

b. Competitive Registries. Comments: Many commenters voiced strong opposition to the idea of competitive and/or for-profit domain name registries, citing one of several concerns. Some suggested that top level domain names are not, by nature, ever truly generic. As such, they will tend to function as "natural monopolies" and should be regulated as a public trust and operated for the benefit of the Internet community as a whole. Others suggested that even if competition initially exists among various domain name registries, lack of portability in the naming systems would create lock-in and switching costs, making competition unsustainable in the long run. Finally, other commenters suggested that no new registry could compete meaningfully with NSI unless all domain name registries were not-for-profit and/or noncompeting.

Some commenters asserted that an experiment involving the creation of additional for-profit registries would be too risky, and irreversible once undertaken. A related concern raised by commenters addressed the rights that for-profit operators might assert with respect to the information contained in registries they operate. These commenters argued that registries would have inadequate incentives to abide by DNS policies and procedures unless the new corporation could terminate a particular entity's license to operate a registry. For-profit operators, under this line of reasoning, would be more likely to disrupt the Internet by resisting license terminations.

Commenters who supported competitive registries conceded that, in the absence of domain name portability, domain name registries could impose switching costs on users who change domain name registries. They cautioned, however, that it would be premature to conclude that switching costs provide a sufficient basis for precluding the proposed move to competitive domain name registries and cited a number of factors that could protect against registry opportunism. These commenters concluded that the potential benefits to customers from enhanced competition outweighed the risk of such opportunism. The responses to the Green Paper also included public comments on the proposed criteria for registries.

Response: Both sides of this argument have considerable merit. It is possible that additional discussion and information will shed light on this issue, and therefore, as discussed below, the U.S. Government has concluded that the issue should be left for further consideration and final action by the new corporation. The U.S. Government is of the view, however, that competitive systems generally result in greater innovation, consumer choice, and satisfaction in the long run. Moreover, the pressure of competition is likely to be the most effective means of discouraging registries from acting monopolistically. Further, in response to the comments

received, the U.S. government believes that new corporation should establish and implement appropriate criteria for gTLD registries. Accordingly, the proposed criteria are not part of this policy statement.

7. The Creation of New gTLDs. The Green Paper suggested that during the period of transition to the new corporation, the U.S. Government, in cooperation with IANA, would undertake a process to add up to five new gTLDs to the authoritative root. Noting that formation of the new corporation would involve some delay, the Green Paper contemplated new gTLDs in the short term to enhance competition and provide information to the technical community and to policy makers, while offering entities that wished to enter into the registry business an opportunity to begin offering service to customers. The Green Paper, however, noted that ideally the addition of new TLDs would be left to the new corporation.

Comments: The comments evidenced very strong support for limiting government involvement during the transition period on the matter of adding new gTLDs. Specifically, most commenters -- both U.S. and non-U.S.-- suggested that it would be more appropriate for the new, globally representative, corporation to decide these issues once it is up and running. Few believed that speed should outweigh process considerations in this matter. Others warned, however, that relegating this contentious decision to a new and untested entity early in its development could fracture the organization. Others argued that the market for a large or unlimited number of new gTLDs should be opened immediately. They asserted that there are no technical impediments to the addition of a host of gTLDs, and the market will decide which TLDs succeed and which do not. Further, they pointed out that there are no artificial or arbitrary limits in other media on the number of places in which trademark holders must defend against dilution.

Response: The challenge of deciding policy for the addition of new domains will be formidable. We agree with the many commenters who said that the new corporation would be the most appropriate body to make these decisions based on global input. Accordingly, as supported by the preponderance of comments, the U.S. Government will not implement new gTLDs at this time.

At least in the short run, a prudent concern for the stability of the system suggests that expansion of gTLDs proceed at a deliberate and controlled pace to allow for evaluation of the impact of the new gTLDs and well-reasoned evolution of the domain space. New top level domains could be created to enhance competition and to enable the new corporation to evaluate the functioning, in the new environment, of the root server system and the software systems that enable shared registration.

8. The Trademark Dilemma. When a trademark is used as a domain name without the trademark owner's consent, consumers may be misled about the source of the product or service offered on the Internet, and trademark owners may not be able to protect their rights without very expensive litigation. For cyberspace to function as an effective commercial market, businesses must have confidence that their trademarks can be protected. On the other hand, management of the Internet must respond to the needs of the Internet community as a whole, and not trademark owners exclusively. The Green Paper proposed a number of steps to balance the needs of domain name holders with the legitimate concerns of trademark owners in the interest of the Internet community as a whole. The proposals were designed to provide trademark holders with the same rights they have in the physical world, to ensure transparency, and to guarantee a dispute resolution mechanism with resort to a court system.

The Green Paper also noted that trademark holders have expressed concern that domain name registrants in faraway places may be able to infringe their rights with no convenient jurisdiction available in which the trademark owner could enforce a judgment protecting those rights. The Green Paper solicited comments on an arrangement whereby, at the time of registration, registrants would agree to submit a contested domain name to the jurisdiction of the courts where the registry is domiciled, where the registry database is maintained, or where the "A" root server is maintained.

Comments: Commenters largely agreed that domain name registries should maintain up-to-date, readily searchable domain name databases that contain the information necessary to locate a domain name holder. In general commenters did not take specific issue with the database specifications proposed in Appendix 2 of the Green Paper, although some commenters proposed additional requirements. A few commenters noted, however, that privacy issues should be considered in this context.

A number of commenters objected to NSI's current business practice of allowing registrants to use domain names before they have actually paid any registration fees. These commenters pointed out that this practice has encouraged cybersquatters and increased the number of conflicts between domain name holders and trademark holders. They suggested that domain name applicants should be required to pay before a desired domain name becomes available for use.

Most commenters also favored creation of an on-line dispute resolution mechanism to provide inexpensive and efficient alternatives to litigation for resolving disputes between trademark owners and domain name registrants. The Green Paper contemplated that each registry would establish specified minimum dispute resolution procedures, but remain free to establish additional trademark protection and dispute resolution mechanisms. Most commenters did not agree with this approach, favoring instead a uniform approach to resolving trademark/domain name disputes.

Some commenters noted that temporary suspension of a domain name in the event of an objection by a trademark holder within a specified period of time after registration would significantly extend trademark holders' rights beyond what is accorded in the real world. They argued that such a provision would create a de facto waiting period for name use, as holders would need to suspend the use of their name until after the objection window had passed to forestall an interruption in service. Further, they argue that such a system could be used anti-competitively to stall a competitor's entry into the marketplace.

The suggestion that domain name registrants be required to agree at the time of registration to submit disputed domain names to the jurisdiction of specified courts was supported by U.S. trademark holders but drew strong protest from trademark holders and domain name registrants outside the United States. A number of commenters characterized this as an inappropriate attempt to establish U.S. trademark law as the law of the Internet. Others suggested that existing jurisdictional arrangements are satisfactory. They argue that establishing a mechanism whereby the judgment of a court can be enforced absent personal jurisdiction over the infringer would upset the balance between the interests of trademark holders and those of other members of the Internet community.

Response: The U.S. Government will seek international support to call upon the World Intellectual Property Organization (WIPO) to initiate a balanced and transparent process, which includes the participation of trademark holders and members of the Internet community who are not trademark holders, to (1) develop recommendations for a uniform approach to resolving trademark/domain name disputes involving cyberpiracy (as opposed to conflicts between trademark holders with legitimate competing rights), (2) recommend a process for protecting famous trademarks in the generic top level domains, and (3) evaluate the effects, based on studies conducted by independent organizations, such as the National Research Council of the National Academy of Sciences, of adding new gTLDs and related dispute resolution procedures on trademark and intellectual property holders. These findings and recommendations could be submitted to the board of the new corporation for its consideration in conjunction with its development of registry and registrar policy and the creation and introduction of new gTLDs.

In trademark/domain name conflicts, there are issues of jurisdiction over the domain name in controversy and jurisdiction over the legal persons (the trademark holder and the domain name holder). This document does not attempt to resolve questions of personal jurisdiction in trademark/domain name conflicts. The legal issues are numerous, involving contract, conflict of laws, trademark, and other questions. In addition, determining how these various legal principles will be applied to the borderless Internet with an unlimited possibility of factual scenarios will require a great deal of thought and deliberation. Obtaining agreement by the parties that jurisdiction over the domain name will be exercised by an alternative dispute resolution body is likely to be at least somewhat less controversial than agreement that the parties will subject themselves to the personal jurisdiction of a particular national court. Thus, the references to jurisdiction in this policy statement are limited to jurisdiction over the domain name in dispute, and not to the domain name holder.

In order to strike a balance between those commenters who thought that registrars and registries should not themselves be engaged in disputes between trademark owners and domain name holders and those commenters who thought that trademark owners should have access to a reliable and up-to-date database, we believe that a database should be maintained that permits trademark owners to obtain the contact information necessary to protect their trademarks.

Further, it should be clear that whatever dispute resolution mechanism is put in place by the new corporation, that mechanism should be directed toward disputes about cybersquatting and cyberpiracy and not to settling the disputes between two parties with legitimate competing interests in a particular mark. Where legitimate competing rights are concerned, disputes are rightly settled in an appropriate court.

Under the revised plan, we recommend that domain name holders agree to submit infringing domain names to the jurisdiction of a court where the "A" root server is maintained, where the registry is domiciled, where the registry database is maintained, or where the registrar is domiciled. We believe that allowing trademark infringement suits to be brought wherever registrars and registries are located will help ensure that all trademark holders - both U.S. and non-U.S. - have the opportunity to bring suits in a convenient jurisdiction and enforce the judgments of those courts.

Under the revised plan, we also recommend that, whatever options are chosen by the new corporation, each registrar should insist that payment be made for the domain name before it becomes available to the applicant. The failure to make a domain name applicant pay for its use of a domain name has encouraged cyberpirates and is a practice that should end as soon as possible.

9. Competition Concerns.

Comments: Several commenters suggested that the U.S. Government should provide full antitrust immunity or indemnification for the new corporation. Others noted that potential antitrust liability would provide an important safeguard against institutional inflexibility and abuses of power.

Response: Applicable antitrust law will provide accountability to and protection for the international Internet community. Legal challenges and lawsuits can be expected within the normal course of business for any enterprise and the new corporation should anticipate this reality.

The Green Paper envisioned the new corporation as operating on principles similar to those of a standard-setting body. Under this model, due process requirements and other appropriate processes that ensure transparency, equity and fair play in the development of policies or practices would need to be included in the new corporation's originating documents. For example, the new corporation's activities would need to be open to all persons who are directly affected by the entity, with no undue financial barriers to participation or unreasonable restrictions on participation based on technical or other such requirements. Entities and individuals would need to be able to participate by expressing a position and its basis, having that position considered, and appealing if adversely affected. Further, the decision making process would need to reflect a balance of interests and should not be dominated by any single interest category. If the new corporation behaves this way, it should be less vulnerable to antitrust challenges.

10. The NSI Agreement.

Comments: Many commenters expressed concern about continued administration of key gTLDs by NSI. They argued that this would give NSI an unfair advantage in the marketplace and allow NSI to leverage economies of scale across their gTLD operations. Some commenters also believe the Green Paper approach would have entrenched and institutionalized NSI's dominant market position over the key domain name going forward. Further, many commenters expressed doubt that a level playing field between NSI and the new registry market entrants could emerge if NSI retained control over .com, .net, and .org.

Response: The cooperative agreement between NSI and the U.S. Government is currently in its ramp down period. The U.S. Government and NSI will shortly commence discussions about the terms and conditions governing the ramp-down of the cooperative agreement. Through these discussions, the U.S. Government expects NSI to agree to take specific actions, including commitments as to pricing and equal access, designed to permit the development of

competition in domain name registration and to approximate what would be expected in the presence of marketplace competition. The U.S. Government expects NSI to agree to act in a manner consistent with this policy statement, including recognizing the role of the new corporation to establish and implement DNS policy and to establish terms (including licensing terms) applicable to new and existing gTLD registries under which registries, registrars and gTLDs are permitted to operate. Further, the U.S. Government expects NSI to agree to make available on an ongoing basis appropriate databases, software, documentation thereof, technical expertise, and other intellectual property for DNS management and shared registration of domain names.

11. A Global Perspective

Comments: A number of commenters expressed concern that the Green Paper did not go far enough in globalizing the administration of the domain name system. Some believed that international organizations should have a role in administering the DNS. Others complained that incorporating the new corporation in the United States would entrench control over the Internet with the U.S. Government. Still others believed that the awarding by the U.S. Government of up to five new gTLDs would enforce the existing dominance of U.S. entities over the gTLD system.

Response: The U.S. Government believes that the Internet is a global medium and that its technical management should fully reflect the global diversity of Internet users. We recognize the need for and fully support mechanisms that would ensure international input into the management of the domain name system. In withdrawing the U.S. Government from DNS management and promoting the establishment of a new, non-governmental entity to manage Internet names and addresses, a key U.S. Government objective has been to ensure that the increasingly global Internet user community has a voice in decisions affecting the Internet's technical management.

We believe this process has reflected our commitment. Many of the comments on the Green Paper were filed by foreign entities, including governments. Our dialogue has been open to all Internet users - foreign and domestic, government and private - during this process, and we will continue to consult with the international community as we begin to implement the transition plan outlined in this paper.

12. The Intellectual Infrastructure Fund.

In 1995, NSF authorized NSI to assess domain name registrants a $50 fee per year for the first two years, 30 percent of which was to be deposited in the Intellectual Infrastructure Fund (IIF), a fund to be used for the preservation and enhancement of the intellectual infrastructure of the Internet.

Comments: Very few comments referenced the IIF. In general, the comments received on the issue supported either refunding the IIF portion of the domain name registration fee to domain registrants from whom it had been collected or applying the funds toward Internet infrastructure development projects generally, including funding the establishment of the new corporation.

Response: As proposed in the Green Paper, allocation of a portion of domain name registration fees to this fund terminated as of March 31, 1998. NSI has reduced its registration fees accordingly. The IIF remains the subject of litigation. The U.S. Government takes the position that its collection has recently been ratified by the U.S. Congress,(19)

and has moved to dismiss the claim that it was unlawfully collected. This matter has not been finally resolved, however.

13. The .us Domain.

At present, the IANA administers .us as a locality-based hierarchy in which second-level domain space is allocated to states and U.S. territories.(20) This name space is further subdivided into localities. General registration under localities is performed on an exclusive basis by private firms that have requested delegation from IANA. The .us name space has typically been used by branches of state and local governments, although some commercial names have been assigned. Where registration for a locality has not been delegated, the IANA itself serves as the registrar.

Comments: Many commenters suggested that the pressure for unique identifiers in the .com gTLD could be relieved if commercial use of the .us space was encouraged. Commercial users and trademark holders, however, find the current locality-based system too cumbersome and complicated for commercial use. They called for expanded use of the .us TLD to alleviate some of the pressure for new generic TLDs and reduce conflicts between American companies and others vying for the same domain name. Most commenters support an evolution of the .us domain designed to make this name space more attractive to commercial users.

Response: Clearly, there is much opportunity for enhancing the .us domain space, and .us could be expanded in many ways without displacing the current structure. Over the next few months, the U.S. Government will work with the private sector and state and local governments to determine how best to make the .us domain more attractive to commercial users. Accordingly, the Department of Commerce will seek public input on this important issue.

ADMINISTRATIVE LAW REQUIREMENTS:

On February 20, 1998, NTIA published for public comment a proposed rule regarding the domain name registration system. That proposed rule sought comment on substantive regulatory provisions, including but not limited to a variety of specific requirements for the membership of the new corporation, the creation during a transition period of a specified number of new generic top level domains and minimum dispute resolution and other procedures related to trademarks. As discussed elsewhere in this document, in response to public comment these aspects of the original proposal have been eliminated. In light of the public comment and the changes to the proposal made as a result, as well as the continued rapid technological development of the Internet, the Department of Commerce has determined that it should issue a general statement of policy, rather than define or impose a substantive regulatory regime for the domain name system. As such, this policy statement is not a

substantive rule, does not contain mandatory provisions and does not itself have the force and effect of law.

The Assistant General Counsel for Legislation and Regulation, Department of Commerce, certified to the Chief Counsel for Advocacy, Small Business Administration, that, for purposes of the Regulatory Flexibility Act, 5 U.S.C. §§ 601 et seq., the proposed rule on this matter, if adopted, would not have a significant economic impact on a substantial number of small entities. The factual basis for this certification was published along with the proposed rule. No comments were received regarding this certification. As such, and because this final rule is a general statement of policy, no final regulatory flexibility analysis has been prepared.

This general statement of policy does not contain any reporting or record keeping requirements subject to the Paperwork Reduction Act, 44 U.S.C. ch. 35 (PRA). However, at the time the U.S. Government might seek to enter into agreements as described in this policy statement, a determination will be made as to whether any reporting or record keeping requirements subject to the PRA are being implemented. If so, the NTIA will, at that time, seek approval under the PRA for such requirement(s) from the Office of Management and Budget.

This statement has been determined to be not significant for purposes of Office of Management and Budget review under Executive Order 12866, entitled Regulatory Planning and Review.

REVISED POLICY STATEMENT:

This document provides the U.S. Government's policy regarding the privatization of the domain name system in a manner that allows for the development of robust competition and that facilitates global participation in the management of Internet names and addresses.

The policy that follows does not propose a monolithic structure for Internet governance. We doubt that the Internet should be governed by one plan or one body or even by a series of plans and bodies. Rather, we seek a stable process to address the narrow issues of management and administration of Internet names and numbers on an ongoing basis.

As set out below, the U.S. Government is prepared to recognize, by entering into agreement with, and to seek international support for, a new, not-for-profit corporation formed by private sector Internet stakeholders to administer policy for the Internet name and address system. Under such agreement(s) or understanding(s), the new corporation would undertake various responsibilities for the administration of the domain name system now performed by or on behalf of the U.S. Government or by third parties under arrangements or agreements with the U.S. Government. The U.S. Government would also ensure that the new corporation has appropriate access to needed databases and software developed under those agreements.

The Coordinated Functions

Management of number addresses is best done on a coordinated basis. Internet numbers are a unique, and at least currently, a limited resource. As technology evolves, changes may be

needed in the number allocation system. These changes should also be coordinated.

Similarly, coordination of the root server network is necessary if the whole system is to work smoothly. While day-to-day operational tasks, such as the actual operation and maintenance of the Internet root servers, can be dispersed, overall policy guidance and control of the TLDs and the Internet root server system should be vested in a single organization that is representative of Internet users around the globe.

Further, changes made in the administration or the number of gTLDs contained in the authoritative root system will have considerable impact on Internet users throughout the world. In order to promote continuity and reasonable predictability in functions related to the root zone, the development of policies for the addition, allocation, and management of gTLDs and the establishment of domain name registries and domain name registrars to host gTLDs should be coordinated.

Finally, coordinated maintenance and dissemination of the protocol parameters for Internet addressing will best preserve the stability and interconnectivity of the Internet. We are not, however, proposing to expand the functional responsibilities of the new corporation beyond those exercised by IANA currently.

In order to facilitate the needed coordination, Internet stakeholders are invited to work together to form a new, private, not-for-profit corporation to manage DNS functions. The following discussion reflects current U.S. Government views of the characteristics of an appropriate management entity. What follows is designed to describe the characteristics of an appropriate entity generally.

Principles for a New System. In making a decision to enter into an agreement to establish a process to transfer current U.S. government management of DNS to such a new entity, the U.S. will be guided by, and consider the proposed entity's commitment to, the following principles:

The U.S. Government should end its role in the Internet number and name address system in a manner that ensures the stability of the Internet. The introduction of a new management system should not disrupt current operations or create competing root systems. During the transition and thereafter, the stability of the Internet should be the first priority of any DNS management system. Security and reliability of the DNS are important aspects of stability, and as a new DNS management system is introduced, a comprehensive security strategy should be developed.

2. Competition.

The Internet succeeds in great measure because it is a decentralized system that encourages innovation and maximizes individual freedom. Where possible, market mechanisms that support competition and consumer choice should drive the management of the Internet because they will lower costs, promote innovation, encourage diversity, and enhance user choice and satisfaction.

3. Private, Bottom-Up Coordination.

Certain management functions require coordination. In these cases, responsible, private-sector action is preferable to government control. A private coordinating process is likely to be more flexible than government and to move rapidly enough to meet the changing needs of the Internet and of Internet users. The private process should, as far as possible, reflect the bottom-up governance that has characterized development of the Internet to date.

4. Representation.

The new corporation should operate as a private entity for the benefit of the Internet community as a whole. The development of sound, fair, and widely accepted policies for the management of DNS will depend on input from the broad and growing community of Internet users. Management structures should reflect the functional and geographic diversity of the Internet and its users. Mechanisms should be established to ensure international participation in decision making.

- 1. Stability

Purpose. The new corporation ultimately should have the authority to manage and perform a specific set of functions related to coordination of the domain name system, including the authority necessary to:

2) oversee operation of the authoritative Internet root server system;

3) oversee policy for determining the circumstances under which new TLDs are added to the root system; and

4) coordinate the assignment of other Internet technical parameters as needed to maintain universal connectivity on the Internet.

- 1) set policy for and direct allocation of IP number blocks to regional Internet number registries;

Funding. Once established, the new corporation could be funded by domain name registries, regional IP registries, or other entities identified by the Board.

Staff. We anticipate that the new corporation would want to make arrangements with current IANA staff to provide continuity and expertise over the course of transition. The new corporation should secure necessary expertise to bring rigorous management to the organization.

Incorporation. We anticipate that the new corporation's organizers will include representatives of regional Internet number registries, Internet engineers and computer scientists, domain name registries, domain name registrars, commercial and noncommercial users, Internet service providers, international trademark holders and Internet experts highly respected throughout the international Internet community. These incorporators should include substantial representation from around the world.

As these functions are now performed in the United States, by U.S. residents, and to ensure stability, the new corporation should be headquartered in the United States, and incorporated in the U.S. as a not-for-profit corporation. It should, however, have a board of directors from around the world. Moreover, incorporation in the United States is not intended to supplant or displace the laws of other countries where applicable.

Structure. The Internet community is already global and diverse and likely to become more so over time. The organization and its board should derive legitimacy from the participation of key stakeholders. Since the organization will be concerned mainly with numbers, names and protocols, its board should represent membership organizations in each of these areas, as well as the direct interests of Internet users.

The Board of Directors for the new corporation should be balanced to equitably represent the interests of IP number registries, domain name registries, domain name registrars, the technical community, Internet service providers (ISPs), and Internet users (commercial, not-for-profit, and individuals) from around the world. Since these constituencies are international, we would expect the board of directors to be broadly representative of the global Internet community.

As outlined in appropriate organizational documents, (Charter, Bylaws, etc.) the new corporation should:

2) direct the Interim Board to establish a system for electing a Board of Directors for the new corporation that insures that the new corporation's Board of Directors reflects the geographical and functional diversity of the Internet, and is sufficiently flexible to permit evolution to reflect changes in the constituency of Internet stakeholders. Nominations to the Board of Directors should preserve, as much as possible, the tradition of bottom-up governance of the Internet, and Board Members should be elected from membership or other associations open to all or through other mechanisms that ensure broad representation and participation in the election process.

3) direct the Interim Board to develop policies for the addition of TLDs, and establish the qualifications for domain name registries and domain name registrars within the system.

4) restrict official government representation on the Board of Directors without precluding governments and intergovernmental organizations from participating as Internet users or in a non-voting advisory capacity.

- 1) appoint, on an interim basis, an initial Board of Directors (an Interim Board) consisting of individuals representing the functional and geographic diversity of the

Internet community. The Interim Board would likely need access to legal counsel with expertise in corporate law, competition law, intellectual property law, and emerging Internet law. The Interim Board could serve for a fixed period, until the Board of Directors is elected and installed, and we anticipate that members of the Interim Board would not themselves serve on the Board of Directors of the new corporation for a fixed period thereafter.

Governance. The organizing documents (Charter, Bylaws, etc.) should provide that the new corporation is governed on the basis of a sound and transparent decision-making process, which protects against capture by a self-interested faction, and which provides for robust, professional management of the new corporation. The new corporation could rely on separate, diverse, and robust name and number councils responsible for developing, reviewing, and recommending for the board's approval policy related to matters within each council's competence. Such councils, if developed, should also abide by rules and decision-making processes that are sound, transparent, protect against capture by a self-interested party and provide an open process for the presentation of petitions for consideration. The elected Board of Directors, however, should have final authority to approve or reject policies recommended by the councils.

Operations. The new corporation's processes should be fair, open and pro-competitive, protecting against capture by a narrow group of stakeholders. Typically this means that decision-making processes should be sound and transparent; the basis for corporate decisions should be recorded and made publicly available. Super-majority or even consensus requirements may be useful to protect against capture by a self-interested faction. The new corporation does not need any special grant of immunity from the antitrust laws so long as its policies and practices are reasonably based on, and no broader than necessary to promote the legitimate coordinating objectives of the new corporation. Finally, the commercial importance of the Internet necessitates that the operation of the DNS system, and the operation of the authoritative root server system should be secure, stable, and robust.

The new corporation's charter should provide a mechanism whereby its governing body will evolve to reflect changes in the constituency of Internet stakeholders. The new corporation could, for example, establish an open process for the presentation of petitions to expand board representation.

Trademark Issues. Trademark holders and domain name registrants and others should have access to searchable databases of registered domain names that provide information necessary to contact a domain name registrant when a conflict arises between a trademark holder and a domain name holder.(21) To this end, we anticipate that the policies established by the new corporation would provide that following information would be included in all registry databases and available to anyone with access to the Internet:

- up-to-date and historical chain of registration information for the domain name;

- a mail address for service of process;

- the date of domain name registration;

- the date that any objection to the registration of the domain name is filed; and

- any other information determined by the new corporation to be reasonably necessary to resolve disputes between domain name registrants and trademark holders expeditiously.

- - up-to-date registration and contact information;

Further, the U.S. Government recommends that the new corporation adopt policies whereby:

2) Domain name registrants would agree, at the time of registration or renewal, that in cases involving cyberpiracy or cybersquatting (as opposed to conflicts between legitimate competing rights holders), they would submit to and be bound by alternative dispute resolution systems identified by the new corporation for the purpose of resolving those conflicts. Registries and Registrars should be required to abide by decisions of the ADR system.

3) Domain name registrants would agree, at the time of registration or renewal, to abide by processes adopted by the new corporation that exclude, either pro-actively or retroactively, certain famous trademarks from being used as domain names (in one or more TLDs) except by the designated trademark holder.

4) Nothing in the domain name registration agreement or in the operation of the new corporation should limit the rights that can be asserted by a domain name registrant or trademark owner under national laws.

- 1) Domain registrants pay registration fees at the time of registration or renewal and agree to submit infringing domain names to the authority of a court of law in the jurisdiction in which the registry, registry database, registrar, or the "A" root servers are located.

THE TRANSITION

Based on the processes described above, the U.S. Government believes that certain actions should be taken to accomplish the objectives set forth above. Some of these steps must be taken by the government itself, while others will need to be taken by the private sector. For example, a new not-for-profit organization must be established by the private sector and its Interim Board chosen. Agreement must be reached between the U.S. Government and the new corporation relating to transfer of the functions currently performed by IANA. NSI and the U.S. Government must reach agreement on the terms and conditions of NSI's evolution into one competitor among many in the registrar and registry marketplaces. A process must be laid out for making the management of the root server system more robust and secure. A relationship between the U.S. Government and the new corporation must be developed to

transition DNS management to the private sector and to transfer management functions.

During the transition the U.S. Government expects to:

2) enter into agreement with the new corporation under which it assumes responsibility for management of the domain name space;

3) ask WIPO to convene an international process including individuals from the private sector and government to develop a set of recommendations for trademark/domain name dispute resolutions and other issues to be presented to the Interim Board for its consideration as soon as possible;

4) consult with the international community, including other interested governments as it makes decisions on the transfer; and

5) undertake, in cooperation with IANA, NSI, the IAB, and other relevant organizations from the public and private sector, a review of the root server system to recommend means to increase the security and professional management of the system. The recommendations of the study should be implemented as part of the transition process; and the new corporation should develop a comprehensive security strategy for DNS management and operations.

- 1) ramp down the cooperative agreement with NSI with the objective of introducing competition into the domain name space. Under the ramp down agreement NSI will agree to (a) take specific actions, including commitments as to pricing and equal access, designed to permit the development of competition in domain name registration and to approximate what would be expected in the presence of marketplace competition, (b) recognize the role of the new corporation to establish and implement DNS policy and to establish terms (including licensing terms) applicable to new and existing gTLDs and registries under which registries, registrars and gTLDs are permitted to operate, (c) make available on an ongoing basis appropriate databases, software, documentation thereof, technical expertise, and other intellectual property for DNS management and shared registration of domain names;

ENDNOTES

1. Available at <http://www.ecommerce.gov>.

2. July 2, 1997 RFC and public comments are located at: <http://www.ntia.doc.gov/ntiahome/domainname/index.html>.

3. [3]The RFC, the Green Paper, and comments received in response to both documents are available on the Internet

at the following address: <http://www.ntia.doc.gov>. Additional comments were submitted after March 23, 1998. These comments have been considered and treated as part of the official record and have been separately posted at the same site, although the comments were not received by the deadline established in the February 20, 1998 Federal Register Notice.

4. See Administrative Law Requirements at p. 19.

5. See Scientific and Advanced-Technology Act of 1992; Pub. L. 102-476 § 4(9), 106 Stat. 2297, 2300 (codified at 42 U.S.C. § 1862 (a)).

6. An unofficial diagram of the general geographic location and institutional affiliations of the 13 Internet root servers, prepared by Anthony Rutkowski, is available at <http://www.wia.org/pub/rootserv.html>.

7. For further information about these systems see: name.space: <http://namespace.pgmedia.net>; AlterNIC: <http://www.alternic.net>; eDNS: <http://www.edns.net>. Reference to these organizations does not constitute an endorsement of their commercial activities.

8. Lengthy discussions by the Internet technical community on DNS issues generally and on the Postel DNS proposal took place on the *newdom*, *com-priv*, *ietf* and *domain-policy* Internet mailing lists.

9. [9] See *draft-Postel-iana-itld-admin-01.txt*; available at <http://www.newdom.com/archive>.

10. For further information about the IAHC see: <http://www.iahc.org> and related links. Reference to this organization does not constitute an endorsement of the commercial activities of its related organizations.

11. December 1996 draft: *draft-iahc-gtldspec-00.txt*; available at <http://info.internet.isi.edu:80/in-drafts/files>.

12. The IAHC final report is available at <http://www.iahc.org/draft-iahc-recommend-00.html>.

13. See generally public comments received in response to July 2, 1997 RFC located at <http://www.ntia.doc.gov/ntiahome/domainname/email>.

14. For a discussion, see Congressional testimony of Assistant Secretary of Commerce Larry Irving, Before the House Committee on Science, Subcommittee on Basic Research, September 25, 1997 available at <http://www.ntia.doc.gov/ntiahome/domainname/email>.

15. See generally public comments received in response to July 2, 1997 RFC located at <http://www.ntia.doc.gov/ntiahome/domainname/email>.

16. [16]The document was published in the *Federal Register* on February 20, 1998, (63 Fed. Reg. 8826 (Feb. 20, 1998)).

17. As used herein, the term "new corporation" is intended to refer to an entity formally organized under well recognized and established business law standards.

18. As noted in the Summary, the President directed the Secretary of Commerce to privatize DNS in a manner that increases competition and facilitates international participation in its management. Accordingly, the Department of Commerce will lead the coordination of the U.S. government's role in this transition.

19. 1998 Supplemental Appropriations and Rescissions Act; Pub. L. 105-174; 112 Stat. 58.

20. [20] Management principles for the .us domain space are set forth in Internet RFC 1480, (http://www.isi.edu/in-notes/rfc1480.txt).

21. These databases would also benefit domain name holders by making it less expensive for new registrars and

registries to identify potential customers, enhancing competition and lowering prices.

National Telecommunications and Information Administration
Contact Information Redacted

commerce.gov | Privacy Policy | Web Policies | FOIA | Accessibility | usa.gov

---

Source URL: https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses

Links
[1] https://www.ntia.doc.gov/category/domain-name-system
[2] mailto Contact Information Redacted

EXHIBIT JMR-12

New gTLD Application Submitted to ICANN by: Afilias Domains No. 3 Limited,

String: WEB

Originally Posted: 13 June 2012

Application ID: 1-1013-6638

Applicant Information

1. Full legal name

Afilias Domains No. 3 Limited,

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact nformation Redacted

4. Fax number

Contact nformation Redacted

5. If applicable, website or URL

http://www.AfiliasDomains3.info

Primary Contact

6(a). Name

John Kane

6(b). Title

Vice President, Corporate Services

6(c). Address

6(d). Phone Number

Contact nformation Redacted

6(e). Fax Number

6(f). Email Address

Contact Information Redacted

Secondary Contact

7(a). Name

John Kane

7(b). Title

Vice President, Corporate Services

7(c). Address

7(d). Phone Number

Contact nformation Redacted

7(e). Fax Number

7(f). Email Address

Contact Informat on Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

limited liability corporation

8(b). State the specific national or other jursidiction that defines the type of entity identified in 8(a).

Republic of Ireland

8(c). Attach evidence of the applicant's establishment.

Attachments are not displayed on this form.

9(a). If applying company is publicly traded, provide the exchange and symbol.

9(b). If the applying entity is a subsidiary, provide the parent company.

Afilias Limited

9(c). If the applying entity is a joint venture, list all joint venture partners.

not a joint venture

Applicant Background

11(a). Name(s) and position(s) of all directors

M. Scott Hemphill	Director
Thomas Wade	Director

11(b). Name(s) and position(s) of all officers and partners

Thomas Wade	CFO

11(c). Name(s) and position(s) of all shareholders holding at least 15% of shares

11(d). For an applying entity that does not have directors, officers, partners, or shareholders: Name(s) and position(s) of all individuals having legal or executive responsibility

Applied-for gTLD string

13. Provide the applied-for gTLD string. If an IDN, provide the U-label.

WEB

14(a). If an IDN, provide the A-label (beginning with "xn--").

14(b). If an IDN, provide the meaning or restatement of the string in English, that is, a description of the literal meaning of the string in the opinion of the applicant.

14(c). If an IDN, provide the language of the label (in English).

14(c). If an IDN, provide the language of the label (as referenced by ISO-639-1).

14(d). If an IDN, provide the script of the label (in English).

14(d). If an IDN, provide the script of the label (as referenced by ISO 15924).

14(e). If an IDN, list all code points contained in the U-label according to Unicode form.

15(a). If an IDN, Attach IDN Tables for the proposed registry.

Attachments are not displayed on this form.

15(b). Describe the process used for development of the IDN tables submitted, including consultations and sources used.

15(c). List any variant strings to the applied-for gTLD string according to the relevant IDN tables.

16. Describe the applicant's efforts to ensure that there are no known operational or rendering problems concerning the applied-for gTLD string. If such issues are known, describe steps that will be taken to mitigate these issues in software and other applications.

Afilias anticipates the introduction of this TLD without operational or rendering problems. Based on a decade of experience launching and operating new TLDs, Afilias, the back-end provider of registry services for this TLD, is confident the launch and operation of this TLD presents no known challenges. The rationale for this opinion includes:
• The string is not complex and is represented in standard ASCII characters and follows relevant technical, operational and policy standards;
• The string length is within lengths currently supported in the root and by ubiquitous Internet programs such as web browsers and mail applications;
• There are no new standards required for the introduction of this TLD;
• No onerous requirements are being made on registrars, registrants or Internet users, and;
• The existing secure, stable and reliable Afilias SRS, DNS, WHOIS and supporting systems and staff are amply provisioned and prepared to meet the needs of this TLD.

17. (OPTIONAL) Provide a representation of the label according to the International Phonetic Alphabet (http://www.langsci.ucl.ac.uk/ipa/).

Mission/Purpose

18(a). Describe the mission/purpose of your proposed gTLD.

Afilias Domains No. 3, the Applicant, is a subsidiary of Afilias Limited, and will be referred to throughout this application as Afilias for simplicity of review by ICANN.

Mission and purpose

The goal of the .WEB TLD is to help users of the Internet establish meaningful and relevant identities while promoting themselves or their groups, companies or organizations at the same time. This TLD will open up new opportunities for individuals, businesses and organizations to garner a unique piece of the Internet in a space where they can secure the domain name they want but can't have currently.

Businesses and organizations will want to acquire a domain in the .WEB TLD:
• A professional web presence is desired to support merchandising, retailing efforts and business goals.
• Retailers may wish to obtain a .WEB domain to create websites to support or announce planned business offerings and marketing efforts in the "web" arena.
• The web is an indispensible part of virtually every individual's and business' life today.

"As of 2011, more than 2.2 billion people – nearly a third of Earth's population – uses the services of the Internet." (source: Internet World Stats, updated 31 March 2011). Considering that many of this population have heretofore been unable to get the domain name they desired because it was already taken or reserved in a .com or .net environment, the need for a new TLD with a well-established name in the industry is obvious. And nothing is as synonymous with "Internet" or "net" as the word, "web".

18(b). How do you expect that your proposed gTLD will benefit registrants, Internet users, and others?

The .WEB TLD will be positioned to become one the most-used, professional Internet spaces available.

i. General goals

.WEB will be an open TLD, generally available to all registrants (except in the Sunrise period as described below). The domains can be used for any purpose, including for business use, for personal use and by organizations. There are no content or use restrictions for this TLD.

Afilias will design and position the .WEB TLD to be one of the most popular TLDs on the Internet. The company will market, brand, provide outreach, and offer marketing support to registrars with the goal of gaining public support for the .WEB TLD. This can only be accomplished by creating a user friendly, easy to use, interesting, professionally relevant and entertaining TLD.

ii. How .WEB adds to the current space

On today's Internet, there are hundreds of thousands of companies around the world vying for the attention of potential users and customers. For this precise reason, the .WEB TLD provides an excellent opportunity for companies who elect to

participate in the domain to separate themselves from the rest of the .com and .net pack.

The .WEB TLD opens up a tremendous number of options for those companies involved with applications who wish to create a targeted identity on the Internet. In addition, it gives those companies the opportunity to build off the name recognition associated with their brand and name. Any company would be very receptive to being able to associate its own products or services with other quality products and services through the .WEB TLD.

iii. User experience goals

As is the goal of all new gTLDs, this TLD intends to create a space where registrants who desire to participate in the .WEB can create identities where potential users and clients can find the kinds of information they want and need. For example, if you are an organization or company whose business is built around use of the Internet, by belonging to this space you will be able to join forces or share information with other organizations or companies with similar interests and common goals. If an entity or group belongs to the .WEB TLD group, they can be assured they are establishing a presence on the Internet which will:
a) closely align them with similar brands,
b) ensure they can keep their own names⁄brands rather than having to “fit in” to the short list of current TLDs available,
c) facilitate ease of discovery when searched for by potential customers and users, and
d) foster confidence of users seeking any information whatsoever regarding applications because this person belongs to the .WEB.

iv. Registry policies

.WEB will be an open TLD, generally available to all registrants except during the Sunrise period.

.WEB domains will be offered for one to ten years as a general rule with a maximum period of no more than ten years. During the Sunrise period, initial registrations will likely have a minimum requirement for number of years. A requirement may be put in place during Sunrise, for example, that all names must be registered for at least five years.

The roll-out of our TLD is anticipated to feature the following phases:
• Reservation of reserved names and premium names, which will be distributed through special mechanisms (detailed below).
• Sunrise — the required period for trademark owners to secure their domains before availability to the general public. This phase will feature applications for domain strings, verification of trademarks via Trademark Clearinghouse and a trademark verification agent, auctions between qualified parties who wish to secure the same string, and a Trademark Claims Service.
• Land rush — this period provides an opportunity for potential registrations to apply for names prior to the General availability period.
• General Availability period — real-time registrations, made on a first-come first-served basis. Trademark Claims Service will be in use at least for the first 60 days after General Availability applications open.

The registration of domain names in the .WEB TLD will follow the standard practices, procedures and policies Afilias, the back-end provider of registry services, currently has in place. This includes the following:
• Domain registration policies (for example, grace periods, transfer policies,

etc.) are defined in response #27.
• Abuse prevention tools and policies, for example, measures to promote WHOIS accuracy and efforts to reduce phishing and pharming, are discussed in detail in our response #28.
• Rights protection mechanisms and dispute resolution mechanism policies (for example, UDRP, URS) are detailed in #29.

Other detailed policies for this domain include policies for reserved names.

Reserved names

Registry reserved names

We will reserve the following classes of domain names, which will not be made generally available to registrants via the Sunrise or subsequent periods:
• All of the reserved names required in Specification 5 of the new gTLD Registry Agreement;
• The geographic names required in Specification 5 of the new gTLD Registry Agreement, and may be released to the extent that Registry Operator reaches agreement with the government and country-code manager;
• The registry operator's own name and variations thereof, and registry operations names (such as registry.tld, and www.tld), for internal use;
• Names related to ICANN and Internet standards bodies (iana.tld, ietf.tld, w3c.tld, etc.), and may be released to the extent that Registry Operator reaches agreement with ICANN.

The list of reserved names will be published publicly before the Sunrise period begins, so that registrars and potential registrants will know which names have been set aside.

Premium names

The registry will also designate a set of premium domain names, set aside for distribution via special mechanisms. The list of premium names will be published publicly before the Sunrise period begins, so that registrars and potential registrants will know that these names are not available. Premium names may be distributed via mechanisms such as requests for proposals, contests, direct sales, and auctions.

For the auctioning of premium names, we intend to contract with an established auction provider that has successfully conducted domain auctions. This will ensure that there is a tested, trustworthy technical platform for the auctions, auditable records, and reliable collection mechanisms. With our chosen auction provider, we will create and post policies and procedures that ensure clear, fair, and ethical auctions. As an example of such a policy, all employees of the registry operator and its contractors will be strictly prohibited from bidding in auctions for domains in the TLD. We expect a comprehensive and robust set of auction rules to cover possible scenarios, such as how domains will be awarded if the winning bidder does not make payment.

v. Privacy and confidential information protection

As per the New gTLD Registry Agreement, we will make domain contact data (and other fields) freely and publicly available via a Web-based WHOIS server. This default set of fields includes the mandatory publication of registrant data. Our Registry-Registrar Agreement will require that registrants consent to this publication.

We shall notify each of our registrars regarding the purposes for which data about any identified or identifiable natural person ("Personal Data") submitted to the

Registry Operator by such registrar is collected and used, and the intended recipients (or categories of recipients) of such Personal Data (the data in question is essentially the registrant and contact data required to be published in the WHOIS). We will require each registrar to obtain the consent of each registrant in the TLD for the collection and use of such Personal Data. The policies will be posted publicly on our TLD web site. As the registry operator, we shall not use or authorize the use of Personal Data in any way that is incompatible with the notice provided to registrars.

Our privacy and data use policies are as follows:
• As registry operator, we do not plan on selling bulk WHOIS data. We will not sell contact data in any way. We will not allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations.
• We may use registration data in the aggregate for marketing purposes.
• DNS query data will never be sold in a way that is personally identifiable.
• We may from time to time use the demographic data collected for statistical analysis, provided that this analysis will not disclose individual Personal Data and provided that such use is compatible with the notice provided to registrars regarding the purpose and procedures for such use.

As the registry operator we shall take significant steps to protect Personal Data collected from registrars from loss, misuse, unauthorized disclosure, alteration, or destruction. In our responses to Question 30 ("Security Policy") and Question 38 ("Escrow") we detail the security policies and procedures we will use to protect the registry system and the data contained therein from unauthorized access and loss.

Please see our response to Question 26 ("WHOIS") regarding "searchable WHOIS" and rate-limiting. That section contains details about how we will limit the mining of WHOIS data by spammers and other parties who abuse access to the WHOIS.

In order to acquire and maintain accreditation for our TLD, we will require registrars to adhere to certain information technology policies designed to help protect registrant data. These will include standards for access to the registry system and password management protocols. Our response to Question 30, "Security Policy" provides details of implementation.

We will allow the use of proxy and privacy services, which can protect the personal data of registrants from spammers and other parties that mine zone files and WHOIS data. We are aware that there are parties who may use privacy services to protect their free speech rights, or to avoid religious or political persecution.

18(c). What operating rules will you adopt to eliminate or minimize social costs?

Afilias has adopted the above-mentioned and other policies to ensure fair and equitable access and cost structures to the Internet community, including:
• no new burdens placed on the Internet community to resolve name disputes
• utilization of standard registration practices and policies (as detailed in responses to questions #27, #28, #29)
• protection of trademarks at launch and on-going operations (as detailed in the response to question #29)
• fair and reasonable wholesale prices
• fair and equitable treatment of registrars

As per the ICANN Registry Agreement, we will use only ICANN-accredited registrars, and will provide non-discriminatory access to registry services to those registrars.

Pricing Policies and Commitments

Pricing for domain names at General Availability will be $8 per domain year for the first year. Applicant reserves the right to reduce this pricing for promotional purposes in a manner available to all accredited registrars. Registry Operator reserves the right to work with ICANN to initiate an increase in the wholesale price of domains if required. Registry Operator will provide reasonable notice to the registrars of any approved price increase.

Community-based Designation

19. Is the application for a community-based TLD?

No

20(a). Provide the name and full description of the community that the applicant is committing to serve.

20(b). Explain the applicant's relationship to the community identified in 20(a).

20(c). Provide a description of the community-based purpose of the applied-for gTLD.

20(d). Explain the relationship between the applied-for gTLD string and the community identified in 20(a).

20(e). Provide a description of the applicant's intended registration policies in support of the community-based purpose of the applied-for gTLD.

20(f). Attach any written endorsements from institutions/groups representative of the community identified in 20(a).

Attachments are not displayed on this form.

Geographic Names

21(a). Is the application for a geographic name?

No

Protection of Geographic Names

22. Describe proposed measures for protection of geographic names at the second and other levels in the applied-for gTLD.

We will protect names with national or geographic significance by reserving the country and territory names at the second level and at all other levels within the TLD, as per the requirements in the New TLD Registry Agreement (Specification 5, paragraph 5).

We will employ a series of rules to translate the geographical names required to be reserved by Specification 5, paragraph 5 to a form consistent with the "host names" format used in domain names.

Considering the Governmental Advisory Committee (GAC) advice "Principles regarding new gTLDs", these domains will be blocked, at no cost to governments, public authorities, or IGOs, before the TLD is introduced (Sunrise), so that no parties may apply for them. We will publish a list of these names before Sunrise, so our registrars and their prospective applicants can be aware that these names are reserved.
We will define a procedure so that governments can request the above reserved domain(s) if they would like to take possession of them. This procedure will be based on existing methodology developed for the release of country names in the .INFO TLD. For example, we will require a written request from the country's GAC representative, or a written request from the country's relevant Ministry or Department. We will allow the designated beneficiary (the Registrant) to register

the name, with an accredited Afilias Registrar, possibly using an authorization number transmitted directly to the designated beneficiary in the country concerned.

As defined by Specification 5, paragraph 5, such geographic domains may be released to the extent that Registry Operator reaches agreement with the applicable government(s). Registry operator will work with respective GAC representatives of the country's relevant Ministry of Department to obtain their release of the names to the Registry Operator.

If internationalized domains names (IDNs) are introduced in the TLD in the future, we will also reserve the IDN versions of the country names in the relevant script (s) before IDNs become available to the public. If we find it advisable and practical, we will confer with relevant language authorities so that we can reserve the IDN domains properly along with their variants.

Regarding GAC advice regarding second-level domains not specified via Specification 5, paragraph 5: All domains awarded to registrants are subject to the Uniform Domain Name Dispute Resolution Policy (UDRP), and to any properly-situated court proceeding. We will ensure appropriate procedures to allow governments, public authorities or IGO's to challenge abuses of names with national or geographic significance at the second level. In its registry-registrar agreement, and flowing down to registrar-registrant agreements, the registry operator will institute a provision to suspend domains names in the event of a dispute. We may exercise that right in the case of a dispute over a geographic name.

Registry Services

23. Provide name and full description of all the Registry Services to be provided.

Afilias Domains No. 3, the Applicant, is a subsidiary of Afilias Limited, and will be referred to throughout this application as Afilias for simplicity of review by ICANN.

Afilias has more experience successfully applying to ICANN and launching new TLDs than any other provider. Afilias is the ICANN-contracted registry operator of the .INFO and .MOBI TLDs, and Afilias is the back-end registry services provider for other ICANN TLDs including .ORG, .ASIA, .AERO, and .XXX.

Registry services for this TLD will be performed by Afilias in the same responsible manner used to support 16 top level domains today. Afilias supports more ICANN-contracted TLDs (6) than any other provider currently. Afilias' primary corporate mission is to deliver secure, stable and reliable registry services. This TLD will utilize an existing, proven team and platform for registry services with:

• A stable and secure, state-of-the-art, EPP-based SRS with ample storage capacity, data security provisions and scalability that is proven with registrars who account for over 95% of all gTLD domain name registration activity (over 375 registrars);
• A reliable, 100% available DNS service (zone file generation, publication and dissemination) tested to withstand severe DDoS attacks and dramatic growth in

Internet use;
• A WHOIS service that is flexible and standards compliant, with search capabilities to address both registrar and end-user needs; includes consideration for evolving standards, such as RESTful, or draft-kucherawy-wierds;
• Experience introducing IDNs in the following languages: German (DE), Spanish (ES), Polish (PL), Swedish (SV), Danish (DA), Hungarian (HU), Icelandic (IS), Latvian (LV), Lithuanian (LT), Korean (KO), Simplified and Traditional Chinese (CN), Devanagari (HI-DEVA), Russian (RU), Belarusian (BE), Ukrainian (UK), Bosnian (BS), Serbian (SR), Macedonian (MK) and Bulgarian (BG) across the TLDs it serves;
• A registry platform that is both IPv6 and DNSSEC enabled;
• An experienced, respected team of professionals active in standards development of innovative services such as DNSSEC and IDN support;
• Methods to limit domain abuse, remove outdated and inaccurate data, and ensure the integrity of the SRS, and;
• Customer support and reporting capabilities to meet financial and administrative needs, e.g., 24x7 call center support, integration support, billing, and daily, weekly, and monthly reporting.

Afilias will support this TLD as the registry operator, leveraging a proven registry infrastructure that is fully operational, staffed with professionals, massively provisioned, and immediately ready to launch and maintain this TLD.

The below response includes a description of the registry services to be provided for this TLD, additional services provided to support registry operations, and an overview of Afilias' approach to registry management.

Registry services to be provided

To support this TLD, Afilias will offer the following registry services, all in accordance with relevant technical standards and policies:
• Receipt of data from registrars concerning registration for domain names and nameservers, and provision to registrars of status information relating to the EPP-based domain services for registration, queries, updates, transfers, renewals, and other domain management functions. Please see our responses to questions #24, #25, and #27 for full details, which we request be incorporated here by reference.
• Operation of the registry DNS servers: The Afilias DNS system, run and managed by Afilias, is a massively provisioned DNS infrastructure that utilizes among the most sophisticated DNS architecture, hardware, software and redundant design created. Afilias' industry-leading system works in a seamless way to incorporate nameservers from any number of other secondary DNS service vendors. Please see our response to question #35 for full details, which we request be incorporated here by reference.
• Dissemination of TLD zone files: Afilias' distinctive architecture allows for real-time updates and maximum stability for zone file generation, publication and dissemination. Please see our response to question #34 for full details, which we request be incorporated here by reference.
• Dissemination of contact or other information concerning domain registrations: A port 43 WHOIS service with basic and expanded search capabilities with requisite measures to prevent abuse. Please see our response to question #26 for full details, which we request be incorporated here by reference.
• Internationalized Domain Names (IDNs): Ability to support all protocol valid Unicode characters at every level of the TLD, including alphabetic, ideographic and right-to-left scripts, in conformance with the ICANN IDN Guidelines. Please see our response to question #44 for full details, which we request be incorporated here by reference.
• DNS Security Extensions (DNSSEC): A fully DNSSEC-enabled registry, with a stable and efficient means of signing and managing zones. This includes the ability to safeguard keys and manage keys completely. Please see our response to question #43 for full details, which we request be incorporated here by reference.

Each service will meet or exceed the contract service level agreement. All registry services for this TLD will be provided in a standards-compliant manner.

Security

Afilias addresses security in every significant aspect–physical, data and network as well as process. Afilias' approach to security permeates every aspect of the registry services provided. A dedicated security function exists within the company to continually identify existing and potential threats, and to put in place comprehensive mitigation plans for each identified threat. In addition, a rapid security response plan exists to respond comprehensively to unknown or unidentified threats. The specific threats and Afilias mitigation plans are defined in our response to question #30(b); please see that response for complete information. In short, Afilias is committed to ensuring the confidentiality, integrity, and availability of all information.

New registry services

No new registry services are planned for the launch of this TLD.

Additional services to support registry operation

Numerous supporting services and functions facilitate effective management of the TLD. These support services are also supported by Afilias, including:
• Customer support: 24x7 live phone and e-mail support for customers to address any access, update or other issues they may encounter. This includes assisting the customer identification of the problem as well as solving it. Customers include registrars and the registry operator, but not registrants except in unusual circumstances. Customers have access to a web-based portal for a rapid and transparent view of the status of pending issues.
• Financial services: billing and account reconciliation for all registry services according to pricing established in respective agreements.

Reporting is an important component of supporting registry operations. Afilias will provide reporting to the registry operator and registrars, and financial reporting.

Reporting provided to registry operator

Afilias reporting provides an extensive suite of reports, including daily, weekly and monthly reports with data at the transaction level that enable us to track and reconcile at whatever level of detail preferred. Afilias provides the exact data required by ICANN in the required format to enable the registry operator to meet its technical reporting requirements to ICANN.

In addition, Afilias offers access to a data warehouse capability that will enable near real-time data to be available 24x7. Afilias' data warehouse capability enables drill-down analytics all the way to the transaction level.

Reporting available to registrars

Afilias provides an extensive suite of reporting to registrars and has been doing so in an exemplary manner for more than ten years. Specifically, Afilias provides daily, weekly and monthly reports with detail at the transaction level to enable registrars to track and reconcile at whatever level of detail they prefer.

Reports are provided in standard formats, facilitating import for use by virtually any registrar analytical tool. Registrar reports are available for download via a secure administrative interface. A given registrar will only have access to its own reports. These include the following:

• Daily Reports: Transaction Report, Billable Transactions Report, and Transfer Reports;
• Weekly: Domain Status and Nameserver Report, Weekly Nameserver Report, Domains Hosted by Nameserver Weekly Report, and;
• Monthly: Billing Report and Monthly Expiring Domains Report.

Weekly registrar reports are maintained for each registrar for four weeks. Weekly reports older than four weeks will be archived for a period of six months, after which they will be deleted.

Financial reporting

Registrar account balances are updated real-time when payments and withdrawals are posted to the registrars' accounts. In addition, the registrar account balances are updated as and when they perform billable transactions at the registry level.

Afilias provides Deposit/Withdrawal Reports that are updated periodically to reflect payments received or credits and withdrawals posted to the registrar accounts.

The following reports are also available: a) Daily Billable Transaction Report, containing details of all the billable transactions performed by all the registrars in the SRS, b) daily e-mail reports containing the number of domains in the registry and a summary of the number and types of billable transactions performed by the registrars, and c) registry operator versions of most registrar reports (for example, a daily Transfer Report that details all transfer activity between all of the registrars in the SRS).

Afilias approach to registry support

Afilias is dedicated to managing the technical operations and support of this TLD in a secure, stable and reliable manner. Afilias has reviewed specific needs and objectives of this TLD. The resulting comprehensive plans are illustrated in technical responses #24-44. Afilias has provided financial responses for this application which demonstrate cost and technology consistent with the size and objectives of this TLD.

Afilias is the registry services provider for this and several other TLD applications. Over the past 11 years of providing services for gTLD and ccTLDs, Afilias has accumulated experience about resourcing levels necessary to provide high quality services with conformance to strict service requirements. Afilias currently supports over 20 million domain names, spread across 16 TLDs, with over 400 accredited registrars.

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

With over a decade of registry experience, Afilias has the depth and breadth of experience that ensure existing and new needs are addressed, all while meeting or exceeding service level requirements and customer expectations. This is evident in Afilias' participation in business, policy and technical organizations supporting registry and Internet technology within ICANN and related organizations. This

allows Afilias to be at the forefront of security initiatives such as: DNSSEC, wherein Afilias worked with Public Interest Registry (PIR) to make the .ORG registry the first DNSSEC enabled gTLD and the largest TLD enabled at the time; in enhancing the Internet experience for users across the globe by leading development of IDNs; in pioneering the use of open-source technologies by its usage of PostgreSQL, and; being the first to offer near-real-time dissemination of DNS zone data.

The ability to observe tightening resources for critical functions and the capacity to add extra resources ahead of a threshold event are factors that Afilias is well versed in. Afilias' human resources team, along with well-established relationships with external organizations, enables it to fill both long-term and short-term resource needs expediently.

Afilias' growth from a few domains to serving 20 million domain names across 16 TLDs and 400 accredited registrars indicates that the relationship between the number of people required and the volume of domains supported is not linear. In other words, servicing 100 TLDs does not automatically require 6 times more staff than servicing 16 TLDs. Similarly, an increase in the number of domains under management does not require in a linear increase in resources. Afilias carefully tracks the relationship between resources deployed and domains to be serviced, and pro-actively reviews this metric in order to retain a safe margin of error. This enables Afilias to add, train and prepare new staff well in advance of the need, allowing consistent delivery of high quality services.

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS (THE " 〈" and "〉 " CHARACTERS), WHICH ICANN INFORMS AFILIAS (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE FULL ANSWER TO THIS QUESTION IS ATTACHED AS A PDF FILE.

Afilias operates a state-of-the-art EPP-based Shared Registration System (SRS) that is secure, stable and reliable. The SRS is a critical component of registry operations that must balance the business requirements for the registry and its customers, such as numerous domain acquisition and management functions. The SRS meets or exceeds all ICANN requirements given that Afilias:
• Operates a secure, stable and reliable SRS which updates in real-time and in full compliance with Specification 6 of the new gTLD Registry Agreement;
• Is committed to continuously enhancing our SRS to meet existing and future needs;
• Currently exceeds contractual requirements and will perform in compliance with Specification 10 of the new gTLD Registry Agreement;
• Provides SRS functionality and staff, financial, and other resources to more than adequately meet the technical needs of this TLD, and;
• Manages the SRS with a team of experienced technical professionals who can seamlessly integrate this TLD into the Afilias registry platform and support the TLD in a secure, stable and reliable manner.

Description of operation of the SRS, including diagrams

Afilias' SRS provides the same advanced functionality as that used in the .INFO and .ORG registries, as well as the fourteen other TLDs currently supported by Afilias. The Afilias registry system is standards-compliant and utilizes proven technology, ensuring global familiarity for registrars, and it is protected by our massively provisioned infrastructure that mitigates the risk of disaster.

EPP functionality is described fully in our response to question #25; please consider those answers incorporated here by reference. An abbreviated list of Afilias SRS functionality includes:
• Domain registration: Afilias provides registration of names in the TLD, in both ASCII and IDN forms, to accredited registrars via EPP and a web-based administration tool.
• Domain renewal: Afilias provides services that allow registrars the ability to renew domains under sponsorship at any time. Further, the registry performs the automated renewal of all domain names at the expiration of their term, and allows registrars to rescind automatic renewals within a specified number of days after the transaction for a full refund.
• Transfer: Afilias provides efficient and automated procedures to facilitate the transfer of sponsorship of a domain name between accredited registrars. Further, the registry enables bulk transfers of domains under the provisions of the Registry-Registrar Agreement.
• RGP and restoring deleted domain registrations: Afilias provides support for the Redemption Grace Period (RGP) as needed, enabling the restoration of deleted registrations.
• Other grace periods and conformance with ICANN guidelines: Afilias provides support for other grace periods that are evolving as standard practice inside the ICANN community. In addition, the Afilias registry system supports the evolving ICANN guidelines on IDNs.

Afilias also supports the basic check, delete, and modify commands.

As required for all new gTLDs, Afilias provides "thick" registry system functionality. In this model, all key contact details for each domain are stored in the registry. This allows better access to domain data and provides uniformity in storing the information.

Afilias' SRS complies today and will continue to comply with global best practices including relevant RFCs, ICANN requirements, and this TLD's respective domain policies. With over a decade of experience, Afilias has fully documented and tested policies and procedures, and our highly skilled team members are active participants of the major relevant technology and standards organizations, so ICANN can be assured that SRS performance and compliance are met. Full details regarding the SRS system and network architecture are provided in responses to questions #31 and #32; please consider those answers incorporated here by reference.

SRS servers and software

All applications and databases for this TLD will run in a virtual environment currently hosted by a cluster of servers equipped with the latest Intel Westmere multi-core processors. (It is possible that by the time this application is evaluated and systems deployed, Westmere processors may no longer be the "latest"; the Afilias policy is to use the most advanced, stable technology available at the time of deployment.) The data for the registry will be stored on storage arrays of solid state drives shared over a fast storage area network. The virtual environment allows the infrastructure to easily scale both vertically and horizontally to cater to changing demand. It also facilitates effective utilization of system resources, thus reducing energy consumption and carbon footprint.

The network firewalls, routers and switches support all applications and servers. Hardware traffic shapers are used to enforce an equitable access policy for connections coming from registrars. The registry system accommodates both IPv4 and IPv6 addresses. Hardware load balancers accelerate TLS⁄SSL handshaking and distribute load among a pool of application servers.

Each of the servers and network devices are equipped with redundant, hot-swappable components and multiple connections to ancillary systems. Additionally, 24x7 support agreements with a four-hour response time at all our data centers guarantee replacement of failed parts in the shortest time possible.

Examples of current system and network devices used are:
• Servers: Cisco UCS B230 blade servers
• SAN storage arrays: IBM Storwize V7000 with Solid State Drives
• SAN switches: Brocade 5100
• Firewalls: Cisco ASA 5585-X
• Load balancers: F5 Big-IP 6900
• Traffic shapers: Procera PacketLogic PL8720
• Routers: Juniper MX40 3D
• Network switches: Cisco Nexus 7010, Nexus 5548, Nexus 2232

These system components are upgraded and updated as required, and have usage and performance thresholds which trigger upgrade review points. In each data center, there is a minimum of two of each network component, a minimum of 25 servers, and a minimum of two storage arrays.

Technical components of the SRS include the following items, continually checked and upgraded as needed: SRS, WHOIS, web admin tool, DNS, DNS distributor, reporting, invoicing tools, and deferred revenue system (as needed).

All hardware is massively provisioned to ensure stability under all forecast volumes from launch through “normal” operations of average daily and peak capacities. Each and every system application, server, storage and network device is continuously monitored by the Afilias Network Operations Center for performance and availability. The data gathered is used by dynamic predictive analysis tools in real-time to raise alerts for unusual resource demands. Should any volumes exceed established thresholds, a capacity planning review is instituted which will address the need for additions well in advance of their actual need.

SRS diagram and interconnectivity description

As with all core registry services, the SRS is run from a global cluster of registry system data centers, located in geographic centers with high Internet bandwidth, power, redundancy and availability. All of the registry systems will be run in a <n+1> setup, with a primary data center and a secondary data center. For detailed site information, please see our responses to questions #32 and #35. Registrars access the SRS in real-time using EPP.

A sample of the Afilias SRS technical and operational capabilities (displayed in Figure 24-a) include:
• Geographically diverse redundant registry systems;
• Load balancing implemented for all registry services (e.g. EPP, WHOIS, web admin) ensuring equal experience for all customers and easy horizontal scalability;
• Disaster Recovery Point objective for the registry is within one minute of the loss of the primary system;
• Detailed and tested contingency plan, in case of primary site failure, and;
• Daily reports, with secure access for confidentiality protection.

As evidenced in Figure 24-a, the SRS contains several components of the registry system. The interconnectivity ensures near-real-time distribution of the data throughout the registry infrastructure, timely backups, and up-to-date billing information.

The WHOIS servers are directly connected to the registry database and provide real-time responses to queries using the most up-to-date information present in the registry.

Committed DNS-related EPP objects in the database are made available to the DNS Distributor via a dedicated set of connections. The DNS Distributor extracts committed DNS-related EPP objects in real time and immediately inserts them into the zone for dissemination.

The Afilias system is architected such that read-only database connections are executed on database replicas and connections to the database master (where write-access is executed) are carefully protected to ensure high availability.

This interconnectivity is monitored, as is the entire registry system, according to the plans detailed in our response to question #42.

Synchronization scheme

Registry databases are synchronized both within the same data center and in the backup data center using a database application called Slony. For further details, please see the responses to questions #33 and #37. Slony replication of transactions from the publisher (master) database to its subscribers (replicas) works continuously to ensure the publisher and its subscribers remain synchronized. When the publisher database completes a transaction the Slony replication system ensures that each replica also processes the transaction. When there are no transactions to process, Slony “sleeps” until a transaction arrives or for one minute, whichever comes first. Slony “wakes up” each minute to confirm with the publisher that there has not been a transaction and thus ensures subscribers are synchronized and the replication time lag is minimized. The typical replication time lag between the publisher and subscribers depends on the topology of the replication cluster, specifically the location of the subscribers relative to the publisher. Subscribers located in the same data center as the publisher are typically updated within a couple of seconds, and subscribers located in a secondary data center are typically updated in less than ten seconds. This ensures real-time or near-real-time synchronization between all databases, and in the case where the secondary data center needs to be activated, it can be done with minimal disruption to registrars.

SRS SLA performance compliance

Afilias has a ten-year record of delivering on the demanding ICANN SLAs, and will continue to provide secure, stable and reliable service in compliance with SLA requirements as specified in the new gTLD Registry Agreement, Specification 10, as presented in Figure 24-b.

The Afilias SRS currently handles over 200 million EPP transactions per month for just .INFO and .ORG. Overall, the Afilias SRS manages over 700 million EPP transactions per month for all TLDs under management.

Given this robust functionality, and more than a decade of experience supporting a thick TLD registry with a strong performance history, Afilias will meet or exceed the performance metrics in Specification 10 of the new gTLD Registry Agreement. The Afilias services and infrastructure are designed to scale both vertically and

horizontally without any downtime to provide consistent performance as this TLD grows. The Afilias architecture is also massively provisioned to meet seasonal demands and marketing campaigns. Afilias' experience also gives high confidence in the ability to scale and grow registry operations for this TLD in a secure, stable and reliable manner.

SRS resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

Over 100 Afilias team members contribute to the management of the SRS code and network that will support this TLD. The SRS team is composed of Software Engineers, Quality Assurance Analysts, Application Administrators, System Administrators, Storage Administrators, Network Administrators, Database Administrators, and Security Analysts located at three geographically separate Afilias facilities. The systems and services set up and administered by these team members are monitored 24x7 by skilled analysts at two NOCs located in Toronto, Ontario (Canada) and Horsham, Pennsylvania (USA). In addition to these team members, Afilias also utilizes trained project management staff to maintain various calendars, work breakdown schedules, utilization and resource schedules and other tools to support the technical and management staff. It is this team who will both deploy this TLD on the Afilias infrastructure, and maintain it. Together, the Afilias team has managed 11 registry transitions and six new TLD launches, which illustrate its ability to securely and reliably deliver regularly scheduled updates as well as a secure, stable and reliable SRS service for this TLD.

25. Extensible Provisioning Protocol (EPP)

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS (THE " 〈" and "〉 " CHARACTERS), WHICH ICANN INFORMS AFILIAS (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE FULL ANSWER TO THIS QUESTION IS ATTACHED AS A PDF FILE.

Afilias has been a pioneer and innovator in the use of EPP. .INFO was the first EPP-based gTLD registry and launched on EPP version 02⁄00. Afilias has a track record of supporting TLDs on standards-compliant versions of EPP. Afilias will operate the EPP registrar interface as well as a web-based interface for this TLD in accordance with RFCs and global best practices. In addition, Afilias will maintain a proper OT&E (Operational Testing and Evaluation) environment to facilitate registrar system development and testing.

Afilias' EPP technical performance meets or exceeds all ICANN requirements as demonstrated by:
• A completely functional, state-of-the-art, EPP-based SRS that currently meets the needs of various gTLDs and will meet this new TLD's needs;
• A track record of success in developing extensions to meet client and registrar

business requirements such as multi-script support for IDNs;
• Supporting six ICANN gTLDs on EPP: .INFO, .ORG, .MOBI, .AERO, .ASIA and .XXX
• EPP software that is operating today and has been fully tested to be standards-compliant;
• Proven interoperability of existing EPP software with ICANN-accredited registrars, and;
• An SRS that currently processes over 200 million EPP transactions per month for both .INFO and .ORG. Overall, Afilias processes over 700 million EPP transactions per month for all 16 TLDs under management.

The EPP service is offered in accordance with the performance specifications defined in the new gTLD Registry Agreement, Specification 10.

EPP Standards

The Afilias registry system complies with the following revised versions of the RFCs and operates multiple ICANN TLDs on these standards, including .INFO, .ORG, .MOBI, .ASIA and .XXX. The systems have been tested by our Quality Assurance ("QA") team for RFC compliance, and have been used by registrars for an extended period of time:
• 3735 - Guidelines for Extending EPP
• 3915 - Domain Registry Grace Period Mapping
• 5730 - Extensible Provisioning Protocol (EPP)
• 5731 - Domain Name Mapping
• 5732 - Host Mapping
• 5733 - Contact Mapping
• 5734 - Transport Over TCP
• 5910 - Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)

This TLD will support all valid EPP commands. The following EPP commands are in operation today and will be made available for this TLD. See attachment #25a for the base set of EPP commands and copies of Afilias XSD schema files, which define all the rules of valid, RFC compliant EPP commands and responses that Afilias supports. Any customized EPP extensions, if necessary, will also conform to relevant RFCs.

Afilias staff members actively participated in the Internet Engineering Task Force (IETF) process that finalized the new standards for EPP. Afilias will continue to actively participate in the IETF and will stay abreast of any updates to the EPP standards.

EPP software interface and functionality

Afilias will provide all registrars with a free open-source EPP toolkit. Afilias provides this software for use with both Microsoft Windows and Unix⁄Linux operating systems. This software, which includes all relevant templates and schema defined in the RFCs, is available on sourceforge.net and will be available through the registry operator's website.

Afilias' SRS EPP software complies with all relevant RFCs and includes the following functionality:
• EPP Greeting: A response to a successful connection returns a greeting to the client. Information exchanged can include: name of server, server date and time in UTC, server features, e.g., protocol versions supported, languages for the text response supported, and one or more elements which identify the objects that the server is capable of managing;
• Session management controls: <login> to establish a connection with a

server, and <logout> to end a session;
• EPP Objects: Domain, Host and Contact for respective mapping functions;
• EPP Object Query Commands: Info, Check, and Transfer (query) commands to retrieve object information, and;
• EPP Object Transform Commands: five commands to transform objects: <create> to create an instance of an object, <delete> to remove an instance of an object, <renew> to extend the validity period of an object, <update> to change information associated with an object, and <transfer> to manage changes in client sponsorship of a known object.

Currently, 100% of the top domain name registrars in the world have software that has already been tested and certified to be compatible with the Afilias SRS registry. In total, over 375 registrars, representing over 95% of all registration volume worldwide, operate software that has been certified compatible with the Afilias SRS registry. Afilias' EPP Registrar Acceptance Criteria are available in attachment #25b, EPP OT&E Criteria.

Free EPP software support

Afilias analyzes and diagnoses registrar EPP activity log files as needed and is available to assist registrars who may require technical guidance regarding how to fix repetitive errors or exceptions caused by misconfigured client software.

Registrars are responsible for acquiring a TLS/SSL certificate from an approved certificate authority, as the registry-registrar communication channel requires mutual authentication; Afilias will acquire and maintain the server-side TLS/SSL certificate. The registrar is responsible for developing support for TLS/SSL in their client application. Afilias will provide free guidance for registrars unfamiliar with this requirement.

Registrar data synchronization

There are two methods available for registrars to synchronize their data with the registry:
• Automated synchronization: Registrars can, at any time, use the EPP <info> command to obtain definitive data from the registry for a known object, including domains, hosts (nameservers) and contacts.
• Personalized synchronization: A registrar may contact technical support and request a data file containing all domains (and associated host (nameserver) and contact information) registered by that registrar, within a specified time interval. The data will be formatted as a comma separated values (CSV) file and made available for download using a secure server.

EPP modifications

There are no unique EPP modifications planned for this TLD.

All ICANN TLDs must offer a Sunrise as part of a rights protection program. Afilias uses EPP extensions that allow registrars to submit trademark and other intellectual property rights (IPR) data to the registry. These extensions are:
• An <ipr:name> element that indicates the name of Registered Mark.
• An <ipr:number> element that indicates the registration number of the IPR.
• An <ipr:ccLocality> element that indicates the origin for which the IPR is established (a national or international trademark registry).
• An <ipr:entitlement> element that indicates whether the applicant holds the trademark as the original "OWNER", "CO-OWNER" or "ASSIGNEE".
• An <ipr:appDate> element that indicates the date the Registered Mark was applied for.
• An <ipr:regDate> element that indicates the date the Registered Mark was

issued and registered.
• An <ipr:class> element that indicates the class of the registered mark.
• An <ipr:type> element that indicates the Sunrise phase the application applies for.

Note that some of these extensions might be subject to change based on ICANN-developed requirements for the Trademark Clearinghouse.

EPP resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

108 Afilias team members directly contribute to the management and development of the EPP based registry systems. As previously noted, Afilias is an active member of IETF and has a long documented history developing and enhancing EPP. These contributors include 11 developers and 14 QA engineers focused on maintaining and enhancing EPP server side software. These engineers work directly with business staff to timely address existing needs and forecast registry⁄registrar needs to ensure the Afilias EPP software is effective today and into the future. A team of eight data analysts work with the EPP software system to ensure that the data flowing through EPP is securely and reliably stored in replicated database systems. In addition to the EPP developers, QA engineers, and data analysts, other EPP contributors at Afilias include: Technical Analysts, the Network Operations Center and Data Services team members.

26. Whois

Afilias operates the WHOIS (registration data directory service) infrastructure in accordance with RFCs and global best practices, as it does for the 16 TLDs it currently supports. Designed to be robust and scalable, Afilias' WHOIS service has exceeded all contractual requirements for over a decade. It has extended search capabilities, and methods of limiting abuse.

The WHOIS service operated by Afilias meets and exceeds ICANN's requirements. Specifically, Afilias will:
• Offer a WHOIS service made available on port 43 that is flexible and standards-compliant;
• Comply with all ICANN policies, and meeting or exceeding WHOIS performance requirements in Specification 10 of the new gTLD Registry Agreement;
• Enable a Searchable WHOIS with extensive search capabilities that offers ease of use while enforcing measures to mitigate access abuse, and;
• Employ a team with significant experience managing a compliant WHOIS service.

Such extensive knowledge and experience managing a WHOIS service enables Afilias to offer a comprehensive plan for this TLD that meets the needs of constituents of the domain name industry and Internet users. The service has been tested by our QA team for RFC compliance, and has been used by registrars and many other parties

for an extended period of time. Afilias' WHOIS service currently serves almost 500 million WHOIS queries per month, with the capacity already built in to handle an order of magnitude increase in WHOIS queries, and the ability to smoothly scale should greater growth be needed.

WHOIS system description and diagram

The Afilias WHOIS system, depicted in figure 26-a, is designed with robustness, availability, compliance, and performance in mind. Additionally, the system has provisions for detecting abusive usage (e.g., excessive numbers of queries from one source). The WHOIS system is generally intended as a publicly available single object lookup system. Afilias uses an advanced, persistent caching system to ensure extremely fast query response times.

Afilias will develop restricted WHOIS functions based on specific domain policy and regulatory requirements as needed for operating the business (as long as they are standards compliant). It will also be possible for contact and registrant information to be returned according to regulatory requirements. The WHOIS database supports multiple string and field searching through a reliable, free, secure web-based interface.

Data objects, interfaces, access and lookups

Registrars can provide an input form on their public websites through which a visitor is able to perform WHOIS queries. The registry operator can also provide a Web-based search on its site. The input form must accept the string to query, along with the necessary input elements to select the object type and interpretation controls. This input form sends its data to the Afilias port 43 WHOIS server. The results from the WHOIS query are returned by the server and displayed in the visitor's Web browser. The sole purpose of the Web interface is to provide a user-friendly interface for WHOIS queries.

Afilias will provide WHOIS output as per Specification 4 of the new gTLD Registry Agreement. The output for domain records generally consists of the following elements:

- The name of the domain registered and the sponsoring registrar;
- The names of the primary and secondary nameserver(s) for the registered domain name;
- The creation date, registration status and expiration date of the registration;
- The name, postal address, e-mail address, and telephone and fax numbers of the domain name holder;
- The name, postal address, e-mail address, and telephone and fax numbers of the technical contact for the domain name holder;
- The name, postal address, e-mail address, and telephone and fax numbers of the administrative contact for the domain name holder, and;
- The name, postal address, e-mail address, and telephone and fax numbers of the billing contact for the domain name holder.

The following additional features are also present in Afilias' WHOIS service:

- Support for IDNs, including the language tag and the Punycode representation of the IDN in addition to Unicode Hex and Unicode HTML formats;
- Enhanced support for privacy protection relative to the display of confidential information.

Afilias will also provide sophisticated WHOIS search functionality that includes the ability to conduct multiple string and field searches.

Query controls

For all WHOIS queries, a user is required to enter the character string representing the information for which they want to search. The object type and interpretation control parameters to limit the search may also be specified. If

object type or interpretation control parameter is not specified, WHOIS will search for the character string in the Name field of the Domain object.

WHOIS queries are required to be either an "exact search" or a "partial search," both of which are insensitive to the case of the input string.

An exact search specifies the full string to search for in the database field. An exact match between the input string and the field value is required.

A partial search specifies the start of the string to search for in the database field. Every record with a search field that starts with the input string is considered a match. By default, if multiple matches are found for a query, then a summary containing up to 50 matching results is presented. A second query is required to retrieve the specific details of one of the matching records.

If only a single match is found, then full details will be provided. Full detail consists of the data in the matching object as well as the data in any associated objects. For example: a query that results in a domain object includes the data from the associated host and contact objects.

WHOIS query controls fall into two categories: those that specify the type of field, and those that modify the interpretation of the input or determine the level of output to provide. Each is described below.

The following keywords restrict a search to a specific object type:
• Domain: Searches only domain objects. The input string is searched in the Name field.
• Host: Searches only nameserver objects. The input string is searched in the Name field and the IP Address field.
• Contact: Searches only contact objects. The input string is searched in the ID field.
• Registrar: Searches only registrar objects. The input string is searched in the Name field.
By default, if no object type control is specified, then the Name field of the Domain object is searched.

In addition, Afilias WHOIS systems can perform and respond to WHOIS searches by registrant name, postal address and contact names. Deployment of these features is provided as an option to the registry operator, based upon registry policy and business decision-making.

Figure 26-b presents the keywords that modify the interpretation of the input or determine the level of output to provide.

By default, if no interpretation control keywords are used, the output will include full details if a single match is found and a summary if multiple matches are found.

Unique TLD requirements

There are no unique WHOIS requirements for this TLD.

Sunrise WHOIS processes

All ICANN TLDs must offer a Sunrise as part of a rights protection program. Afilias uses EPP extensions that allow registrars to submit trademark and other intellectual property rights (IPR) data to the registry. The following corresponding data will be displayed in WHOIS for relevant domains:
• Trademark Name: element that indicates the name of the Registered Mark.
• Trademark Number: element that indicates the registration number of the IPR.
• Trademark Locality: element that indicates the origin for which the IPR is established (a national or international trademark registry).

• Trademark Entitlement: element that indicates whether the applicant holds the trademark as the original “OWNER”, “CO-OWNER” or “ASSIGNEE”.
• Trademark Application Date: element that indicates the date the Registered Mark was applied for.
• Trademark Registration Date: element that indicates the date the Registered Mark was issued and registered.
• Trademark Class: element that indicates the class of the Registered Mark.
• IPR Type: element that indicates the Sunrise phase the application applies for.

IT and infrastructure resources

All the applications and databases for this TLD will run in a virtual environment hosted by a cluster of servers equipped with the latest Intel Westmere multi-core processors (or a more advanced, stable technology available at the time of deployment). The registry data will be stored on storage arrays of solid-state drives shared over a fast storage area network. The virtual environment allows the infrastructure to easily scale both vertically and horizontally to cater to changing demand. It also facilitates effective utilization of system resources thus reducing energy consumption and carbon footprint.

The applications and servers are supported by network firewalls, routers and switches. The WHOIS system accommodates both IPv4 and IPv6 addresses.

Each of the servers and network devices are equipped with redundant hot-swappable components and multiple connections to ancillary systems. Additionally, 24x7 support agreements with our hardware vendor with a 4-hour response time at all our data centers guarantees replacement of failed parts in the shortest time possible.

Models of system and network devices used are:
• Servers: Cisco UCS B230 blade servers
• SAN storage arrays: IBM Storwize V7000 with Solid State Drives
• Firewalls: Cisco ASA 5585-X
• Load balancers: F5 Big-IP 6900
• Traffic shapers: Procera PacketLogic PL8720
• Routers: Juniper MX40 3D
• Network switches: Cisco Nexus 7010, Nexus 5548, Nexus 2232

There will be at least four virtual machines (VMs) offering WHOIS service. Each VM will run at least two WHOIS server instances - one for registrars and one for the public. All instances of the WHOIS service is made available to registrars and the public are rate limited to mitigate abusive behavior.

Frequency of synchronization between servers

Registration data records from the EPP publisher database will be replicated to the WHOIS system database on a near-real-time basis whenever an update occurs.

Specifications 4 and 10 compliance

The WHOIS service for this TLD will meet or exceed the performance requirements in the new gTLD Registry Agreement, Specification 10. Figure 26-c provides the exact measurements and commitments. Afilias has a 10 year track record of exceeding WHOIS performance and a skilled team to ensure this continues for all TLDs under management.

The WHOIS service for this TLD will meet or exceed the requirements in the new gTLD Registry Agreement, Specification 4.

RFC 3912 compliance

Afilias will operate the WHOIS infrastructure in compliance with RFCs and global best practices, as it does with the 16 TLDs Afilias currently supports.

Afilias maintains a registry-level centralized WHOIS database that contains information for every registered domain and for all host and contact objects. The WHOIS service will be available on the Internet standard WHOIS port (port 43) in compliance with RFC 3912. The WHOIS service contains data submitted by registrars during the registration process. Changes made to the data by a registrant are submitted to Afilias by the registrar and are reflected in the WHOIS database and service in near-real-time, by the instance running at the primary data center, and in under ten seconds by the instance running at the secondary data center, thus providing all interested parties with up-to-date information for every domain. This service is compliant with the new gTLD Registry Agreement, Specification 4.

The WHOIS service maintained by Afilias will be authoritative and complete, as this will be a “thick” registry (detailed domain contact WHOIS is all held at the registry); users do not have to query different registrars for WHOIS information, as there is one central WHOIS system. Additionally, visibility of different types of data is configurable to meet the registry operator’s needs.

Searchable WHOIS

Afilias offers a searchable WHOIS on a web-based Directory Service. Partial match capabilities are offered on the following fields: domain name, registrar ID, and IP address. In addition, Afilias WHOIS systems can perform and respond to WHOIS searches by registrant name, postal address and contact names.

Providing the ability to search important and high-value fields such as registrant name, address and contact names increases the probability of abusive behavior. An abusive user could script a set of queries to the WHOIS service and access contact data in order to create or sell a list of names and addresses of registrants in this TLD. Making the WHOIS machine readable, while preventing harvesting and mining of WHOIS data, is a key requirement integrated into the Afilias WHOIS systems. For instance, Afilias limits search returns to 50 records at a time. If bulk queries were ever necessary (e.g., to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process), Afilias makes such query responses available to carefully screened and limited staff members at the registry operator (and customer support staff) via an internal data warehouse. The Afilias WHOIS system accommodates anonymous access as well as pre-identified and profile-defined uses, with full audit and log capabilities.

The WHOIS service has the ability to tag query responses with labels such as “Do not redistribute” or “Special access granted”. This may allow for tiered response and reply scenarios. Further, the WHOIS service is configurable in parameters and fields returned, which allow for flexibility in compliance with various jurisdictions, regulations or laws.

Afilias offers exact-match capabilities on the following fields: registrar ID, nameserver name, and nameserver’s IP address (only applies to IP addresses stored by the registry, i.e., glue records). Search capabilities are fully available, and results include domain names matching the search criteria (including IDN variants). Afilias manages abuse prevention through rate limiting and CAPTCHA (described below). Queries do not require specialized transformations of internationalized domain names or internationalized data fields

Please see “Query Controls” above for details about search options and capabilities.

Deterring WHOIS abuse

Afilias has adopted two best practices to prevent abuse of the WHOIS service: rate limiting and CAPTCHA.

Abuse of WHOIS services on port 43 and via the Web is subject to an automated rate-limiting system. This ensures that uniformity of service to users is unaffected by a few parties whose activities abuse or otherwise might threaten to overload the WHOIS system.

Abuse of web-based public WHOIS services is subject to the use of CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) technology. The use of CAPTCHA ensures that uniformity of service to users is unaffected by a few parties whose activities abuse or otherwise might threaten to overload the WHOIS system. Afilias will adopt a CAPTCHA on its Web-based WHOIS.

Data mining of any sort on the WHOIS system is strictly prohibited, and this prohibition is published in WHOIS output and in terms of service.

For rate limiting on IPv4, there are configurable limits per IP and subnet. For IPv6, the traditional limitations do not apply. Whenever a unique IPv6 IP address exceeds the limit of WHOIS queries per minute, the same rate-limit for the given 64 bits of network prefix that the offending IPv6 IP address falls into will be applied. At the same time, a timer will start and rate-limit validation logic will identify if there are any other IPv6 address within the original 80-bit(/48) prefix. If another offending IPv6 address does fall into the /48 prefix then rate-limit validation logic will penalize any other IPv6 addresses that fall into that given 80-bit (/48) network. As a security precaution, Afilias will not disclose these limits.

Pre-identified and profile-driven role access allows greater granularity and configurability in both access to the WHOIS service, and in volume/frequency of responses returned for queries.

Afilias staff are key participants in the ICANN Security & Stability Advisory Committee’s deliberations and outputs on WHOIS, including SAC003, SAC027, SAC033, SAC037, SAC040, and SAC051. Afilias staff are active participants in both technical and policy decision making in ICANN, aimed at restricting abusive behavior.

WHOIS staff resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

Within Afilias, there are 11 staff members who develop and maintain the compliant

WHOIS systems. They keep pace with access requirements, thwart abuse, and continually develop software. Of these resources, approximately two staffers are typically required for WHOIS-related code customization. Other resources provide quality assurance, and operations personnel maintain the WHOIS system itself. This team will be responsible for the implementation and on-going maintenance of the new TLD WHOIS service.

27. Registration Life Cycle

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS (THE " 〈" and "〉 " CHARACTERS), WHICH ICANN INFORMS AFILIAS (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE FULL ANSWER TO THIS QUESTION IS ATTACHED AS A PDF FILE.

Afilias has been managing registrations for over a decade. Afilias has had experience managing registrations for over a decade and supports comprehensive registration lifecycle services including the registration states, all standard grace periods, and can address any modifications required with the introduction of any new ICANN policies.

This TLD will follow the ICANN standard domain lifecycle, as is currently implemented in TLDs such as .ORG and .INFO. The below response includes: a diagram and description of the lifecycle of a domain name in this TLD, including domain creation, transfer protocols, grace period implementation and the respective time frames for each; and the existing resources to support the complete lifecycle of a domain.

As depicted in Figure 27-a, prior to the beginning of the Trademark Claims Service or Sunrise IP protection program[s], Afilias will support the reservation of names in accordance with the new gTLD Registry Agreement, Specification 5. After the quiet period for Sunrise closes, there will be a land rush period providing applicants the opportunity to register their domain prior to general availability; this will be followed by a 30 day quiet period.

Registration period

After the IP protection programs, the landrush and the general launch, eligible registrants may choose an accredited registrar to register a domain name. The registrar will check availability on the requested domain name and if available, will collect specific objects such as, the required contact and host information from the registrant. The registrar will then provision the information into the registry system using standard Extensible Provisioning Protocol ("EPP") commands through a secure connection to the registry backend service provider.

When the domain is created, the standard five day Add Grace Period begins, the domain and contact information are available in WHOIS, and normal operating EPP domain statuses will apply. Other specifics regarding registration rules for an active domain include:
• The domain must be unique;
• Restricted or reserved domains cannot be registered;
• The domain can be registered from 1-10 years;
• The domain can be renewed at any time for 1-10 years, but cannot exceed 10 years;
• The domain can be explicitly deleted at any time;
• The domain can be transferred from one registrar to another except during the first 60 days following a successful registration or within 60 days following a

transfer; and,
Contacts and hosts can be modified at any time.

The following describe the domain status values recognized in WHOIS when using the EPP protocol following RFC 5731.
• OK or Active: This is the normal status for a domain that has no pending operations or restrictions.
• Inactive: The domain has no delegated name servers.
• Locked: No action can be taken on the domain. The domain cannot be renewed, transferred, updated, or deleted. No objects such as contacts or hosts can be associated to, or disassociated from the domain. This status includes: Delete Prohibited ⁄ Server Delete Prohibited, Update Prohibited ⁄ Server Update Prohibited, Transfer Prohibited, Server Transfer Prohibited, Renew Prohibited, Server Renew Prohibited.
• Hold: The domain will not be included in the zone. This status includes: Client Hold, Server Hold.
• Transfer Prohibited: The domain cannot be transferred away from the sponsoring registrar. This status includes: Client Transfer Prohibited, Server Transfer Prohibited.

The following describe the registration operations that apply to the domain name during the registration period.

a. Domain modifications: This operation allows for modifications or updates to the domain attributes to include:
i. Registrant Contact
ii. Admin Contact
iii. Technical Contact
iv. Billing Contact
v. Host or nameservers
vi. Authorization information
vii. Associated status values

A domain with the EPP status of Client Update Prohibited or Server Update Prohibited may not be modified until the status is removed.

b. Domain renewals: This operation extends the registration period of a domain by changing the expiration date. The following rules apply:
i. A domain can be renewed at any time during its registration term,
ii. The registration term cannot exceed a total of 10 years.

A domain with the EPP status of Client Renew Prohibited or Server Renew Prohibited cannot be renewed.

c. Domain deletions: This operation deletes the domain from the Shared Registry Services (SRS). The following rules apply:
i. A domain can be deleted at any time during its registration term, f the domain is deleted during the Add Grace Period or the Renew⁄Extend Grace Period, the sponsoring registrar will receive a credit,
ii. A domain cannot be deleted if it has “child” nameservers that are associated to other domains.

A domain with the EPP status of Client Delete Prohibited or Server Delete Prohibited cannot be deleted.

d. Domain transfers: A transfer of the domain from one registrar to another is conducted by following the steps below.
i. The registrant must obtain the applicable <authInfo> code from the sponsoring (losing) registrar.
• Every domain name has an authInfo code as per EPP RFC 5731. The authInfo code is

a six- to 16-character code assigned by the registrar at the time the name was created. Its purpose is to aid identification of the domain owner so proper authority can be established (it is the "password" to the domain).
• Under the Registry-Registrar Agreement, registrars will be required to provide a copy of the authInfo code to the domain registrant upon his or her request.
ii. The registrant must provide the authInfo code to the new (gaining) registrar, who will then initiate a domain transfer request. A transfer cannot be initiated without the authInfo code.
• Every EPP <transfer> command must contain the authInfo code or the request will fail. The authInfo code represents authority to the registry to initiate a transfer.
iii. Upon receipt of a valid transfer request, the registry automatically asks the sponsoring (losing) registrar to approve the request within five calendar days.
• When a registry receives a transfer request the domain cannot be modified, renewed or deleted until the request has been processed. This status must not be combined with either Client Transfer Prohibited or Server Transfer Prohibited status.
• If the sponsoring (losing) registrar rejects the transfer within five days, the transfer request is cancelled. A new domain transfer request will be required to reinitiate the process.
• If the sponsoring (losing) registrar does not approve or reject the transfer within five days, the registry automatically approves the request.
iv. After a successful transfer, it is strongly recommended that registrars change the authInfo code, so that the prior registrar or registrant cannot use it anymore.
v. Registrars must retain all transaction identifiers and codes associated with successful domain object transfers and protect them from disclosure.
vi. Once a domain is successfully transferred the status of TRANSFERPERIOD is added to the domain for a period of five days.
vii. Successful transfers will result in a one year term extension (resulting in a maximum total of 10 years), which will be charged to the gaining registrar.

e. Bulk transfer: Afilias supports bulk transfer functionality within the SRS for situations where ICANN may request the registry to perform a transfer of some or all registered objects (includes domain, contact and host objects) from one registrar to another registrar. Once a bulk transfer has been executed, expiry dates for all domain objects remain the same, and all relevant states of each object type are preserved. In some cases the gaining and the losing registrar as well as the registry must approved bulk transfers. A detailed log is captured for each bulk transfer process and is archived for audit purposes.

Afilias will support ICANN’s Transfer Dispute Resolution Process. Afilias will also respond to Requests for Enforcement (law enforcement or court orders) and will follow that process.

1. Auto-renew grace period
The Auto-Renew Grace Period displays as AUTORENEWPERIOD in WHOIS. An auto-renew must be requested by the registrant through the sponsoring registrar and occurs if a domain name registration is not explicitly renewed or deleted by the expiration date and is set to a maximum of 45 calendar days. In this circumstance the registration will be automatically renewed by the registry system the first day after the expiration date. If a Delete, Extend, or Transfer occurs within the AUTORENEWPERIOD the following rules apply:
i. Delete. If a domain is deleted the sponsoring registrar at the time of the deletion receives a credit for the auto-renew fee. The domain then moves into the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.
ii. Renew⁄Extend. A domain can be renewed as long as the total term does not exceed 10 years. The account of the sponsoring registrar at the time of the extension will be charged for the additional number of years the registration is renewed.

iii. Transfer (other than ICANN-approved bulk transfer). If a domain is transferred, the losing registrar is credited for the auto-renew fee, and the year added by the operation is cancelled. As a result of the transfer, the expiration date of the domain is extended by minimum of one year as long as the total term does not exceed 10 years. The gaining registrar is charged for the additional transfer year(s) even in cases where a full year is not added because of the maximum 10 year registration restriction.

2. Redemption grace period
During this period, a domain name is placed in the PENDING DELETE RESTORABLE status when a registrar requests the deletion of a domain that is not within the Add Grace Period. A domain can remain in this state for up to 30 days and will not be included in the zone file. The only action a registrar can take on a domain is to request that it be restored. Any other registrar requests to modify or otherwise update the domain will be rejected. If the domain is restored it moves into PENDING RESTORE and then OK. After 30 days if the domain is not restored it moves into PENDING DELETE SCHEDULED FOR RELEASE before the domain is released back into the pool of available domains.

3. Pending delete
During this period, a domain name is placed in PENDING DELETE SCHEDULED FOR RELEASE status for five days, and all Internet services associated with the domain will remain disabled and domain cannot be restored. After five days the domain is released back into the pool of available domains.

Other grace periods

All ICANN required grace periods will be implemented in the registry backend service provider's system including the Add Grace Period (AGP), Renew⁄Extend Grace Period (EGP), Transfer Grace Period (TGP), Auto-Renew Grace Period (ARGP), and Redemption Grace Period (RGP). The lengths of grace periods are configurable in the registry system. At this time, the grace periods will be implemented following other gTLDs such as .ORG. More than one of these grace periods may be in effect at any one time. The following are accompanying grace periods to the registration lifecycle.

Add grace period
The Add Grace Period displays as ADDPERIOD in WHOIS and is set to five calendar days following the initial registration of a domain. If the domain is deleted by the registrar during this period, the registry provides a credit to the registrar for the cost of the registration. If a Delete, Renew⁄Extend, or Transfer operation occurs within the five calendar days, the following rules apply.
i. Delete. If a domain is deleted within this period the sponsoring registrar at the time of the deletion is credited for the amount of the registration. The domain is deleted from the registry backend service provider's database and is released back into the pool of available domains.
ii. Renew⁄Extend. If the domain is renewed within this period and then deleted, the sponsoring registrar will receive a credit for both the registration and the extended amounts. The account of the sponsoring registrar at the time of the renewal will be charged for the initial registration plus the number of years the registration is extended. The expiration date of the domain registration is extended by that number of years as long as the total term does not exceed 10 years.
iii. Transfer (other than ICANN-approved bulk transfer). Transfers under Part A of the ICANN Policy on Transfer of Registrations between registrars may not occur during the ADDPERIOD or at any other time within the first 60 days after the initial registration. Enforcement is the responsibility of the registrar sponsoring the domain name registration and is enforced by the SRS.

Renew ⁄ extend grace period

The Renew ⁄ Extend Grace Period displays as RENEWPERIOD in WHOIS and is set to five calendar days following an explicit renewal on the domain by the registrar. If a Delete, Extend, or Transfer occurs within the five calendar days, the following rules apply:

i. Delete. If a domain is deleted within this period the sponsoring registrar at the time of the deletion receives a credit for the renewal fee. The domain then moves into the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.

ii. Renew⁄Extend. A domain registration can be renewed within this period as long as the total term does not exceed 10 years. The account of the sponsoring registrar at the time of the extension will be charged for the additional number of years the registration is renewed.

iii. Transfer (other than ICANN-approved bulk transfer). If a domain is transferred within the Renew⁄Extend Grace Period, there is no credit to the losing registrar for the renewal fee. As a result of the transfer, the expiration date of the domain registration is extended by a minimum of one year as long as the total term for the domain does not exceed 10 years.

If a domain is auto-renewed, then extended, and then deleted within the Renew⁄Extend Grace Period, the registrar will be credited for any auto-renew fee charged and the number of years for the extension. The years that were added to the domain's expiration as a result of the auto-renewal and extension are removed. The deleted domain is moved to the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.

Transfer Grace Period

The Transfer Grace period displays as TRANSFERPERIOD in WHOIS and is set to five calendar days after the successful transfer of domain name registration from one registrar to another registrar. Transfers under Part A of the ICANN Policy on Transfer of Registrations between registrars may not occur during the TRANSFERPERIOD or within the first 60 days after the transfer. If a Delete or Renew⁄Extend occurs within that five calendar days, the following rules apply:

i. Delete. If the domain is deleted by the new sponsoring registrar during this period, the registry provides a credit to the registrar for the cost of the transfer. The domain then moves into the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.

ii. Renew⁄Extend. If a domain registration is renewed within the Transfer Grace Period, there is no credit for the transfer. The registrar's account will be charged for the number of years the registration is renewed. The expiration date of the domain registration is extended by the renewal years as long as the total term does not exceed 10 years.

Registration lifecycle resources

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way. Virtually all Afilias resource are involved in the registration lifecycle of domains.

There are a few areas where registry staff devote resources to registration lifecycle issues:

a. Supporting Registrar Transfer Disputes. The registry operator will have a compliance staffer handle these disputes as they arise; they are very rare in the

existing gTLDs.
b. Afilias has its development and quality assurance departments on hand to modify the grace period functionality as needed, if ICANN issues new Consensus Policies or the RFCs change.

Afilias has more than 30 staff members in these departments.

28. Abuse Prevention and Mitigation

Afilias will take the requisite operational and technical steps to promote WHOIS data accuracy, limit domain abuse, remove outdated and inaccurate data, and other security measures to ensure the integrity of the TLD. The specific measures include, but are not limited to:
• Posting a TLD Anti-Abuse Policy that clearly defines abuse, and provide point-of-contact information for reporting suspected abuse;
• Committing to rapid identification and resolution of abuse, including suspensions;
• Ensuring completeness of WHOIS information at the time of registration;
• Publishing and maintaining procedures for removing orphan glue records for names removed from the zone, and;
• Establishing measures to deter WHOIS abuse, including rate-limiting, determining data syntax validity, and implementing and enforcing requirements from the Registry-Registrar Agreement.

Abuse policy

The Anti-Abuse Policy stated below will be enacted under the contractual authority of the registry operator through the Registry-Registrar Agreement, and the obligations will be passed on to and made binding upon registrants. This policy will be posted on the TLD web site along with contact information for registrants or users to report suspected abuse.

The policy is designed to address the malicious use of domain names. The registry operator and its registrars will make reasonable attempts to limit significant harm to Internet users. This policy is not intended to take the place of the Uniform Domain Name Dispute Resolution Policy (UDRP) or the Uniform Rapid Suspension System (URS), and it is not to be used as an alternate form of dispute resolution or as a brand protection mechanism. Its intent is not to burden law-abiding or innocent registrants and domain users; rather, the intent is to deter those who use domain names maliciously by engaging in illegal or fraudulent activity.

Repeat violations of the abuse policy will result in a case-by-case review of the abuser(s), and the registry operator reserves the right to escalate the issue, with the intent of levying sanctions that are allowed under the TLD anti-abuse policy.

The below policy is a recent version of the policy that has been used by the .INFO registry since 2008, and the .ORG registry since 2009. It has proven to be an effective and flexible tool.

.WEB Anti-Abuse Policy
The following Anti-Abuse Policy is effective upon launch of the TLD. Malicious use of domain names will not be tolerated. The nature of such abuses creates security and stability issues for the registry, registrars, and registrants, as well as for users of the Internet in general. The registry operator definition of abusive use

of a domain includes, without limitation, the following:
• Illegal or fraudulent actions;
• Spam: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to email spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of web sites and Internet forums;
• Phishing: The use of counterfeit web pages that are designed to trick recipients into divulging sensitive data such as personally identifying information, usernames, passwords, or financial data;
• Pharming: The redirecting of unknowing users to fraudulent sites or services, typically through, but not limited to, DNS hijacking or poisoning;
• Willful distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include, without limitation, computer viruses, worms, keyloggers, and Trojan horses.
• Malicious fast-flux hosting: Use of fast-flux techniques with a botnet to disguise the location of web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities.
• Botnet command and control: Services run on a domain name that are used to control a collection of compromised computers or "zombies," or to direct distributed denial-of-service attacks (DDoS attacks);
• Illegal Access to Other Computers or Networks: Illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).

Pursuant to the Registry-Registrar Agreement, registry operator reserves the right at its sole discretion to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status, that it deems necessary: (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of registry operator, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement and this Anti-Abuse Policy, or (5) to correct mistakes made by registry operator or any registrar in connection with a domain name registration. Registry operator also reserves the right to place upon registry lock, hold, or similar status a domain name during resolution of a dispute.

The policy stated above will be accompanied by notes about how to submit a report to the registry operator's abuse point of contact, and how to report an orphan glue record suspected of being used in connection with malicious conduct (see below).

Abuse point of contact and procedures for handling abuse complaints

The registry operator will establish an abuse point of contact. This contact will be a role-based e-mail address of the form "abuse@registry.WEB". This e-mail address will allow multiple staff members to monitor abuse reports on a 24x7 basis, and then work toward closure of cases as each situation calls for. For tracking purposes, the registry operator will have a ticketing system with which all complaints will be tracked internally. The reporter will be provided with the ticket reference identifier for potential follow-up. Afilias will integrate its existing ticketing system to ensure uniform tracking and handling of the complaint. This role-based approach has been used successfully by ISPs, e-mail service providers, and registrars for many years, and is considered a global best practice.

The registry operator's designated abuse handlers will then evaluate complaints received via the abuse system address. They will decide whether a particular issue is of concern, and decide what action, if any, is appropriate.

In general, the registry operator will find itself receiving abuse reports from a wide variety of parties, including security researchers and Internet security companies, financial institutions such as banks, Internet users, and law enforcement agencies among others. Some of these parties may provide good forensic data or supporting evidence of the malicious behavior. In other cases, the party reporting an issue may not be familiar with how to provide such data or proof of malicious behavior. It is expected that a percentage of abuse reports to the registry operator will not be actionable, because there will not be enough evidence to support the complaint (even after investigation), and because some reports or reporters will simply not be credible.

The security function includes a communication and outreach function, with information sharing with industry partners regarding malicious or abusive behavior, in order to ensure coordinated abuse mitigation across multiple TLDs.

Assessing abuse reports requires great care, and the registry operator will rely upon professional, trained investigators who are versed in such matters. The goals are accuracy, good record-keeping, and a zero false-positive rate so as not to harm innocent registrants.

Different types of malicious activities require different methods of investigation and documentation. Further, the registry operator expects to face unexpected or complex situations that call for professional advice, and will rely upon professional, trained investigators as needed.

In general, there are two types of domain abuse that must be addressed:
a) Compromised domains. These domains have been hacked or otherwise compromised by criminals, and the registrant is not responsible for the malicious activity taking place on the domain. For example, the majority of domain names that host phishing sites are compromised. The goal in such cases is to get word to the registrant (usually via the registrar) that there is a problem that needs attention with the expectation that the registrant will address the problem in a timely manner. Ideally such domains do not get suspended, since suspension would disrupt legitimate activity on the domain.
b) Malicious registrations. These domains are registered by malefactors for the purpose of abuse. Such domains are generally targets for suspension, since they have no legitimate use.

The standard procedure is that the registry operator will forward a credible alleged case of malicious domain name use to the domain's sponsoring registrar with a request that the registrar investigate the case and act appropriately. The registrar will be provided evidence collected as a result of the investigation conducted by the trained abuse handlers. As part of the investigation, if inaccurate or false WHOIS registrant information is detected, the registrar is notified about this. The registrar is the party with a direct relationship with—and a direct contract with—the registrant. The registrar will also have vital information that the registry operator will not, such as:
• Details about the domain purchase, such as the payment method used (credit card, PayPal, etc.);
• The identity of a proxy-protected registrant;
• The purchaser's IP address;
• Whether there is a reseller involved, and;
• The registrant's past sales history and purchases in other TLDs (insofar as the registrar can determine this).

Registrars do not share the above information with registry operators due to

privacy and liability concerns, among others. Because they have more information with which to continue the investigation, and because they have a direct relationship with the registrant, the registrar is in the best position to evaluate alleged abuse. The registrar can determine if the use violates the registrar's legal terms of service or the registry Anti-Abuse Policy, and can decide whether or not to take any action. While the language and terms vary, registrars will be expected to include language in their registrar-registrant contracts that indemnifies the registrar if it takes action, and allows the registrar to suspend or cancel a domain name; this will be in addition to the registry Anti-Abuse Policy. Generally, registrars can act if the registrant violates the registrar's terms of service, or violates ICANN policy, or if illegal activity is involved, or if the use violates the registry's Anti-Abuse Policy.

If a registrar does not take action within a time period indicated by the registry operator (usually 24 hours), the registry operator might then decide to take action itself. At all times, the registry operator reserves the right to act directly and immediately if the potential harm to Internet users seems significant or imminent, with or without notice to the sponsoring registrar.

The registry operator will be prepared to call upon relevant law enforcement bodies as needed. There are certain cases, for example, Illegal pharmacy domains, where the registry operator will contact the Law Enforcement Agencies to share information about these domains, provide all the evidence collected and work closely with them before any action will be taken for suspension. The specific action is often dependent upon the jurisdiction of which the registry operator, although the operator in all cases will adhere to applicable laws and regulations.

When valid court orders or seizure warrants are received from courts or law enforcement agencies of relevant jurisdiction, the registry operator will order execution in an expedited fashion. Compliance with these will be a top priority and will be completed as soon as possible and within the defined timelines of the order. There are certain cases where Law Enforcement Agencies request information about a domain including but not limited to:
• Registration information
• History of a domain, including recent updates made
• Other domains associated with a registrant's account
• Patterns of registrant portfolio

Requests for such information is handled on a priority basis and sent back to the requestor as soon as possible. Afilias sets a goal to respond to such requests within 24 hours.

The registry operator may also engage in proactive screening of its zone for malicious use of the domains in the TLD, and report problems to the sponsoring registrars. The registry operator could take advantage of a combination of the following resources, among others:
• Blocklists of domain names and nameservers published by organizations such as SURBL and Spamhaus.
• Anti-phishing feeds, which will provide URLs of compromised and maliciously registered domains being used for phishing.
• Analysis of registration or DNS query data [DNS query data received by the TLD nameservers.]

The registry operator will keep records and track metrics regarding abuse and abuse reports. These will include:
• Number of abuse reports received by the registry's abuse point of contact described above;
• Number of cases and domains referred to registrars for resolution;
• Number of cases and domains where the registry took direct action;
• Resolution times;

• Number of domains in the TLD that have been blacklisted by major anti-spam blocklist providers, and;
• Phishing site uptimes in the TLD.

Removal of orphan glue records

By definition, orphan glue records used to be glue records. Glue records are related to delegations and are necessary to guide iterative resolvers to delegated nameservers. A glue record becomes an orphan when its parent nameserver record is removed without also removing the corresponding glue record. (Please reference the ICANN SSAC paper SAC048 at: http://www.icann.org/en/committees/security/sac048.pdf.) Orphan glue records may be created when a domain (example.tld) is placed on EPP ServerHold or ClientHold status. When placed on Hold, the domain is removed from the zone and will stop resolving. However, any child nameservers (now orphan glue) of that domain (e.g., ns1.example.tld) are left in the zone. It is important to keep these orphan glue records in the zone so that any innocent sites using that nameserver will continue to resolve. This use of Hold status is an essential tool for suspending malicious domains.

Afilias observes the following procedures, which are being followed by other registries and are generally accepted as DNS best practices. These procedures are also in keeping with ICANN SSAC recommendations.

When a request to delete a domain is received from a registrar, the registry first checks for the existence of glue records. If glue records exist, the registry will check to see if other domains in the registry are using the glue records. If other domains in the registry are using the glue records then the request to delete the domain will fail until no other domains are using the glue records. If no other domains in the registry are using the glue records then the glue records will be removed before the request to delete the domain is satisfied. If no glue records exist then the request to delete the domain will be satisfied.

If a registrar cannot delete a domain because of the existence of glue records that are being used by other domains, then the registrar may refer to the zone file or the "weekly domain hosted by nameserver report" to find out which domains are using the nameserver in question and attempt to contact the corresponding registrar to request that they stop using the nameserver in the glue record. The registry operator does not plan on performing mass updates of the associated DNS records.

The registry operator will accept, evaluate, and respond appropriately to complaints that orphan glue is being used maliciously. Such reports should be made in writing to the registry operator, and may be submitted to the registry's abuse point-of-contact. If it is confirmed that an orphan glue record is being used in connection with malicious conduct, the registry operator will have the orphan glue record removed from the zone file. Afilias has the technical ability to execute such requests as needed.

Methods to promote WHOIS accuracy

The creation and maintenance of accurate WHOIS records is an important part of registry management. As described in our response to question #26, WHOIS, the registry operator will manage a secure, robust and searchable WHOIS service for this TLD.

WHOIS data accuracy

The registry operator will offer a "thick" registry system. In this model, all key

contact details for each domain name will be stored in a central location by the registry. This allows better access to domain data, and provides uniformity in storing the information. The registry operator will ensure that the required fields for WHOIS data (as per the defined policies for the TLD) are enforced at the registry level. This ensures that the registrars are providing required domain registration data. Fields defined by the registry policy to be mandatory are documented as such and must be submitted by registrars. The Afilias registry system verifies formats for relevant individual data fields (e.g. e-mail, and phone/fax numbers). Only valid country codes are allowed as defined by the ISO 3166 code list. The Afilias WHOIS system is extensible, and is capable of using the VAULT system, described further below.

Similar to the centralized abuse point of contact described above, the registry operator can institute a contact email address which could be utilized by third parties to submit complaints for inaccurate or false WHOIS data detected. This information will be processed by Afilias' support department and forwarded to the registrars. The registrars can work with the registrants of those domains to address these complaints. Afilias will audit registrars on a yearly basis to verify whether the complaints being forwarded are being addressed or not. This functionality, available to all registry operators, is activated based on the registry operator's business policy.

Afilias also incorporates a spot-check verification system where a randomly selected set of domain names are checked periodically for accuracy of WHOIS data. Afilias' .PRO registry system incorporates such a verification system whereby 1% of total registrations or 100 domains, whichever number is larger, are spot-checked every month to verify the domain name registrant's critical information provided with the domain registration data. With both a highly qualified corps of engineers and a 24x7 staffed support function, Afilias has the capacity to integrate such spot-check functionality into this TLD, based on the registry operator's business policy. Note: This functionality will not work for proxy protected WHOIS information, where registrars or their resellers have the actual registrant data. The solution to that problem lies with either registry or registrar policy, or a change in the general marketplace practices with respect to proxy registrations.

Finally, Afilias' registry systems have a sophisticated set of billing and pricing functionality which aids registry operators who decide to provide a set of financial incentives to registrars for maintaining or improving WHOIS accuracy. For instance, it is conceivable that the registry operator may decide to provide a discount for the domain registration or renewal fees for validated registrants, or levy a larger cost for the domain registration or renewal of proxy domain names. The Afilias system has the capability to support such incentives on a configurable basis, towards the goal of promoting better WHOIS accuracy.

Role of registrars

As part of the RRA (Registry Registrar Agreement), the registry operator will require the registrar to be responsible for ensuring the input of accurate WHOIS data by their registrants. The Registrar/Registered Name Holder Agreement will include a specific clause to ensure accuracy of WHOIS data, and to give the registrar rights to cancel or suspend registrations if the Registered Name Holder fails to respond to the registrar's query regarding accuracy of data. ICANN's WHOIS Data Problem Reporting System (WDPRS) will be available to those who wish to file WHOIS inaccuracy reports, as per ICANN policy (http://wdprs.internic.net/).

Controls to ensure proper access to domain functions

Several measures are in place in the Afilias registry system to ensure proper access to domain functions, including authentication provisions in the RRA

relative to notification and contact updates via use of AUTH-INFO codes.

IP address access control lists, TLS⁄SSL certificates and proper authentication are used to control access to the registry system. Registrars are only given access to perform operations on the objects they sponsor.

Every domain will have a unique AUTH-INFO code. The AUTH-INFO code is a 6- to 16-character code assigned by the registrar at the time the name is created. Its purpose is to aid identification of the domain owner so proper authority can be established. It is the "password" to the domain name. Registrars must use the domain's password in order to initiate a registrar-to-registrar transfer. It is used to ensure that domain updates (update contact information, transfer, or deletion) are undertaken by the proper registrant, and that this registrant is adequately notified of domain update activity. Only the sponsoring registrar of a domain has access to the domain's AUTH-INFO code stored in the registry, and this is accessible only via encrypted, password-protected channels.

Information about other registry security measures such as encryption and security of registrar channels are confidential to ensure the security of the registry system. The details can be found in the response to question #30b.

Validation and abuse mitigation mechanisms

Afilias has developed advanced validation and abuse mitigation mechanisms. These capabilities and mechanisms are described below. These services and capabilities are discretionary and may be utilized by the registry operator based on their policy and business need.

Afilias has the ability to analyze the registration data for known patterns at the time of registration. A database of these known patterns is developed from domains and other associated objects (e.g., contact information) which have been previously detected and suspended after being flagged as abusive. Any domains matching the defined criteria can be flagged for investigation. Once analyzed and confirmed by the domain anti-abuse team members, these domains may be suspended. This provides proactive detection of abusive domains.

Provisions are available to enable the registry operator to only allow registrations by pre-authorized and verified contacts. These verified contacts are given a unique code that can be used for registration of new domains.

Registrant pre-verification and authentication

One of the systems that could be used for validity and identity authentication is VAULT (Validation and Authentication Universal Lookup). It utilizes information obtained from a series of trusted data sources with access to billions of records containing data about individuals for the purpose of providing independent age and id verification as well as the ability to incorporate additional public or private data sources as required. At present it has the following: US Residential Coverage - 90% of Adult Population and also International Coverage - Varies from Country to Country with a minimum of 80% coverage (24 countries, mostly European).

Various verification elements can be used. Examples might include applicant data such as name, address, phone, etc. Multiple methods could be used for verification include integrated solutions utilizing API (XML Application Programming Interface) or sending batches of requests.

• Verification and Authentication requirements would be based on TLD operator requirements or specific criteria.

• Based on required WHOIS Data; registrant contact details (name, address, phone)
• If address⁄ZIP can be validated by VAULT, the validation process can continue (North America +25 International countries)
• If in-line processing and registration and EPP⁄API call would go to the verification clearinghouse and return up to 4 challenge questions.
• If two-step registration is required, then registrants would get a link to complete the verification at a separate time. The link could be specific to a domain registration and pre-populated with data about the registrant.
• If WHOIS data is validated a token would be generated and could be given back to the registrar which registered the domain.
• WHOIS data would reflect the Validated Data or some subset, i.e., fields displayed could be first initial and last name, country of registrant and date validated. Other fields could be generic validation fields much like a "privacy service".
• A "Validation Icon" customized script would be sent to the registrants email address. This could be displayed on the website and would be dynamically generated to avoid unauthorized use of the Icon. When clicked on the Icon would should limited WHOIS details i.e. Registrant: jdoe, Country: USA, Date Validated: March 29, 2011, as well as legal disclaimers.
• Validation would be annually renewed, and validation date displayed in the WHOIS.

Abuse prevention resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way. Abuse prevention and detection is a function that is staffed across the various groups inside Afilias, and requires a team effort when abuse is either well hidden or widespread, or both. While all of Afilias' 200+ employees are charged with responsibility to report any detected abuse, the engineering and analysis teams, numbering over 30, provide specific support based on the type of abuse and volume and frequency of analysis required. The Afilias security and support teams have the authority to initiate mitigation.

Afilias has developed advanced validation and abuse mitigation mechanisms. These capabilities and mechanisms are described below. These services and capabilities are discretionary and may be utilized by the registry operator based on their policy and business need.

This TLD's anticipated volume of registrations in the first three years of operations is listed in response #46. Afilias' anti-abuse function anticipates the expected volume and type of registrations, and together will adequately cover the staffing needs for this TLD. The registry operator will maintain an abuse response team, which may be a combination of internal staff and outside specialty contractors, adjusting to the needs of the size and type of TLD. The team structure planned for this TLD is based on several years of experience responding to, mitigating, and managing abuse for TLDs of various sizes. The team will generally consist of abuse handlers (probably internal), a junior analyst, (either internal or external), and a senior security consultant (likely an external resource providing the registry operator with extra expertise as needed). These responders will be specially trained in the investigation of abuse complaints, and will have the latitude to act expeditiously to suspend domain names (or apply

other remedies) when called for.

The exact resources required to maintain an abuse response team must change with the size and registration procedures of the TLD. An initial abuse handler is necessary as a point of contact for reports, even if a part-time responsibility. The abuse handlers monitor the abuse email address for complaints and evaluate incoming reports from a variety of sources. A large percentage of abuse reports to the registry operator may be unsolicited commercial email. The designated abuse handlers can identify legitimate reports and then decide what action is appropriate, either to act upon them, escalate to a security analyst for closer investigation, or refer them to registrars as per the above-described procedures. A TLD with rare cases of abuse would conform to this structure.

If multiple cases of abuse within the same week occur regularly, the registry operator will consider staffing internally an additional security analyst to investigate the complaints as they become more frequent. Training an abuse analyst requires 3-6 months and likely requires the active guidance of an experienced senior security analyst for guidance and verification of assessments and recommendations being made.

If this TLD were to regularly experience multiple cases of abuse within the same day, a full-time senior security analyst would likely be necessary. A senior security analyst capable of fulfilling this role should have several years of experience and able to manage and train the internal abuse response team.

The abuse response team will also maintain subscriptions for several security information services, including the blocklists from organizations like SURBL and Spamhaus and anti-phishing and other domain related abuse (malware, fast-flux etc.) feeds. The pricing structure of these services may depend on the size of the domain and some services will include a number of rapid suspension requests for use as needed.

For a large TLD, regular audits of the registry data are required to maintain control over abusive registrations. When a registrar with a significant number of registrations has been compromised or acted maliciously, the registry operator may need to analyze a set of registration or DNS query data. A scan of all the domains of a registrar is conducted only as needed. Scanning and analysis for a large registrar may require as much as a week of full-time effort for a dedicated machine and team.

29. Rights Protection Mechanisms

Rights protection is a core responsibility of the TLD operator, and is supported by a fully-developed plan for rights protection that includes:
• Establishing mechanisms to prevent unqualified registrations (e.g., registrations made in violation of the registry’s eligibility restrictions or policies);
• Implementing a robust Sunrise program, utilizing the Trademark Clearinghouse, the services of one of ICANN’s approved dispute resolution providers, a trademark validation agent, and drawing upon sunrise policies and rules used successfully in previous gTLD launches;
• Implementing a professional trademark claims program that utilizes the Trademark Clearinghouse, and drawing upon models of similar programs used successfully in previous TLD launches;
• Complying with the URS requirements;
• Complying with the UDRP;
• Complying with the PDDRP, and;

• Including all ICANN-mandated and independently developed rights protection mechanisms (“RPMs”) in the registry-registrar agreement entered into by ICANN-accredited registrars authorized to register names in the TLD.

The response below details the rights protection mechanisms at the launch of the TLD (Sunrise and Trademark Claims Service) which comply with rights protection policies (URS, UDRP, PDDRP, and other ICANN RPMs), outlines additional provisions made for rights protection, and provides the resourcing plans.

Safeguards for rights protection at the launch of the TLD

The launch of this TLD will include the operation of a trademark claims service according to the defined ICANN processes for checking a registration request and alerting trademark holders of potential rights infringement.

The Sunrise Period will be an exclusive period of time, prior to the opening of public registration, when trademark and service mark holders will be able to reserve marks that are an identical match in the .WEB domain. Following the Sunrise Period, Afilias will open registration to qualified applicants.

The anticipated Rollout Schedule for the Sunrise Period will be approximately as follows:
• Launch of the TLD – Sunrise Period begins for trademark holders and service mark holders to submit registrations for their exact marks in the .ART domain.
• Quiet Period – The Sunrise Period will close and will be followed by a Quiet Period for testing and evaluation.
• Land rush period opens after the Quiet period
• Quiet period of 30 days begins after the close of Land rush
• One month after close of Quiet Period – Registration in the .ART domain will be opened to qualified applicants.

Sunrise Period Requirements & Restrictions
Those wishing to reserve their marks in the .WEB domain during the Sunrise Period must own a current trademark or service mark listed in the Trademark Clearinghouse.

Notice will be provided to all trademark holders in the Clearinghouse if someone is seeking a Sunrise registration. This notice will be provided to holders of marks in the Clearinghouse that are an Identical Match (as defined in the Trademark Clearing House) to the name to be registered during Sunrise.

Each Sunrise registration will require a minimum term, to be determined at a later date.

Afilias will establish the following Sunrise eligibility requirements (SERs) as minimum requirements, verified by Clearinghouse data, and incorporate a Sunrise Dispute Resolution Policy (SDRP). The SERs include: (i) ownership of a mark that satisfies the criteria set forth in section 7.2 of the Trademark Clearing House specifications, (ii) description of international class of goods or services covered by registration; (iii) representation that all provided information is true and correct; and (iv) provision of data sufficient to document rights in the trademark.

The SDRP will allow challenges based on the following four grounds: (i) at time the challenged domain name was registered, the registrants did not hold a trademark registration of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty; (ii) the domain name is not identical to the mark on which the registrant based its Sunrise registration; (iii) the trademark registration on which the registrant based its

Sunrise registration is not of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty; or (iv) the trademark registration on which the domain name registrant based its Sunrise registration did not issue on or before the effective date of the Registry Agreement and was not applied for on or before ICANN announced the applications received.

Ongoing rights protection mechanisms

Several mechanisms will be in place to protect rights in this TLD. As described in our responses to questions #27 and #28, measures are in place to ensure domain transfers and updates are only initiated by the appropriate domain holder, and an experienced team is available to respond to legal actions by law enforcement or court orders.

This TLD will conform to all ICANN RPMs including URS (defined below), UDRP, PDDRP, and all measures defined in Specification 7 of the new TLD agreement.

Uniform Rapid Suspension (URS)

The registry operator will implement decisions rendered under the URS on an ongoing basis. Per the URS policy posted on ICANN's Web site as of this writing, the registry operator will receive notice of URS actions from the ICANN-approved URS providers. These emails will be directed immediately to the registry operator's support staff, which is on duty 24x7. The support staff will be responsible for creating a ticket for each case, and for executing the directives from the URS provider. All support staff will receive pertinent training.

As per ICANN's URS guidelines, within 24 hours of receipt of the notice of complaint from the URS provider, the registry operator shall "lock" the domain, meaning the registry shall restrict all changes to the registration data, including transfer and deletion of the domain names, but the name will remain in the TLD DNS zone file and will thus continue to resolve. The support staff will "lock" the domain by associating the following EPP statuses with the domain and relevant contact objects:

- ServerUpdateProhibited, with an EPP reason code of "URS"
- ServerDeleteProhibited, with an EPP reason code of "URS"
- ServerTransferProhibited, with an EPP reason code of "URS"
- The registry operator's support staff will then notify the URS provider immediately upon locking the domain name, via email.

The registry operator's support staff will retain all copies of emails from the URS providers, assign them a tracking or ticket number, and will track the status of each opened URS case through to resolution via spreadsheet or database.

The registry operator's support staff will execute further operations upon notice from the URS providers. The URS provider is required to specify the remedy and required actions of the registry operator, with notification to the registrant, the complainant, and the registrar.

As per the URS guidelines, if the complainant prevails, the "registry operator shall suspend the domain name, which shall remain suspended for the balance of the registration period and would not resolve to the original web site. The nameservers shall be redirected to an informational web page provided by the URS provider about the URS. The WHOIS for the domain name shall continue to display all of the information of the original registrant except for the redirection of the nameservers. In addition, the WHOIS shall reflect that the domain name will not be able to be transferred, deleted or modified for the life of the registration."

Rights protection via the RRA

The following will be memorialized and be made binding via the Registry-Registrar and Registrar-Registrant Agreements:

• The registry may reject a registration request or a reservation request, or may delete, revoke, suspend, cancel, or transfer a registration or reservation under the following criteria:
a. to enforce registry policies and ICANN requirements; each as amended from time to time;
b. that is not accompanied by complete and accurate information as required by ICANN requirements and/or registry policies or where required information is not updated and/or corrected as required by ICANN requirements and/or registry policies;
c. to protect the integrity and stability of the registry, its operations, and the TLD system;
d. to comply with any applicable law, regulation, holding, order, or decision issued by a court, administrative authority, or dispute resolution service provider with jurisdiction over the registry;
e. to establish, assert, or defend the legal rights of the registry or a third party or to avoid any civil or criminal liability on the part of the registry and/or its affiliates, subsidiaries, officers, directors, representatives, employees, contractors, and stockholders;
f. to correct mistakes made by the registry or any accredited registrar in connection with a registration; or
g. as otherwise provided in the Registry-Registrar Agreement and/or the Registrar-Registrant Agreement.

Reducing opportunities for behaviors such as phishing or pharming

In our response to question #28, the registry operator has described its anti-abuse program. Rather than repeating the policies and procedures here, please see our response to question #28 for full details.

In the case of this TLD, Afilias will apply an approach that addresses registered domain names (rather than potentially registered domains). This approach will not infringe upon the rights of eligible registrants to register domains, and allows Afilias internal controls, as well as community-developed UDRP and URS policies and procedures if needed, to deal with complaints, should there be any.

Afilias is a member of various security fora which provide access to lists of names in each TLD which may be used for malicious purposes. Such identified names will be subject to the TLD anti-abuse policy, including rapid suspensions after due process.

Rights protection resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

Supporting RPMs requires several departments within the registry operator as well

as within Afilias. The implementation of Sunrise and the Trademark Claims service and on-going RPM activities will pull from the 102 Afilias staff members of the engineering, product management, development, security and policy teams at Afilias which are on duty 24x7. A trademark validator will also be assigned within the registry operator, whose responsibilities may require as much as 50% of full-time employment if the domains under management were to exceed several million. No additional hardware or software resources are required to support this as Afilias has fully-operational capabilities to manage abuse today.

30(a). Security Policy: Summary of the security policy for the proposed registry

Afilias aggressively and actively protects the registry system from known threats and vulnerabilities, and has deployed an extensive set of security protocols, policies and procedures to thwart compromise. Afilias' robust and detailed plans are continually updated and tested to ensure new threats are mitigated prior to becoming issues. Afilias will continue these rigorous security measures, which include:
• Multiple layers of security and access controls throughout registry and support systems;
• 24x7 monitoring of all registry and DNS systems, support systems and facilities;
• Unique, proven registry design that ensures data integrity by granting only authorized access to the registry system, all while meeting performance requirements;
• Detailed incident and problem management processes for rapid review, communications, and problem resolution, and;
• Yearly external audits by independent, industry-leading firms, as well as twice-yearly internal audits.

Security policies and protocols

Afilias has included security in every element of its service, including facilities, hardware, equipment, connectivity/Internet services, systems, computer systems, organizational security, outage prevention, monitoring, disaster mitigation, and escrow/insurance, from the original design, through development, and finally as part of production deployment. Examples of threats and the confidential and proprietary mitigation procedures are detailed in our response to question #30(b).

There are several important aspects of the security policies and procedures to note:
• Afilias hosts domains in data centers around the world that meet or exceed global best practices.
• Afilias' DNS infrastructure is massively provisioned as part of its DDoS mitigation strategy, thus ensuring sufficient capacity and redundancy to support new gTLDs.
• Diversity is an integral part of all of our software and hardware stability and robustness plan, thus avoiding any single points of failure in our infrastructure.
• Access to any element of our service (applications, infrastructure and data) is only provided on an as-needed basis to employees and a limited set of others to fulfill their job functions. The principle of least privilege is applied.
• All registry components–critical and non-critical–are monitored 24x7 by staff at our NOCs, and the technical staff has detailed plans and procedures that have stood the test of time for addressing even the smallest anomaly. Well-documented incident management procedures are in place to quickly involve the on-call

technical and management staff members to address any issues.

Afilias follows the guidelines from the ISO 27001 Information Security Standard (Reference: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103) for the management and implementation of its Information Security Management System. Afilias also utilizes the COBIT IT governance framework to facilitate policy development and enable controls for appropriate management of risk (Reference: http://www.isaca.org/cobit). Best practices defined in ISO 27002 are followed for defining the security controls within the organization. Afilias continually looks to improve the efficiency and effectiveness of our processes, and follows industry best practices as defined by the IT Infrastructure Library, or ITIL (Reference: http://www.itil-officialsite.com/).

The Afilias registry system is located within secure data centers that implement a multitude of security measures both to minimize any potential points of vulnerability and to limit any damage should there be a breach. The characteristics of these data centers are described fully in our response to question #30(b).

The Afilias registry system employs a number of multi-layered measures to prevent unauthorized access to its network and internal systems. Before reaching the registry network, all traffic is required to pass through a firewall system. Packets passing to and from the Internet are inspected, and unauthorized or unexpected attempts to connect to the registry servers are both logged and denied. Management processes are in place to ensure each request is tracked and documented, and regular firewall audits are performed to ensure proper operation. 24x7 monitoring is in place and, if potential malicious activity is detected, appropriate personnel are notified immediately.

Afilias employs a set of security procedures to ensure maximum security on each of its servers, including disabling all unnecessary services and processes and regular application of security-related patches to the operating system and critical system applications. Regular external vulnerability scans are performed to verify that only services intended to be available are accessible.

Regular detailed audits of the server configuration are performed to verify that the configurations comply with current best security practices. Passwords and other access means are changed on a regular schedule and are revoked whenever a staff member's employment is terminated.

Access to registry system

Access to all production systems and software is strictly limited to authorized operations staff members. Access to technical support and network operations teams where necessary are read only and limited only to components required to help troubleshoot customer issues and perform routine checks. Strict change control procedures are in place and are followed each time a change is required to the production hardware/application. User rights are kept to a minimum at all times. In the event of a staff member's employment termination, all access is removed immediately.

Afilias applications use encrypted network communications. Access to the registry server is controlled. Afilias allows access to an authorized registrar only if each of the authentication factors matches the specific requirements of the requested authorization. These mechanisms are also used to secure any web-based tools that allow authorized registrars to access the registry. Additionally, all write transactions in the registry (whether conducted by authorized registrars or the registry's own personnel) are logged.

EPP connections are encrypted using TLS/SSL, and mutually authenticated using both

certificate checks and login⁄password combinations. Web connections are encrypted using TLS⁄SSL for an encrypted tunnel to the browser, and authenticated to the EPP server using login⁄password combinations.

All systems are monitored for security breaches from within the data center and without, using both system-based and network-based testing tools. Operations staff also monitor systems for security-related performance anomalies. Triple-redundant continual monitoring ensures multiple detection paths for any potential incident or problem. Details are provided in our response to questions #30(b) and #42. Network Operations and Security Operations teams perform regular audits in search of any potential vulnerability.

To ensure that registrar hosts configured erroneously or maliciously cannot deny service to other registrars, Afilias uses traffic shaping technologies to prevent attacks from any single registrar account, IP address, or subnet. This additional layer of security reduces the likelihood of performance degradation for all registrars, even in the case of a security compromise at a subset of registrars.

There is a clear accountability policy that defines what behaviors are acceptable and unacceptable on the part of non-staff users, staff users, and management. Periodic audits of policies and procedures are performed to ensure that any weaknesses are discovered and addressed. Aggressive escalation procedures and well-defined Incident Response management procedures ensure that decision makers are involved at early stages of any event.

In short, security is a consideration in every aspect of business at Afilias, and this is evidenced in a track record of a decade of secure, stable and reliable service.

Independent assessment

Supporting operational excellence as an example of security practices, Afilias performs a number of internal and external security audits each year of the existing policies, procedures and practices for:
• Access control;
• Security policies;
• Production change control;
• Backups and restores;
• Batch monitoring;
• Intrusion detection, and
• Physical security.

Afilias has an annual Type 2 SSAE 16 audit performed by PricewaterhouseCoopers (PwC). Further, PwC performs testing of the general information technology controls in support of the financial statement audit. A Type 2 report opinion under SSAE 16 covers whether the controls were properly designed, were in place, and operating effectively during the audit period (calendar year). This SSAE 16 audit includes testing of internal controls relevant to Afilias' domain registry system and processes. The report includes testing of key controls related to the following control objectives:
• Controls provide reasonable assurance that registrar account balances and changes to the registrar account balances are authorized, complete, accurate and timely.
• Controls provide reasonable assurance that billable transactions are recorded in the Shared Registry System (SRS) in a complete, accurate and timely manner.
• Controls provide reasonable assurance that revenue is systemically calculated by the Deferred Revenue System (DRS) in a complete, accurate and timely manner.
• Controls provide reasonable assurance that the summary and detail reports, invoices, statements, registrar and registry billing data files, and ICANN

transactional reports provided to registry operator(s) are complete, accurate and timely.
• Controls provide reasonable assurance that new applications and changes to existing applications are authorized, tested, approved, properly implemented and documented.
• Controls provide reasonable assurance that changes to existing system software and implementation of new system software are authorized, tested, approved, properly implemented and documented.
• Controls provide reasonable assurance that physical access to data centers is restricted to properly authorized individuals.
• Controls provide reasonable assurance that logical access to system resources is restricted to properly authorized individuals.
• Controls provide reasonable assurance that processing and backups are appropriately authorized and scheduled and that deviations from scheduled processing and backups are identified and resolved.

The last Type 2 report issued was for the year 2010, and it was unqualified, i.e., all systems were evaluated with no material problems found.

During each year, Afilias monitors the key controls related to the SSAE controls. Changes or additions to the control objectives or activities can result due to deployment of new services, software enhancements, infrastructure changes or process enhancements. These are noted and after internal review and approval, adjustments are made for the next review.

In addition to the PricewaterhouseCoopers engagement, Afilias performs internal security audits twice a year. These assessments are constantly being expanded based on risk assessments and changes in business or technology.

Additionally, Afilias engages an independent third-party security organization, PivotPoint Security, to perform external vulnerability assessments and penetration tests on the sites hosting and managing the Registry infrastructure. These assessments are performed with major infrastructure changes, release of new services or major software enhancements. These independent assessments are performed at least annually. A report from a recent assessment is attached with our response to question #30(b).

Afilias has engaged with security companies specializing in application and web security testing to ensure the security of web-based applications offered by Afilias, such as the Web Admin Tool (WAT) for registrars and registry operators.

Finally, Afilias has engaged IBM's Security services division to perform ISO 27002 gap assessment studies so as to review alignment of Afilias' procedures and policies with the ISO 27002 standard. Afilias has since made adjustments to its security procedures and policies based on the recommendations by IBM.

Special TLD considerations

Afilias' rigorous security practices are regularly reviewed; if there is a need to alter or augment procedures for this TLD, they will be done so in a planned and deliberate manner.

Commitments to registrant protection

With over a decade of experience protecting domain registration data, Afilias understands registrant security concerns. Afilias supports a "thick" registry system in which data for all objects are stored in the registry database that is the centralized authoritative source of information. As an active member of IETF

(Internet Engineering Task Force), ICANN's SSAC (Security & Stability Advisory Committee), APWG (Anti-Phishing Working Group), MAAWG (Messaging Anti-Abuse Working Group), USENIX, and ISACA (Information Systems Audits and Controls Association), the Afilias team is highly attuned to the potential threats and leading tools and procedures for mitigating threats. As such, registrants should be confident that:
• Any confidential information stored within the registry will remain confidential;
• The interaction between their registrar and Afilias is secure;
• The Afilias DNS system will be reliable and accessible from any location;
• The registry system will abide by all polices, including those that address registrant data;
• Afilias will not introduce any features or implement technologies that compromise access to the registry system or that compromise registrant security.

Afilias has directly contributed to the development of the documents listed below and we have implemented them where appropriate. All of these have helped improve registrants' ability to protect their domains name(s) during the domain name lifecycle.
• [SAC049]: SSAC Report on DNS Zone Risk Assessment and Management (03 June 2011)
• [SAC044]: A Registrant's Guide to Protecting Domain Name Registration Accounts (05 November 2010)
• [SAC040]: Measures to Protect Domain Registration Services Against Exploitation or Misuse (19 August 2009)
• [SAC028]: SSAC Advisory on Registrar Impersonation Phishing Attacks (26 May 2008)
• [SAC024]: Report on Domain Name Front Running (February 2008)
• [SAC022]: Domain Name Front Running (SAC022, SAC024) (20 October 2007)
• [SAC011]: Problems caused by the non-renewal of a domain name associated with a DNS Name Server (7 July 2006)
• [SAC010]: Renewal Considerations for Domain Name Registrants (29 June 2006)
• [SAC007]: Domain Name Hijacking Report (SAC007) (12 July 2005)

To protect any unauthorized modification of registrant data, Afilias mandates TLS⁄SSL transport (per RFC 5246) and authentication methodologies for access to the registry applications. Authorized registrars are required to supply a list of specific individuals (five to ten people) who are authorized to contact the registry. Each such individual is assigned a pass phrase. Any support requests made by an authorized registrar to registry customer service are authenticated by registry customer service. All failed authentications are logged and reviewed regularly for potential malicious activity. This prevents unauthorized changes or access to registrant data by individuals posing to be registrars or their authorized contacts.

These items reflect an understanding of the importance of balancing data privacy and access for registrants, both individually and as a collective, worldwide user base.

The Afilias 24⁄7 Customer Service Center consists of highly trained staff who collectively are proficient in 15 languages, and who are capable of responding to queries from registrants whose domain name security has been compromised–for example, a victim of domain name hijacking. Afilias provides specialized registrant assistance guides, including specific hand-holding and follow-through in these kinds of commonly occurring circumstances, which can be highly distressing to registrants

Security resourcing plans

Please refer to our response to question #30b for security resourcing plans.

© Internet Corporation For Assigned Names and Numbers.

EXHIBIT JMR-13

JMR-13

New gTLD Application Submitted to ICANN by: Charleston Road Registry Inc.

String: web

Originally Posted: 13 June 2012

Application ID: 1-1681-58699

Applicant Information

1. Full legal name

Charleston Road Registry Inc.

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact Information Redacted

4. Fax number

Con ac nforma ion Redac ed

5. If applicable, website or URL

Primary Contact

6(a). Name

Sarah Falvey

6(b). Title

Senior Policy Analyst

6(c). Address

6(d). Phone Number

Con ac nforma ion Redac ed

6(e). Fax Number

6(f). Email Address

Contact Information Redacted

Secondary Contact

7(a). Name

Chris Iannuccilli

7(b). Title

Director of Marketing

7(c). Address

7(d). Phone Number

Con ac nforma ion Redac ed

7(e). Fax Number

7(f). Email Address

Contact Information Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

Corporation

8(b). State the specific national or other jursidiction that defines the type of entity identified in 8(a).

State of Delaware (General Corporations Code)

8(c). Attach evidence of the applicant's establishment.

Attachments are not displayed on this form.

9(a). If applying company is publicly traded, provide the exchange and symbol.

9(b). If the applying entity is a subsidiary, provide the parent company.

Google Inc.

9(c). If the applying entity is a joint venture, list all joint venture partners.

Applicant Background

11(a). Name(s) and position(s) of all directors

Christine Flores	Director

11(b). Name(s) and position(s) of all officers and partners

Donald S. Harrison	Assistant Secretary
James Marocco	CFO and Treasurer
Christine Flores	CEO, President, and Secretary

11(c). Name(s) and position(s) of all shareholders holding at least 15% of shares

Google In.	Not Applicable

11(d). For an applying entity that does not have directors, officers, partners, or shareholders: Name(s) and position(s) of all individuals having legal or executive responsibility

Applied-for gTLD string

13. Provide the applied-for gTLD string. If an IDN, provide the U-label.

web

14(a). If an IDN, provide the A-label (beginning with "xn--").

14(b). If an IDN, provide the meaning or restatement of the string in English, that is, a description of the literal meaning of the string in the opinion of the applicant.

14(c). If an IDN, provide the language of the label (in English).

14(c). If an IDN, provide the language of the label (as referenced by ISO-639-1).

14(d). If an IDN, provide the script of the label (in English).

14(d). If an IDN, provide the script of the label (as referenced by ISO 15924).

14(e). If an IDN, list all code points contained in the U-label according to Unicode form.

15(a). If an IDN, Attach IDN Tables for the proposed registry.

Attachments are not displayed on this form.

15(b). Describe the process used for development of the IDN tables submitted, including consultations and sources used.

15(c). List any variant strings to the applied-for gTLD string according to the relevant IDN tables.

16. Describe the applicant's efforts to ensure that there are no known operational or rendering problems concerning the applied-for gTLD string. If such issues are known, describe steps that will be taken to mitigate these issues in software and other applications.

While the string for which Charleston Road Registry (CRR) is applying, .web, is not an IDN and, therefore, does not contain characters which require mixed right-to-left or left-to-right functionalities, CRR has nonetheless familiarized itself with the requirements and components of the IDNA protocol by reviewing the relevant RFCs and the relevant background information found on the ICANN IDN Wiki. CRR has also tested the .web string for rendering issues; none were found.

17. (OPTIONAL) Provide a representation of the label according to the International Phonetic Alphabet (http://www.langsci.ucl.ac.uk/ipa/).

Mission/Purpose

18(a). Describe the mission/purpose of your proposed gTLD.

18.a. Mission⁄Purpose of the Proposed gTLD

Charleston Road Registry is an American company, wholly owned by Google, which was established to provide registry services to the Internet public. Google is an American multinational public corporation and global technology leader focused on improving the ways its hundreds of millions of users connect with information. Since its formation, Google has been developing technology that can improve upon existing ways of doing business on the Internet. Google provides a variety of services and tools for Internet users and advertisers of all sizes, from simple search features and local ads to enterprise-scale business applications and global advertising solutions. These tools make it easier for people to make use of the world's information and enable entrepreneurs and publishers around the world to grow their businesses.

In line with Google's general mission, Charleston Road Registry's mission is to help make information universally accessible by extending the utility of the DNS while enhancing the performance, security and stability of the Internet for users worldwide. Charleston Road Registry aspires to create unique web spaces where users can learn about products, services and information in a targeted manner and in ways never before seen on the Internet. Its business objective is to manage Google's gTLD portfolio and Google's registry operator business. As discussed further in the responses to questions 23 and 31, Charleston Road Registry intends to outsource all critical registry functions to Google Registry Services.

The proposed gTLD will provide the marketplace with a new all-purpose gTLD for second-level domain names, .web. The mission of this gTLD is to act as an alternative to current gTLDs, in particular .com and .net. This mission will enhance consumer choice by providing new availability in the second-level domain space and increasing competition amongst generic gTLDs. Charleston Road Registry believes that registrants will find value in associating with this gTLD, which could have a vast array of purposes for enterprises, small businesses, groups or individuals seeking a second-level domain name already registered in .com or .net, or those simply seeking a competitive alternative to existing gTLDs. This assertion is supported by industry data: over 375,000 new second-level domains were registered in January 2012 in the .com and .net gTLDs, and the two gTLDs support a total of 115 million second-level domains -- more than 80% of all second-level domains registered in one of the 6 open U.S. gTLDs (.com, .net, .info, .org, .biz, .us) [Source: http:⁄⁄www.dailychanges.com⁄].

The proposed gTLD will also provide Charleston Road Registry with the means to meet its business objectives.

18(b). How do you expect that your proposed gTLD will benefit registrants, Internet users, and others?

18.b. Benefits to Registrants, Internet Users, and Others

18.b.i.1 Specialty

The goal of the proposed gTLD is to create a new Internet environment that provides registrants, Internet users, and the public with the opportunity to associate with a meaningful term. Specialization will arise from this environment through market dynamics as entities align their offerings with the term.

The specialization goal of .web is to provide an alternative, general purpose gTLD that offers consumers more choices to align their web spaces to a generic gTLD than the existing options today.

18.b.i.2 Service Levels

Through its association with Google, Charleston Road Registry is uniquely positioned to enable and support the proposed gTLD by providing its service reliability and speed of delivery as a part of its services. Google brings unique expertise and a proven record of excellence in infrastructure operations: Google now runs the largest DNS system in the world, has industry-leading uptime on its services, such as web search, and offers enterprise services on which governments and businesses depend.

Google is known for its high level of quality and speed, and Charleston Road Registry's service level goal for the proposed gTLD is to extend that high level of quality, speed, and service to registrars. Indeed, two of Google's core principles in providing Internet search and related goods and services are "focus on the user and all else will follow" and that "fast is better than slow."

Charleston Road Registry is committed to using the most technologically advanced, secure, and reliable registry services for all of the domain names in the gTLD so as to not compromise the service levels, security, and stability of the gTLD to users worldwide.

Charleston Road Registry will provide both Engineering and Customer Service support to registrars. All registrars will also have the same level of access to Charleston Road Registry resources to resolve disputes and technical and/or administrative customer service issues.

Charleston Road Registry will provide all registrars with 24-hours-a-day, 7-days-a-week Customer Support in the form of telephone, email, and/or web chat for technical and non-technical issues relating to the operation of the gTLD system. Charleston Road Registry will provide all registrars with the same level of access to customer support via telephone, email, and Charleston Road Registry's website; email and web-based interactions will be the primary method of provisioning customer service support to registrars.

Additionally, Charleston Road Registry will implement strict policies and procedures to minimize abusive domain name registrations and uses and other activities that have a negative impact on Internet users. It will dedicate ample resources for the purpose of responding promptly to abuse complaints from government, judicial and/or law enforcement.

18.b.i.3 Reputation

Google has a proven record of providing high-quality, secure online services. Charleston Road Registry seeks to enhance Google's reputation for excellence, superior quality, and high level of security and become known as an exemplary domain name services provider. When registrants assess opportunities in the marketplace to obtain a name, they will have confidence in Charleston Road Registry's ability to meet ongoing needs as the registry operator for the proposed gTLD. When Internet users visit a domain name in the proposed gTLD environment, they will be able to reliably expect and experience the high level of security and quality on which Google's reputation has been built.

The registry will be structured so that Charleston Road Registry allows registrars to register and oversee second-level domain names in the proposed gTLD; that registrars develop and deploy a reasonable process for ensuring that those domain names are used for gTLD-relevant purposes as specified in the registry-registrar agreement; and per Specification 4 that the WHOIS is thick and reliable; and that the registry is responsive to legal rights owners (if applicable) who may have complaints about potentially abusive registrations.

In addition, Charleston Road Registry's operation of the new gTLD will provide the opportunity for registrars and registrants to build and/or bolster their unique brands and brand reputation in association with the proposed gTLD.

18.b.ii.1 Competition

Charleston Road Registry supports the advancement of registry operators as a whole and the diffusion of gTLDs amongst diverse stakeholders to generate increased competition for the benefit of the Internet public. Increased competition will result in more competitive prices for consumers, generate efficiencies and increase productivity in enterprises, and spur innovation in the gTLD space.

The proposed gTLD, .web, will provide a new online structure for the aggregation of other level domain-specific content. As an alternative to existing second-level domains, Charleston Road Registry anticipates that the .web gTLD will increase competition among registrars by increasing consumer choice and creating new opportunities for registrar pricing differentiation. Charleston Road Registry also anticipates the .web gTLD will help grow the volume of entities and individuals offering content online, thereby increasing competition among such entities and individuals to provide new, unique, and more relevant content and offerings.

Managing this Internet space will allow Charleston Road Registry to provide to registrars and registrants the high level of technical operations quality and service for which Google is known, which in turn will incent other existing and new gTLDs to improve the quality of their offerings.

Charleston Road Registry will facilitate a fair and equitable registrar process, providing open access to any registrar who meets ICANN accreditation guidelines by fully complying with the Registry Operator Code of Conduct. Charleston Road Registry is committed to treating all registrars equitably and will not offer preferential treatment to Google in its capacity as registrar.

18.b.ii.2 Differentiation

Charleston Road Registry believes in the commercial viability of alternatives to existing gTLDs such as .com and .net. The proposed gTLD will provide the marketplace with opportunities for differentiation not currently available in the gTLD space.

The .web gTLD providers registrants with the opportunity to differentiate from other web spaces based on their word choice within the second-level domain name.

Given its association with Google, Charleston Road Registry offers a unique value proposition to registrars resulting from the strength of Google's trusted brand, technical leadership, and support for free speech on the Internet. Registrars will have the opportunity to leverage this brand in devising their own market positions.

18.b.ii.3 Innovation

The proposed gTLD will foster innovation by creating a new space for the categorization and classification of online content. It will therein provide a mechanism by which registrars and registrants can better brand and manage their online presence by associating it with the .web namespace. This namespace delivers value to the public through the provision of new and differentiated content, goods, and services to Internet users.

The proposed gTLD provides registrars with the opportunity to create and offer tailored new products and services that benefit registrants and/or improve user experience in association

with the registration of a second-level domain in the .web gTLD.

In addition, the proposed gTLD will promote innovation in the marketplace by providing additional second-level domain options for the public's use. This will invite new entrants to establish a domain name presence, facilitating innovation in their offerings, and their interactions with Internet users.

Charleston Road Registry considers the proposed gTLD to be a platform for innovation with existing and future Google products and services. Charleston Road Registry, therefore, may incorporate these new offerings into future registry service options (subject to the ICANN approval process), infusing new ideas into the gTLD for the betterment of the public.

Google consistently aims to improve upon technologies that connect people with information, as demonstrated by a proven record of innovation and iteration. Charleston Road Registry strives to offer its constituents this same level of continuous development in advancing its management and operation of the gTLD, engendering benefits to registrars, registrants, and end users.

18.b.iii User Experience

Charleston Road Registry will strive to provide the highest level of user experience through operational stability, security, and performance to serve the interest of registrants in the proposed gTLD. Charleston Road Registry is uniquely positioned to provide this level of experience given its relationship with Google; Google invested over $3 billion in its IT infrastructure in 2011 and maintains a record of excellence in infrastructure operations.

The proposed gTLD will provide registrants with the opportunity to differentiate their dedicated domain space such that the end users are able to discern the type of content intended to be found within the proposed gTLD. This will enable increased user visibility of registrants' offerings, as well as provide registrants with the opportunity to enhance their respective content offerings and innovate in new ways.

The proposed gTLD will provide a more trusted and user-friendly environment where domain names and content related to the .web gTLD can flourish. Charleston Road Registry seeks to have users deem the gTLD trustworthy and reliable and recognize it as an aggregated source of targeted goods, services, and information.

The proposed gTLD, furthermore, facilitates an improved online user experience through greater structure and categorization on the Internet.

18.b.iv Registration Policies

Charleston Road Registry believes that given its wide variety of uses, the .web gTLD will best add value to the gTLD space by remaining totally open and unencumbered by registrant restrictions. There will, therefore, be no restrictions on second-level domain name registrations in the proposed gTLD, .web.

Charleston Road Registry will make access to Registry Services, including the shared registration system, available to all ICANN-accredited registrars. Domain names within the proposed gTLD will be available to the general public for registration and use.

Charleston Road Registry is committed to implementing strong and integrated intellectual property rights protection mechanisms. Doing so is critical to Google's goals of model Internet citizenship and fostering Internet development, especially in emerging regions. Accordingly, Charleston Road Registry intends to offer a suite of rights protection measures, which builds upon ICANN's required policies while fulfilling our commitment to encouraging innovation, competition and choice on the Internet.

18.b.v Protection of Privacy and Confidential Information

Charleston Road Registry will strive to ensure the appropriate level of privacy and security will be met for its users. Charleston Road Registry and its provider of registry services, Google, have imposed measures to achieve this protection; additional specifics regarding the practices for the registry include but are not limited to the following:

- All data transmitted from registrars to the registry will be encrypted using transport layer security (TLS) or other similar data protection schemes to ensure that third parties cannot access personally identifying information or other sensitive data as it crosses the Internet.

- Charleston Road Registry will attempt to prevent the misuse of WHOIS data for improper purposes such as spam, intellectual property theft, or phishing. Charleston Road Registry will attempt to identify patterns of abusive usage of the WHOIS and will appropriately use CAPTCHA, query throttling or other techniques to prevent information scraping.

- Google will restrict access to data and information systems maintained by the registry to a specific list of individuals involved with supporting the Google Registry system in production. Google will review this list on a periodic basis to ensure that the level of access granted to individuals is appropriate. Google uses two-factor authentication and other mechanisms to ensure that staff with access to user information are properly identified prior to using registry systems.

- Google data backups stored offsite are encrypted with passwords that are securely managed on Google's internal systems. Google can effectively remove the ability to access this data by destroying the relevant encryption password.

- Supplying Google account information will be optional for registrants unless the domain registration is directly associated with another Google product offering. Google will not disclose Google account information except for any contact information provided by the user that is required by ICANN (per Specification 4) to be displayed in response to a WHOIS query.

- Registrar billing and payment information will not be stored alongside domain name registration information. All registrar billing and payment information will be stored in a payment card industry (PCI)-compliant billing system similar to that used by Google Ads.

- Data will not be shared with third parties without the permission of registrants, except as required for registry operations or as required under the law, such as in response to a subpoena, other such court order, or demonstrated official need by law enforcement.

Beyond these specific mechanisms, both Charleston Road Registry and Google will govern its approach to privacy by the Charleston Road Registry Privacy Policy. This policy applies to registrars, registrants and end users of registry services such as DNS zone publication and WHOIS data publication. The Privacy Policy is located at http://charlestonroadregistry.com/privacy.html.

18.b.vi. Outreach and Communications Efforts

Once Charleston Road Registry begins developing public-facing resources in its gTLD, it intends to inform the public about the gTLD and the opportunity to obtain domain space there through investments in marketing and public relations.

Charleston Road Registry intends to promote gTLDs in its portfolio, such that the public gains an awareness and understanding of new gTLDs and the availability of new second-level domain space on the Internet. Charleston Road Registry believes that this approach will make the strongest impact in modifying consumer behavior and is the best path to achieving success for all new gTLDs collectively.

Charleston Road Registry will reach out to the Internet community via a number of different outreach and communications methods and venues to deliver its mission and message to the public, including but not limited to: press briefings, videos posted on various Internet sites, blogs and other social media, and paid advertising. In addition, when developing resources for localized Internet registrars in different global regions, Charleston Road Registry will use local marketing and communications platforms as needed.

18(c). What operating rules will you adopt to eliminate or minimize social costs?

18.c. Minimizing Social Costs and Other Negative Consequences

18.c.i
Registration will be managed by Charleston Road Registry in three phases.

Phase 1 - The first phase will be an extended 60-day sunrise phase. Only owners of trademarks listed in the Trademark Clearinghouse may participate in this phase, and such owners may register domain names that consist of an identical match to their listed trademarks. If multiple qualified parties express an interest in registering the same domain name, Charleston Road Registry will award the domain name through an auction or other predetermined process that will be published prior to the Sunrise Period. At the end of the sunrise phase, at a minimum, Charleston Road Registry will follow ICANN rules for subsequent attributions of trademarked second-level domains and will offer other protections for trademark owners, including but not limited to an extended Trademark Claims Service of indefinite length.

Phase 2 - The second phase will be a limited term registration phase. During this phase, any interested applicant may apply for all second-level domain names not previously registered in the sunrise period. Trademarked terms will be subject to the Rights Protection Mechanisms set forth in Response 29. At the end of the second phase, if multiple parties have expressed an interest in registering the same second-level domain name, Charleston Road Registry will award the domain name through an auction auction or other predetermined process that will be published prior to the commencement of this phase.

Phase 3 - The third phase will be a steady state phase for the duration of registry operation. During this phase, any interested applicant may apply for all second-level domain names not previously registered in an earlier phase. Trademarked terms will be subject to the Rights Protection Mechanisms set forth in Response 29. If multiple parties express an interest in registering the same d/main name, Charleston Road Registry will award the domain name on a strictly first come, first served basis.

18.c.ii
While Charleston Road Registry reserves the right to charge different prices for unique second-level domains within the gTLD, once Charleston Road Registry determines the price for a particular second-level domain, Charleston Road Registry will not price discriminate among ICANN-accredited registrars. Charleston Road Registry does not intend but reserves the right to offer introductory discounts and bulk registration discounts. Volume discounts, marketing support and incentive programs may be made available, and if so will be offered to all ICANN-accredited registrars without preference.

18.c.iii
Pursuant to the ICANN-Registry Operator Agreement, Charleston Road Registry will provide written notice a minimum of 30 days prior to any increases in price for initial registrations, as well as written notice 180 days prior to any increase in registration renewals. Further, Charleston Road Registry will offer uniform pricing for renewals as specified in the ICANN-Registry Operator Agreement.

Charleston Road Registry does not currently intend to make contractual commitments to registrants regarding the magnitude of price escalation. Charleston Road Registry does, however, intend to keep its practices competitive and aligned to activity in the marketplace.

Community-based Designation

19. Is the application for a community-based TLD?

No

20(a). Provide the name and full description of the community that the applicant is committing to serve.

20(b). Explain the applicant's relationship to the community identified in 20(a).

20(c). Provide a description of the community-based purpose of the applied-for gTLD.

20(d). Explain the relationship between the applied-for gTLD string and the community identified in 20(a).

20(e). Provide a description of the applicant's intended registration policies in support of the community-based purpose of the applied-for gTLD.

20(f). Attach any written endorsements from institutions/groups representative of the community identified in 20(a).

Attachments are not displayed on this form.

Geographic Names

21(a). Is the application for a geographic name?

No

Protection of Geographic Names

22. Describe proposed measures for protection of geographic names at the second and other levels in the applied-for gTLD.

As specified throughout this application, Charleston Road Registry (CRR) plans to implement comprehensive anti-abuse mechanisms. CRR will protect against the abusive registration of geographic names at the second and other levels in the applied-for gTLD by reserving to the registry protected geographic names in order to prevent registration of such strings.

In that regard, CRR has thoroughly reviewed Specification 5 of the Registry Agreement, the Government Advisory Committee's (GAC) "Principles Regarding New gTLDs", and the .info methodology for reservation and release of country names. Accordingly, CRR will, in connection with its registry services operator and registrar, initially reserve from registration by any party names with national or geographic significance within the TLD during the TLD's Sunrise Period and Trademark Claims Period.

The names with national or geographic significance (hereto referred to as "geographic names") that will be initially blocked are those specified in Specification 5 of the New gTLD Registry Agreement, namely:

(1) The short form (in English) of all country and territory names contained on the ISO 3166-1 list, as updated from time to time, including the European Union, which is exceptionally reserved on the ISO 3166-1 list, and its scope extended in August 1999 to any application needing to represent the name European Union;
(2) The United Nations Group of Experts on Geographical Names, Technical Reference Manual for the Standardization of Geographical Names, Part III Names of Countries of the World; and
(3) The list of United Nations member states in 6 official United Nations languages prepared by the Working Group on Country Names of the United Nations Conference on the Standardization of Geographical Names.

As noted above, the top-level domain shall not permit the public to register domain names with national or geographic significant at the second-level. The names will be set aside by use of the Reserved state making them inaccessible (See response to Question 27 for details). Google, as the registry services provider, has arranged for such reservation to occur prior to the launch of the TLD.

In the event there is a compelling use of a two-character geographic name, the two-character label string may be released to the extent that CRR reaches agreement with the government and country-code manager and consults with the GAC and ICANN. The Registry may also propose the future release of these reserved names based on the implementation by the prospective registrant of measures to avoid confusion with the corresponding country codes.

As with the .info TLD, only if a potential second-level domain registrant makes a proper showing of governmental support for country or territorial names will CRR relay this request to ICANN. CRR also plans to consult with the GAC and of ICANN before proceeding to delegate the domain at issue.

Registry Services

23. Provide name and full description of all the Registry Services to be provided.

Charleston Road Registry (CRR) will outsource the entirety of its technical operations to Google. In addition to running the technical platform, Google will provide CRR with staffing and support to ensure that all registry services meet both the requirements laid out by ICANN in the new generic top-level domain (gTLD) Applicant Guidebook as well as in the gTLD registry agreement. Additional details of Google's provision of services to CRR are set forth in Question 31, Section 31.1.

By making use of Google's Registry platform, CRR will provide the following registry services:

- Receipt of data from registrars concerning registration of domain names and name servers

- Dissemination of top-level domain (TLD) zone files
- Dissemination of contact or other information concerning domain name registrations (WHOIS service)
- Internationalized Domain Names (IDN) Support for all domain names
- Domain Name System Security Extensions (DNSSEC) support
- IPv6 Support
- Data escrow
- Redemption grace period for domain names
- Registrar and developer account creation

“Q23_Registry Services Diagram” shows major services being exposed by high-level systems. Note that this diagram shows only data flow and does not specify the physical deployment characteristics of these services.

Details on these services are discussed below.

23.1. Receipt of Registration Data

Google will receive registration data from users in a manner consistent with standard registry operations. This will be handled via the extensible provisioning protocol (EPP) interface through ICANN-accredited third-party registrars. Google will operate a robust Shared Registration Service (SRS) that allows registrars to add, modify, and delete domain registrations and provides full support for the domain registration lifecycle.

Google’s shared registration system (SRS) infrastructure consists of three major components: an extensible provisioning protocol (EPP) server that provides an EPP interface to registrars; the Google SRS Frontend, which provides web-based access to the state of the Google Registry, the registrar’s profile and access to registration reports for the registrar; and the Google SRS Backend, which implements most business logic, interacts with the data store, and pushes updates to DNS and WHOIS servers in order to disseminate TLD Zone files as well as registrant contact information.

Details of the SRS are described in Question 24, EPP support in Question 25, and the registration lifecycle in Question 27.

23.2. Dissemination of TLD Zone Files

TLD zone data will be propagated in near real time to Google’s Authoritative DNS infrastructure, which will serve as the primary means of publication of the TLD zone files. This DNS infrastructure is based on Google’s existing Public DNS product, which handles over 70 billion queries per day. This DNS implementation will be fully compliant with RFCs 1034, 1035, 1982, 2181, 2182, 2671, 3226, 3596, 3597, 3901, 4343, 4472, 4972, and 5966 as well as ICANN’s Specification 10. A full description of Google’s Authoritative DNS infrastructure is described in Question 35.

In addition to real-time publication via port 53, the Google Registry will also support publication of the entire zone, as described below:

The master zone file will be internally generated and cached in the Google Shared Registration System (GSRS) as modifications to GSRS’s persistent store are made. The zone data will be signed by the Authoritative DNS infrastructure; a copy of the signed data is also returned to the GSRS. The entire master zone file will then be available to authorized parties at an HTTP URL shared with them over the web.

The master zone file at this location will be guaranteed to be no more than one hour old.

When retrieving the zone file, the client will pass a single HTTP request parameter (“key”), in order to identify individually the qualified client requesting access. This parameter will be the API key given to the registrar during account signup.

The mimetype “text/dns” will be set on the HTTP response and the content encoding will be gzip.

The master zone file will follow the format specified by RFC 1035, with the additional

restrictions as specified in Specification 4, Section 2.1.4 of the gTLD Applicant Guidebook. DNSSEC resource records will also be present.

In addition, the master zone file will be made available through the Centralized Zone Data Access Provider as specified in Specification 4, Section 2.1.4 of the gTLD Applicant Guidebook.

23.3. Dissemination of Contact Information (WHOIS)

Google will create an implementation of the WHOIS protocol (as defined by RFC 3912) that will listen on port 43 for WHOIS requests. Google's WHOIS service will communicate to the name registry through a private API end-point in order to retrieve the necessary information for WHOIS responses. In addition, Google will operate a public WHOIS, web-based Directory Service at 〈WHOIS.nic.web〉 providing free, public query-based access. Both traditional WHOIS and web-based WHOIS will be made available over both IPv4 and IPv6.

As required by Specification 4 in the gTLD Applicant Guidebook, Google's WHOIS service will perform in the following manner:
- Semi-free text format followed by a blank line and disclaimer specifying the rights of the Registry Operator, and user querying the database.
- Each data object shall be represented as a set of key/value pairs, with lines beginning with keys, followed by a colon and a space as delimiters, followed by the value.
- For fields where more than one value exists, multiple key/value pairs with the same key shall be allowed.
- The first key/value pair after a new-line starts a new record, and is used to identify the record itself.
- The format of fields governed by EPP RFCs 5730-5734 (domain status, individual and organizational names, address, street, city, state/province, postal code, country, telephone and fax numbers, email addresses, date and times) will be formatted as specified by those RFCs.

Updates to WHOIS data will be made in near real-time, with the registry's service level agreement (SLA) committing to 95% of the updates reaching the serving infrastructure within 15 minutes. Details of WHOIS support are included in Question 26.

23.4. Internationalized Domain Names

IDNs allow registrars to register domain names with unicode code points representing non-ASCII-based character sets. IDNs constrained by the IDN Tables for this TLD will be supported by the Google Registry. Google's IDN implementation will make use of the IDNA standard and be fully compliant with both RFCs 5890-5893 and ICANN's IDN implementation guidelines. For more information on the IDN implementation for the TLD, see Question 44.

23.5. DNS Security Extensions

The Google Registry will support DNSSEC. In particular, registrants will be able to specify a DS record as part of normal domain name registration with their registrars, which will be transmitted to the Google Registry via its EPP interface. The Google Registry will then sign the DS record, along with all other DNS resource records in the TLD Zone, forming a chain of trust between the Google Registry and second-level domain name. The Google Registry itself will publish its own DS record with the root. Google's DNSSEC implementation will be fully compliant with RFCs 4033, 4034, 4035, 5910, 4509, 4641, and 5155. More information on this topic, including the DNSSEC Policy statement for the TLD is contained in Question 43.

23.6. IPv6 Support

The Google Registry operates on Google's production network, which supports IPv6. Specifically, the Google Registry will specifically support IPv6 access to all registry service endpoints (WHOIS, EPP, DNS, etc.). All services are provided through dual-stack, which is considered the industry-standard best practice for supporting IPv6. In addition, domain name registrants will be able to create IPv6 AAAA glue records for nameservers in the TLD zone. Further detail about Google's IPv6 implementation is available in Question 36.

23.7. Data Escrow

Google will escrow relevant registration data, as required by ICANN's registry agreement. Google will ensure that its data escrow will be fully ICANN compliant and performed in accordance to industry best practices. In addition to Google's practice of hosting critical data on redundant and geographically disparate datacenters, data escrow will provide further assurance against data loss and ensure that all Google Registry data can be retrieved in a timely manner. For more information on Data Escrow, see Question 38.

23.8. Redemption Grace Period for Domain Names

After a domain name has been deleted by a registrar, the domain name shall move into a Redemption Grace Period. The status of the domain will be listed as PENDING DELETE RESTORABLE. When a domain is in this state, it is deleted from the zone for the TLD. This is a strong indicator to the registrant that it must act take action in order to restore the domain to its previous state. For details, see Question 27.

23.9. Creation of Registrar and Developer Accounts

Google's Registry will use Google Accounts to manage registrars.

To create a Google Account, all parties will be directed to the following URL:

http://www.google.com/accounts

Once a prospective registrar or developer has created an account in Google, the registrar or developer can upgrade from a standard Google account to a registrar and/or developer, if certain requirements are met.

To obtain a set of credentials used to interact with the Google Registry, a registrar will proceed through the following workflow:
A. The Google registrar logs in with Google account credentials.
B. The Google registrar submits an application identifying that it is an accredited ICANN registrar, and that it wishes to interact with the Google Registry.
C. The Google registrar requests and resets initial EPP credentials, which are separate from a Google account.

Once a Registrar has been certified and authorized for billing, they will be ready to interact with Google through Google EPP. At this point, the registrar can also view reports on domains registered, EPP transactions, remaining account balance, and other TLD registry statistics.

"Q23_Registrar Registration Process Diagram" shows the registration process for registrars.

In addition to registrars, Google will also provide accounts to developers and other authorized users, who will obtain credentials through the following workflow:
A. The developer logs in the previously created Google account.
B. The developer requests an API key to be used for all public API calls.
C. The developer reviews access restrictions, quota, and service-level agreements and agrees to appropriate terms.
D. Google Registry grants access to zone data exported by the domain.

"Q23_Developer Registration Process Diagram" shows the registration process for developers.

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

All Shared Registration System (SRS) services described in Question 23 will run on Google's robust, high-performance platform. Google's production platform is an extremely high-capacity, high-availability, scalable platform designed to support some of the most resource-intensive and often-used applications on the Internet, including Google Search, Gmail, and YouTube. Google builds large clusters out of thousands of individual servers. Google uses a common set of tools to allocate resources, provide access to basic services such as storage and locking, and to simplify programmers' ability to build distributed systems using the cluster's hardware. Rather than relying on expensive hardware to provide reliability, Google uses a more cost effective approach based on commodity components, and builds fault tolerance into its software. Google simultaneously increases performance, reliability, and scalability of our production systems by splitting work into shards and running multiple replicas of the same process.

The numbered sections below discuss details of our SRS implementation and capacity plans.

24.1. Google SRS (GSRS)

The Google Shared Registration System (GSRS) will provide all standard registry services:

- Receipt of data from registrars concerning registration of domain names and name servers
- Dissemination of top-level domain (TLD) zone files
- Dissemination of contact or other information concerning domain name registrations (WHOIS service)
- Internationalized Domain Names Support for all domain names
- Domain Name System Security Extensions (DNSSEC) support
- IPv6 Support
- Data Escrow

For descriptions and details of all SRS functions, see Question 23.

24.2. Google SRS Components

GSRS will be a multi-tier application that consists of the following components.

- Google SRS Front End (GSRS-FE): Presentation. A web application which provides an interface between registrars, developers, and other parties that need access to Google Registry information through a web interface. GSRS-FE will also include a web-based WHOIS interface.
- Google SRS Back End (GSRS-BE): Business Logic. A representational state transfer (RESTful) service that exposes and controls all registry data. Most business logic related to registry data storage and persistence will be implemented in GSRS-BE.
- Google EPP (GEPP): API Proxy. A public end-point for EPP (Extensible Provisioning Protocol) for the top-level domain. GEPP will translate all EPP requests and responses to interface with GSRS-BE. For more information on EPP support, see Question 25.
- Google WHOIS (GWHO): A public end-point for WHOIS queries for the top-level domain. GWHO will translate all WHOIS requests and responses to interface with the GSRS-BE. For more information on WHOIS support, see Question 26.

In addition, GSRS will integrate with the following internal systems. These internal systems are designed for extremely high performance and robustness, and use the same technologies used for other high-capacity services currently in production.

- Google Persistence Service (Persistence): A multi-master persistence solution which will run on top of Google's proprietary database, BigTable. The Google Persistence Service coordinates between masters using an algorithm for fault-tolerant distributed systems, such as Paxos. BigTable is Google's internal implementation of a distributed hash table used for the majority of our persistence needs.
- Google Accounts (Authentication): An existing platform for creation and authentication of user accounts. Google Accounts provides a standard login page for all Google products, as well as programmatic access for internal applications to retrieve credentials for the logged-in user.
- Google Monetization (Billing, as needed for the TLD): A monetization and billing system. Enables Google products to create accounts, create invoices, and perform financial transactions for Google customers.
- Google Authoritative DNS (Master Zone File): A robust public DNS server. Google

Authoritative DNS will receive master zone file information from the GSRS-BE and distribute DNS information to clients.

“Q24_SRS Services Diagram” shows the interactions with these systems as requests come into a Google datacenter and are handled appropriately. Note that, as shown in “Q24_SRS Services Diagram”, all SRS requests are passed to the GSRS-BE, which contains all business logic for Google Registry. Integrated services are then used as needed. Google plans to provision these services to handle significantly greater load than our most aggressive expectations -- see below for details.

24.3. Google SRS Deployment Parameters

Google plans to deploy GSRS in five geographically-distributed datacenters throughout North America. Traffic to these datacenters is dynamically adjusted according to load, and the system will be provisioned to allow two simultaneous datacenter outages without substantial performance impact.

Each datacenter will include several replicas to handle specific machine failures for any GSRS service. Google’s production servers include the ability to expand to add new servers dynamically according to need. If SRS performance suddenly requires additional throughput capacity -- for instance, during a Distributed Denial of Service (DDoS) attack -- Google will be able to enable up to 100 additional replica servers in any datacenter dynamically. The limit of 100 additional replica machines is a self-imposed limit and may be revised upward based on ongoing operational considerations.

Each machine will be able to support a minimum of 250 queries per second (read or write), where one query contains one record. For architectural simplicity, our initial implementation will read data without any additional SRS-level caches.

24.4. GSRS Performance Scaling

Google plans to deploy sufficient capacity to handle SRS request load on the same scale as the largest top-level domains on the Internet. These computations are detailed in “Q24_GSRS Performance and Scaling”.

The key factor for scaling GSRS performance capacity will be the GSRS-BE component. Other components for GSRS (both GSRS-FE and GEPP) will receive user requests and then transform them into Remote Procedure Call (RPC) calls to GSRS-BE. GSRS-FE and GEPP will not perform any CPU-, disk-, or memory-intensive computations themselves. The performance capacity estimations below will therefore discuss only GSRS-BE capacity.

Based on existing domains and calculations for inbound traffic, Google estimates that there will be about 2300 queries per second for EPP operations, consisting mostly of checks for existing domains, and 3600 queries per second for WHOIS operations. In total, Google estimates that GEPP-BE must handle roughly 5900 queries per second for a scale of 100 million domains. Other operations, such as zone file operations and developer API calls, will create a relatively negligible level of load.

Google will meet the SRS throughput requirement, with a 50% utilization rate, with 48 machines allocated across the five datacenters. At this level of utilization, our active capacity will be double the expected throughput requirement. If a datacenter is lost through a production outage or change request, then additional machines will be enabled immediately to take upon the additional load with no manual intervention required. Google production systems have the standard capability to enable new machines to handle increased capacity needs immediately.

These estimations do not include any smart caching anywhere in the architecture. If the Google Registry reaches a very large number of domains and additional capacity measures are required, Google will consider a design for an appropriate WHOIS and EPP check result caching plan to relieve load and to improve latency characteristics.

These estimates use a very aggressive set of assumptions for scaling, which should be sufficient for a large open domain.

24.5. GSRS Network Scaling

Google expects that our SRS network bandwidth requirements will be greatly below Google's existing per-datacenter network capacity, even for its lowest-capacity datacenters in production. Details of its computations are included below.

Google assumes that 99% of RPC calls across both EPP and WHOIS will be less than 5 kB. EPP and WHOIS queries return more of a fixed number of records, and most queries will return only one record. 5 kB is derived as an estimate from taking the sample WHOIS output in the applicant guidebook, and multiplying it by three to account for XML inflation as if the same information passed through an EPP interface. Considering that most EPP commands are expected to be 〈check〉 commands, this is a very conservative estimate.

Google then uses 5 kB as the assumed size to calculate the estimates for bandwidth per machine and per datacenter at maximum load.

Network Bandwidth Requirements per Machine = Queries per Second * Size of RPC Calls

With 250 qps and 5 kB per query, Google expect a maximum of about 12.5 MB⁄s of bandwidth requirement. This is about one-eighth of our current absolute minimum commodity standard of 1 Gb Ethernet. Our backbone routers connect many metro networks around the globe at 10Gb or greater.

Network Bandwidth Requirement per datacenter = Requirements per Machine * Number of Machines

With 12.5 MB⁄s of bandwidth per machine, and 100 machines maximum per datacenter, Google expects a maximum of about 1.25 GB⁄s data requirements during a major event that requires increased load demand. All Google datacenters' connections to its production network have a multiple 10 GB⁄s links, and many exceed this by far.

Based on these computations, Google believes that the network bandwidth required by the SRS system for as many as 100 million second-level domains will never exceed the capacity that even our smallest datacenter can provide.

24.6. Multi-Master Design

GSRS will use a multi-master architecture. This architecture is detailed further in Question 32. Machines across multiple datacenters will serve active traffic, with no machines on cold or hot standby. All instances of the data store update in real-time, and updates to registry data are committed across a quorum of replicas before the write is confirmed. When GSRS or a dependent service goes down or is drained by an outage, Google's network architecture will redirect all affected traffic to another datacenter. Google will design most services as stateless, so service instances will not require any coordination mechanisms.

24.7 Google SRS Adherence to Specification 6

The Google Registry, and in particular the SRS will be compliant with all RFCs outlined in Specification 6. Any RFCs mentioned below and their successors will be complied with.

24.7.1 - Standards Compliance

24.7.1.1 DNS

Google's domain name system (DNS) implementation will comply with RFCs 1034, 1035, 1982, 2181, 2182, 2671, 3226, 3596, 3597, 4343, and 5966. See Question 35 for more details on DNS RFC implementation compliance.

24.7.1.2 EPP

Google's EPP implementation will comply with RFCs 5910, 5730, 5731, 5732, 5733, 5734, 3915, and 3735 for any extensions developed. Please see Question 25 for more details on EPP RFC implementation compliance.

24.7.1.3 DNSSEC

Google's DNSSEC implementation will comply with RFCs 4033, 4034, 4035, 4509, 5155, and the best practices indicated in RFC 4641. A DPS statement will be published for each TLD supported by the Google Registry. Please see Question 43 for more details on DNSSEC implementation compliance.

24.7.1.4 IDN

Google's implementation of internationalized domain names (IDN) will comply with RFCs 5890, 5891, 5892, 5893 and ICANN's published IDN Guidelines. Please see Question 44 for more details on IDN RFC implementation compliance.

24.7.1.5 IPv6

Google's implementation of IPv6 will follow BCP 91 and RFCs 4472. All Registry services will be offered over IPv6. Please see Question 36 for more details on Google's IPv6 implementation.

24.7.2 Registry Services and Wildcard Prohibition

Google understands the definition of "registry services" as defined in section 2.1 of Specification 6. Google will not support wildcard matching or resolution in the TLD zone as required by Section 2.2 of Specification 6.

24.7.3 Registry Continuity

Google will ensure registry continuity as specified in Section 3 of Specification 6. High availability, extraordinary event handling, and business continuity will be provided with respect to the TLD. See Question 39 for more details on Google's Registry continuity plan.

24.7.4 Abuse Mitigation

Google will implement the abuse mitigation requirements as specified in Section 4 of Specification 6. An abuse contact will be made available. See Question 28 for more details on Google's abuse handling. Google will also take action to remove malicious use of orphan glue records when provided evidence in written form that such records are present in connection with malicious content.

24.7.5 Supported Initial and Renewal Registration Periods

Google will implement the supported initial and renewal registration periods as specified in Section 5 of Specification 6. The Google Registry will support domain name registration with validity periods of between one to 10 years in increments of one year. Renewal registration may extend registration to a maximum of 10 years from renewal date in increments of one year.

24.8. Google SRS SLA and Adherence to Specification 10

The Google SRS will significantly exceed the requirements of the Service Level Requirement Matrix defined in Specification 10 in the gTLD Applicant Guidebook. All EPP and WHOIS/RDDS calls supported by the Google SRS system will have a 99.9% monthly uptime.

For the purpose of measuring this commitment, Google uses the following definitions:
RPC: A series of TCP/IP packets forming a distinct request, and the corresponding TCP/IP packets forming the response.
Error RPC: An RPC which does not return with 3x 95th percentile latency, or which fails because of internal transient errors.
Error Minute: Any minute during which 10% of RPC requests are error RPCs.
Monthly Uptime: The total number of minutes in a month minus the number of error minutes divided over the total number of minutes in the month, rounded to the nearest .01%.

When calculating monthly uptime percentage, Google does not distinguish between scheduled and unscheduled downtime.

Google will meet or exceed all service level agreements (SLA) described in the ICANN Applicant Guidebook. Specifically, Google will meet the commitments as specified in attachment "Q24_SLAs". Note that the values represent a commitment to exceed SLA Requirements in

Specification 10.

DNS
- DNS Availability: 0 minutes of downtime.
- DNS Name Server Availability: Less than 31 minutes of downtime per month (At least 99.93% availability)
- TCP DNS resolution RTT: 300ms for at least 95% of the queries
- UDP DNS resolution RTT: 300ms for at least 95% of the queries
- DNS update time: 15 min, for at least 95% of the probes

RDDS (WHOIS)
- RDDS Availability: Less than 43 minutes of downtime per month. (At least 99.9% availability)
- RDDS Query RTT: Less than 400 ms.
- RDDS Update Time: Less than 15 minutes for 95% of probes.

EPP
- EPP Service Availability: Less than 43 minutes of downtime per month. (At least 99.9% availability)
- EPP Session-Command RTT: Less than 1000 ms for at least 95% of commands.
- EPP Query-Command RTT: Less than 400 ms for at least 95% of commands.
- EPP Transform-Command RTT: Less than 800 ms for at least 95% of commands.

Downtime values are on a monthly basis.

Google has the track record to deliver SRS to 99.9% availability. Google is confident in its ability to meet these SLAs for SRS because of its experience with engineering highly-available platforms. As discussed by Urs Hoelzle, Senior Vice President of Technical Architecture, Google has designed its major services to obtain 99.99% reliability [1].

24.9. SRS Technical Support

Charleston Road Registry will provide registrars with access to telephone, email, and web chat support, and will escalate issues to the Google technical team as technical faults are identified. For a further elaboration of the escalation process, see Question 42.

Google will notify ICANN and registrars, at least 24 hours beforehand, of maintenance for all planned outages and maintenance which will directly, significantly, and visibly affect users of the SRS.

24.10. Resourcing Plans

Google will implement these technical requirements using the teams and resources discussed below.

The cost of these services will generally be set at reasonable market rates per agreement between Charleston Road Registry and Google. The expected costs are discussed in Questions 46 and 47.

All services that GSRS will depend on are already well-provisioned and ready to assume the additional load of the Google SRS, including up to 100 million second-level domains, which is well in excess of expected need. The load that GSRS will generate for existing systems will be significantly less than the capacity already designated as part of normal growth for Google and the company’s need for high-performance hardware and support personnel resources.

24.10.1. Registry Team

The Google Registry Team will be responsible for designing and implementing our SRS, EPP, and WHOIS systems, including IDNs. They will also be responsible for creating tests and monitoring for these systems.

During initial implementation, this team will consist of at least four to seven software engineers responsible for implementing the project. Additionally, Google plans to staff one software engineer who is responsible for engineering testing and monitoring for the Google Registry, and one software engineer who is responsible for backup, restoration and escrow. In

total, Google plans to implement the Google Registry with a team of six to nine software engineers.

After the Google Registry is complete, Google expects to staff a team to support the ongoing operation of the registry. This team will consist of at least four engineers who will participate in on-call rotation, respond to alerts, provide support to ICANN and registrars for emergency escalations, and maintain responsibility for bug fixes and improvements. This team will continue maintenance throughout the life of the registry.

This team's responsibilities will generally be limited to registry-specific components. The Google Registry Team will work closely with other relevant teams, including the Authoritative DNS support team, Storage Site Reliability Engineering team, network engineering and operations, and customer support teams. These other teams are described in more detail in Question 31 (Section 31.16) as well as the relevant sections throughout this application.

24.11. Summary and Key Insights

Google has an existing production infrastructure that can exceed the performance requirements of the SRS platform:
- Google has a global network of datacenters to provide the scalability to meet the performance requirements of SRS.
- Google has a multi-master high availability strategy to meet the reliability requirements of SRS.
- Google has the proven operational processes and personnel to support the requirements going forward.
- The use of Google's platform allows Charleston Road Registry to commit to service levels that substantially exceed the ICANN requirements in Specification 10.

24.12. Footnotes

[1] New York Times, "99.999% Reliable? Don't Hold Your Breath".
http://www.nytimes.com/2011/01/09/business/09digi.html

25. Extensible Provisioning Protocol (EPP)

The primary purpose of Google EPP will be to provide for a provisioning interface to the Google Registry using the standardized EPP protocol.

Google has no initial plans to provide a software development kit, since there already are a variety of open- and closed-source EPP client implementations available on the web today.

Google's EPP service will act as a connector between EPP clients and Google's backend systems, which will handle business logic for registry operations.

25.1. RFC Compliance

Google's EPP interface will handle the follow tasks:

- Listen for EPP connections over port 700.
- Support and maintain the EPP session through the life of the connection.
- Translate EPP requests and responses between equivalent requests and responses exposed by the Google SRS Backend private API.
- Terminate the Transport Security Layer (TLS) connection as defined by RFC 5734. TLS client certificates will be self-certified and transmitted to Google via the registrar application process. The credentials in the certificate will be matched against the account identified by the EPP username and password.

Google EPP will support a well defined set of EPP RFCS with a small set of additional, well-defined EPP extensions.

25.1.1. Core Protocol - RFC 5730 (http://tools.ietf.org/html/rfc5730)

RFC 5730 defines EPP, a simple object provisioning XML protocol. The base protocol itself is agnostic to the type of objects being provisioned and allows for extensions to the protocol.

Upon connection, a session is established with a 〈greeting〉 message from the server as defined by the RFC. From there, the client will login with a 〈login〉 command, then entertain a series of request and response cycles, and then finally ends the session with a 〈logout〉 command.

All EPP commands will be supported according to the RFC in their standard command and response formats.

As part of the 〈greeting〉, a 〈dcp〉 element is presented indicating Google's data-collection-policy for the Registry. In general, the 〈dcp〉 element will attempt to mirror (as far as the protocol can mirror) Google's Privacy Policy as stated in http://www.google.com/policies/privacy/. A copy of our full Privacy Policy as of March 1, 2012, is also included in Question 31 as an attachment.

For all commands, only objects defined by RFCs 5731 (domains), 5732 (hosts), and 5733 (contacts) will be supported. No other extensions will be used.

For the 〈login〉 command, the following policy specifics will be implemented:
- A maximum of three failed login attempts per connection
- On the 12th failed login attempt, the account will be locked out and require support to reactivate.
- Changing the EPP password with the optional 〈newPW〉 element will not be supported. Password changes will instead be handled through the password change interface on the Google SRS Front End. Error code 2501, "Authentication error; server closing connection" will always be returned if this command is used.
- The 〈version〉 element must be set to 1.0.
- The 〈lang〉 element must be set to "en".

For all other EPP commands there will be no implementation policy specifics.

Standard behavior as defined by the RFC for each command is expected:
- 〈check〉 : Determine if an object can be provisioned within the registry
- 〈info〉 : Retrieve information associated with a given object
- 〈poll〉 : Discover and retrieve service messages by a server for individual clients
- 〈create〉 : Create an instance of an object
- 〈delete〉 : Remove an instance of an existing object
- 〈renew〉 : Extend the validity of an existing object
- 〈transfer〉 : Determine real-time status of pending and completed transfer requests
- 〈transfer op="request"〉 : Request that an object be transferred
- 〈transfer op="approve"〉 : Approve a transfer request
- 〈transfer op="reject"〉 : Reject a transfer request
- 〈transfer op="cancel"〉 : Cancel a transfer request
- 〈update〉 : Update the information in an existing object

25.1.2. Domain Objects – RFC 5731 (http://tools.ietf.org/html/rfc5731)

RFC 5731 defines support for domain objects over the EPP protocol.

Since RFC 5732 will be supported as well, domain objects will not be able to specify attributes to describe a name server host machine, but rather must reference the relevant host with 〈domain:hostObj〉 references.

When 〈domain:authInfo〉 is used, a 〈domain:pw〉 must be passed within to denote the password for the domain (or registrant using the "roid" attribute to denote this), or a 〈domain:null〉 to null it out.

For EPP commands dealing with domain object validity, domains will be by default valid indefinitely unless otherwise specified.

A 2305 error response code will be issued if there are dependent children subordinate to the

domain, which still exist in the repository if a 〈delete〉 command is issued.

For all domains which require additional vetting of the registrant because of gTLD registration policy reasons, offline review of the domain may occur for transformation EPP commands. Otherwise, no offline review will occur in general.

25.1.3. Host Objects - RFC 5732 (http://tools.ietf.org/html/rfc5732)

RFC 5732 provides EPP mappings for host objects. This RFC will be supported in its entirety. There are no special considerations needed for the Google Registry.

There will be no offline review before provisioning of any host.

25.1.4. Contact Objects - RFC 5733 (http://tools.ietf.org/html/rfc5733)

This RFC provides EPP mapping for contact objects. This RFC will be supported in its entirety.

As specified by the RFC, unless prohibited by the server's stated data collection policy, per-field disclosure policies will be supported via the 〈contact:disclose〉 element when provisioning contacts.

There will be no offline review before provisioning of any contact.

25.1.5. EPP Transport over TCP - RFC 5734 (http://tools.ietf.org/html/rfc5734)

RFC 5734 defines connection handling procedures regarding the EPP mechanism.

The following policy is adopted from suggestions from this RFC:
-There will be no more than ten concurrent TCP connections from a single source destination IP without first contacting Google to establish an alternate upper limit.
- If a well-formed EPP request is not received at least every 30 seconds, the TCP/IP connection may be severed.
- TLS is mandatory to connect to Google EPP.
- A single TLS client certificate will be required for each EPP user and password pair. Multiple user/password pairs will not be permitted for a single TLS client certificate.
- A Certificate Name (CN) and subject AltName:dnsName will be set to the hostname of GEPP to be validated against by the client.

25.1.6. DS records - RFC 5910 (http://tools.ietf.org/html/rfc5910)

RFC 5910 governs the additions to the EPP domain mapping RFC for provisioning DS records for a particular domain. Of the two possible supported mechanisms by the RFC, Google EPP will support the "DS Data Interface", where the client is responsible for the creation of the DS information and is required to pass DS information when performing adds and removes.

Other particular implementation specifics include:
- The optional 〈secDNS:maxSigLife〉 element will not be initially supported, and a 2102 error code will be returned.
- 〈secDNS:update〉 with an attribute of urgent will not be initially supported, and a 2102 error code will be returned if present.

25.1.7. Grace periods - RFC 3915 (http://tools.ietf.org/html/rfc3915)

RFC 3915 extends the EPP RFCs to account for grace period functionality. Grace periods allow for actions to be reversed or revoked within a specified period of time. In particular, this RFC governs four grace periods: add grace period, auto renew grace period, renew grace period and transfer grace period. Google will comply with this RFC in its entirety.

25.1.8. IDN RFCs

In addition to RFCs directly related to EPP, RFCs defining internationalized domain names (IDN) (5890, 5891, 5892, and 5893) and how they are specified will be implemented for Google EPP. In particular, IDNs will be specified using punycode and in the subset of unicode character code points dictated by the IDN tables attached to this gTLD application.

25.2. EPP Extensions

A small set of well-defined EPP extensions will also be supported.

25.2.1. Launch Phase Mapping for EPP

This draft RFC is currently found here:
http://tools.ietf.org/html/draft-tan-epp-launchphase
It defines mappings to create domains and application for domains during “launch” phases. It will be supported in its entirety.

The following launch phases will be used by CRR:
- Sunrise
- Landrush
- Claims

Only encoded signed marks will be accepted in order to minimize signature validation issues.

25.2.2. Mark and Signed Mark Objects Mappings

This draft RFC is currently found here:
http://tools.ietf.org/html/draft-lozano-tmch-smd
It defines mappings for Mark and Signed Mark objects onto XML. It will be supported in its entirety, as necessitated by 25.2.1.

25.2.3. Premium Domain Names Pricing Extension

This extension is currently found here:
http://ausregistry.github.io/doc/price-1.0/price-1.0.html
It defines an EPP extension to request and return pricing information on premium domains. It also provides a mechanism for registrars to acknowledge and verify the pricing information on a premium domain before registering it. The extension will be supported in its entirety.

25.2.4 Namestore Extension

This extension is currently found here:
http://www.verisigninc.com/assets/namestore-extension.pdf
It defines a mechanism for registrars to specify which TLD their EPP command is addressed against. It will be used to multiplex many different TLDs in a single EPP endpoint. It will be supported in its entirety.

25.3. Google EPP Testing

Google will develop Google EPP using a software methodology, which ensures correct functionality by concurrently developing unit and large functional tests alongside the production code itself. Standard XML parsing libraries will be used depending on the implementation language. Implementation will also include monitoring rules that test EPP workflows in production on an ongoing basis. Before deploying to production, Google will create staging environments during development for internal manual and automated testing.

25.4. Operational Testing and Evaluation for Registrars

All ICANN-accredited registrars must first complete operational testing and evaluation (OT&E) before submitting EPP commands through the production Google EPP environment. The aim of this testing is to ensure that registrars are functioning properly.

OT&E instructions will be presented to the registrar after it has created a registrar account with the Google Registry. In general, these instructions will include a series of ordered EPP commands the registrar must perform along with test account credentials.

The registrar, once the registrar is ready for certification, it will request a Google

Registry Front End evaluation. The test environment will reset to a nominal state, and at this point, the registrar must execute the series of ordered EPP commands within a specified amount of time. If registrar fails OT&E, the registrar will be notified of the failure, and can try again at a later date. If the registrar passes OT&E, the registrar will be notified, and be given production EPP credentials.

25.5. Resourcing Plans

Google Inc. will implement these technical requirements using the teams and resources discussed below.

The cost of these services will generally be set at reasonable market rates per agreement between Charleston Road Registry and Google. The expected costs are discussed in Questions 46 and 47.

25.5.1. Registry Team

The Registry Team will be responsible for designing and implementing the shared registration system (SRS), EPP, and WHOIS systems, including IDNs. They will also be responsible for creating tests and monitoring for these systems.

During initial implementation, this team will consist of at least four to seven software engineers responsible for implementing the project. Additionally, Google plans to staff one software engineer who is responsible for engineering testing and monitoring for the registry, and one software engineer who is responsible for backup, restoration and escrow. In total, Google plans to implement the registry with a team of six to nine software engineers.

After the registry is complete, Google expects to staff a team to support the ongoing operation of the registry. This team will consist of at least four engineers who will participate in on-call rotation, respond to alerts, provide support to ICANN and registrars for emergency escalations, and maintain responsibility for bug fixes and improvements. This team will continue maintenance throughout the life of the registry.

This team’s responsibilities will generally be limited to registry-specific components. The Registry Team will work closely with other relevant teams, including the Authoritative DNS support team, Storage Site Reliability Engineering team, network engineering and operations, and customer support teams. These other teams are described in more detail in Question 31 (Section 31.16), as well as the relevant sections throughout this application.

25.6. Summary and Key Insights

Google can design, build and run EPP interface that meets the requirements of a gTLD registry because of:
- A thorough understanding of the requirements for the systems.
- A reuse of existing industry, standard EPP XML schemas to de-risk system implementation.
- A proven software development methodology that will verify implementation against requirements.
- Operational procedures that facilitate the ongoing maintenance of the platform and the support of onboarding of new registrars.

26. Whois

Google will implement and maintain a “thick” data model WHOIS service, in which the registry will store and serve contact information related to each domain name -- as opposed to a “thin” model, which provides a query referral to a registrar.

Google will operate a public WHOIS service available via port 43 in accordance with RFC 3912, and a web-based Directory Service at 〈WHOIS.nic.web〉 providing free, public query-based access. Both of these services will be made available over both IPv4 and IPv6.

Google’s WHOIS service on port 43 will comply with the WHOIS protocol as described in RFC 3912

by accepting an ASCII request (terminated with a 〈CR〉 〈LF〉) and replying with an ASCII response, terminating the TCP connection once the output is finished. RFC 3912 does not contain further detail on the format of the response payload itself; the format will be as described in “SPECIFICATION 4: SPECIFICATION FOR REGISTRATION DATA PUBLICATION SERVICES”, Section 1, and relevant Best Practices.

If ICANN specifies alternative formats and protocols, Google will implement these as soon as reasonably practical and will implement IDN related WHOIS requirements as they evolve. As a matter of policy, Google WHOIS will not return IDN variants for WHOIS queries. Queries for specific domains must be made.

26.1 High-level overview of the WHOIS service.

The attachment “Q26_WHOIS Services Diagram” shows an overview diagram of WHOIS services, and other relevant aspects of Google’s network.

Step 1: Request.
When a request is received (via the web or “traditional” interface), the appropriate service will extract the query from the request and perform checks to combat abusive behavior (such as Denial of Service and “WHOIS scraping”). Google has extensive infrastructure that profiles requests and applies heuristics to determine if requests are legitimate or “scraping”, and we plan to use this infrastructure to limit abuse of the WHOIS service. This functionality is described in Question 30, Section 30.b.3.2.

The request will also increment a counter to allow for reporting of statistics.

Step 2: Lookup.

The service will then query the registry database service, using the GSRS backend API. As the WHOIS service will query the database for the response, Google will provide fresh answers, instead of extracting all of the data from the database and synchronizing the data between servers. In order to provide fast, accurate responses, and to act as the first line of defense against DoS attacks, the WHOIS service may cache the result and reply from cache on subsequent queries for a maximum of 15 minutes.

Step 3: Reply
Once a result, or an indication that the requested information does not exist, is received from the database it will be converted into the appropriate response format: HTML for web-based requests, or RFC 3912 style responses for port 43 requests.

Step 4: Response.
The result of the lookup will then be returned to the requester.

26.2. WHOIS Infrastructure

Google operates a fast, reliable, and redundant network, and has developed frameworks for encoding and making remote procedure calls (RPCs). This infrastructure can be leveraged to provide communication and connectivity with other registry systems.

Google has significant experience developing secure, stable, resilient, and high-performance applications that perform lookups against a datastore, and has built substantial infrastructure for running such applications and scaling them to meet demand.

As described in detail in the responses to Questions 31 and 32, the WHOIS service will be designed as a simple, stateless server that accepts user queries and transforms them into RPCs that will be serviced by the SRS backend server. This model allows additional capacity to be scaled in accordance with need simply by adding additional replicas of the WHOIS server, and means that the resource requirements to operate this layer of the service should be minimal. Google continuously monitors the load on production servers and systems and proactively upgrades and supplements systems before there is any degradation in service. The registry will be initially provisioned to support at least 100 million domain names, which substantially exceeds the expected load, but Google’s overall scale would allow the scope of the service to be increased substantially if required.

We estimate that each second-level domain will generate slightly more than 3 WHOIS queries per day. Based on our projections, this will result in an expected load of 3600 qps (queries per second) from WHOIS requests. Since each machine can handle 250 qps, and we plan for a 50% utilization rate, we expect to provision about 30 machines. For more details of our expected WHOIS load and performance capacity, see Question 24.

This infrastructure will also help Google meet and exceed the specified Service Level Agreements, including those in Section 10 of the Registry Agreement, as discussed in the response to Question 24. We plan to serve WHOIS queries with at least 99.9% availability, with less than 500 ms latency, and an update time of less than 15 minutes for 95% of updates.

26.3 WHOIS Synchronization

As mentioned in previous sections, all incoming RPCs to equivalent calls to the Google SRS Backend. This means that there is no synchronization between Google WHOIS and the SRS since Google WHOIS maintains no persistent state. However, as also previously mentioned, Google may deploy a cache in the WHOIS service to reduce load on the GSRS BE and database while reducing latency, creating a freshness delay of up to 15 minutes.

26.4. WHOIS Data and Request/Response Example

Google WHOIS will follow data formats specified in Specification 4 in the application guidebook. Here is an example WHOIS domain query and response.

Query::
EXAMPLE.web

Response:
Domain Name: EXAMPLE.web
Domain ID: D424242-web
WHOIS Server: WHOIS.nic.web
Updated Date: 2012-08-13T20:13:00Z
Creation Date: 2012-02-14T00:45:00Z
Registry Expiry Date: 2014-10-08T00:44:59Z
Sponsoring Registrar: EXAMPLE REGISTRAR LLC
Sponsoring Registrar IANA ID: 314159265
Domain Status: clientDeleteProhibited
Domain Status: clientRenewProhibited
Domain Status: clientTransferProhibited
Domain Status: serverUpdateProhibited
Registrant ID: 5372808-ERL
Registrant Name: EXAMPLE REGISTRANT
Registrant Organization: EXAMPLE ORGANIZATION
Registrant Street: 123 EXAMPLE STREET
Registrant City: ANYTOWN
Registrant State/Province: AP
Registrant Postal Code: A1A1A1
Registrant Country: EX
Registrant Phone: +1.5555551212
Registrant Phone Ext: 1234
Registrant Fax: +1.5555551213
Registrant Fax Ext: 4321
Registrant Email: EMAIL@EXAMPLE.web
Admin ID: 5372809-ERL
Admin Name: EXAMPLE REGISTRANT ADMINISTRATIVE
Admin Organization: EXAMPLE REGISTRANT ORGANIZATION
Admin Street: 123 EXAMPLE STREET
Admin City: ANYTOWN
Admin State/Province: AP
Admin Postal Code: A1A1A1
Admin Country: EX
Admin Phone: +1.5555551212
Admin Phone Ext: 1234
Admin Fax: +1.5555551213

```
Admin Fax Ext:
Admin Email: EMAIL@EXAMPLE.web
Tech ID: 5372811-ERL
Tech Name: EXAMPLE REGISTRAR TECHNICAL
Tech Organization: EXAMPLE REGISTRAR LLC
Tech Street: 123 EXAMPLE STREET
Tech City: ANYTOWN
Tech State/Province: AP
Tech Postal Code: A1A1A1
Tech Country: EX
Tech Phone: +1.1235551234
Tech Phone Ext: 1234
Tech Fax: +1.5555551213
Tech Fax Ext: 93
Tech Email: EMAIL@EXAMPLE.web
Name Server: NS01.EXAMPLEREGISTRAR.web
Name Server: NS02.EXAMPLEREGISTRAR.web
DNSSEC: signedDelegation
DNSSEC: unsigned
〉〉〉 Last update of WHOIS database: 2012-08-13T20:15:00Z 〈〈〈
```

26.5 Bulk Registration Data Access to ICANN

The Google Registry will comply with Section 3 of Specification 4 in the application guidebook to provide ICANN bulk registration data access.

Data will be provided on a weekly basis. Data will include data committed as of 00:00:00 UTC on the day previous to the one designated for retrieval by ICANN.

The Google Registry will provide at a minimum all content requested in the specification: domain name, domain name repository, object id, registrar id, statuses, last updated date, creation date, expiration date, and name server names. For sponsoring registrars, the registry will provide: registrar name, registrar repository object id, hostname of registrar Whois server, and URL of registrar.

The format of the data will be provided as specified in Specification 2 for Data Escrow.

The Google Registry will have the file ready for download as of 00:00:00 UTC on the day designated for retrieval by ICANN. The file will be made available for download by SFTP with a hostname, username, and password provided to ICANN.

26.6. Resourcing

Google Inc. will implement these technical requirements using the teams and resources discussed below.

The cost of these services will generally be set at reasonable market rates per agreement between Charleston Road Registry and Google. The expected costs are discussed in Questions 46 and 47.

26.6.1. Registry Team

Our Registry Team will be responsible for designing and implementing our SRS, EPP, and WHOIS systems, including IDNs. They will also be responsible for creating tests and monitoring for these systems.

During initial implementation, this team will consist of at least 4-7 software engineers responsible for implementing the project. Additionally, we plan to staff one software engineer who is responsible for engineering testing and monitoring for the registry, and one software engineer who is responsible for backup, restoration and escrow. In total, we plan to implement the registry with a team of 6-9 software engineers.

After the registry is complete, we expect to staff a team to support the ongoing operation of the registry. This team will consist of at least four engineers who will participate in on-

call rotation, respond to alerts, provide support to ICANN and registrars for emergency escalations, and maintain responsibility for bug fixes and improvements. This team will continue maintenance throughout the life of the registry.

This team's responsibilities will generally be limited to registry-specific components. The Registry Team will work closely with other relevant teams, including the Authoritative DNS support team, Storage Site Reliability Engineering team, network engineering and operations, and customer support teams. These other teams are described in more detail in Question 31 (Section 31.16), as well as the relevant sections throughout this application.

26.7. Summary and Key Insights

- Google will operate a thick WHOIS service with an interface on port 43 complying with RFC 3912 as well as a web-based query interface. These services will display data in accordance with Specification 4 of the registry agreement.
- Google's WHOIS service offers a simple, stateless, scalable front end to the registry's SRS-BE servers. The capacity of the service can be expanded simply by adding additional replica WHOIS servers. Google will initially scale the service to support a registry with 100 million domain names.

27. Registration Life Cycle

Charleston Road Registry (CRR) sets forth below a description of the various stages and states of a second-level domain (SLD) in its proposed registry system. Please see "Q27_Registry Life Cycle Diagram" for a graphical depiction of the domain registration lifecycle.

27.1. Life Cycle States

The following registration life cycle states are described in the sections below:

- Reserved
- Available
- Add Grace Period
- Registered
- Renew Grace Period
- Auto-Renew Grace Period
- Pending Restore
- Redemption Grace Period
- Pending Delete
- Pending Transfer
- Transfer Grace Period

State changes provide specific use cases to the DNS (Domain Name System) architecture explained in responses for Question 31 (Technical Overview), Question 32 (Architecture) and Question 35 (DNS Service). Note that this response makes references to EPP (Extensible Provisioning Protocol) functionality which is fully described in Question 25. Additionally, state changes may change the information retrievable via Registration Data Directory Services (RDDS, a combination of WHOIS and Web-based WHOIS) as described in Question 26.

27.2. Reserved

Reserved domains are not generally available to register. For example, such restrictions may result from agreements with ICANN/IANA for operational/technical reasons or with governments for geographic names. See response to Question 22 (Protection of Geographic Names) for further details. The registry will maintain a schedule of reserved words as per Specification 5 of the Registry Agreement. For a reserved domain, an EPP 〈check〉 query would return a value of avail="0", and there would be no entry in the zone file or RDDS associated with the domain name. EPP 〈create〉 requests will result in a rejection, except those that have prior approval from CRR. The registry foresees two cases as envisioned by Specification 5 of the New gTLD Agreement, particularly applicable to geographic names: 1) CRR releases an SLD for use by the applicable government or country-code manager. In this case, at the end of the

registration, the SLD would return to the Reserved state. 2) CRR works with the affected government(s) or country-code manager(s) to permanently make available SLD(s). In this case, at the end of a reservation the string would revert to the Available state.

In addition to an explicit Reserved state, CRR will also support a functional equivalent to reserving through registration. This approach follows the practices of the .info registry. That is, CRR will reserve certain names by registering them for the registry, pursuant to Section 2.6 of the gTLD registry agreement. Names reserved using this approach follow the life cycle described below. Generally, CRR will use the state machine to control reservations but leaves open the possibility of using reservation by registration when more appropriate.

27.3. Available

If a second level domain (SLD) is not reserved, it is considered available if either of the following holds true:
- The SLD has not existed previously.
- The SLD has passed through the Pending Delete state.

Domains that are available do not exist in the zone file or RDDS. The Shared Registry System – Back End (SRS-BE) would return a value of avail="1" when responding to the EPP 〈check〉 query for domain in the Available state.

All other states would return a value of avail="0".

27.4. Add Grace Period (AGP)

Names that are selected for registration are entered into the zone file at the start of this five-day add-grace period (〈addPeriod〉). Registrars are charged for submitting 〈create〉 requests to the registry.

The Google SRS-Backend (GSRS-BE) manages the 5-day grace period countdown, including the transition of the state to Registered. During the Add Grace Period, registrars can cancel the registration and receive a credit for the cost of the original registration (with domain names becoming immediately Available or Reserved, as appropriate), subject to ICANN's AGP Limits Policy. GSRS-BE will set the status of the Domain Name to 〈addPeriod〉 while making the zone file and RDDS updates, and then reset it when grace period ends.

27.5. Registered

Owners of domain names can register them for a period of one to ten years. The registrar may renew the SLD for no less than one and no more than ten years from the current day using the EPP 〈renew〉 command. GSRS-BE will manage state changes based on expiration date of domains, including updates to the zone file and RDDS. By default, status of the object is "ok". Subsequent EPP 〈transform〉 commands or actions by SRS-BE may change that value to indicate restrictions present or transformations pending.

27.6 Renew Grace Period (RGP)

Upon receipt of a 〈renew〉 EPP command, SRS-BE will transition the domain name to the state of Renew Grace Period (〈renewPeriod〉). The renew grace period allows registrars to correct the mistaken renewal of an SLD. The Renew Grace Period lasts for five (5) days during which the receipt of a 〈delete〉 EPP command will result in the crediting back to the registrar the cost of the renewal. After this grace period ends, the domain name will revert to the Registered state. Domains in the RGP may transition to the following states: Redemption Grace Period (by meaning of a delete) or Pending Transfer (by means of a transfer) as described in sections 27.8 and 27.11, respectively.

27.7. Auto-Renew Grace Period (ARGP)

GSRS-BE will automatically renew a registration once it has expired and charge the registrar the current renewal fee. By default, CRR will extend the registration for one year. The ARGP is intended to allow registrars to delete a registration which has been auto-renewed and to receive a refund for the renewal fee. For a predetermined number of days after an automatic renewal, the domain is in state of the Auto-Renew Grace Period (〈autoRenewPeriod〉). During

this grace period, GSRS-BE will accept requests from the EPP for the existing owner to update, renew, transfer and delete the registration provided there is not a corresponding status that prohibits the transformation. The registrar will then be charged the cost of this new transaction. If the registry happens to receive a 〈delete〉 EPP command during the ARGP, CRR will credit the cost of a renewal to the registrar. Without intervention, SRS-BE will then update the domain's state to Registered.

27.8. Redemption Grace Period (RdGP)

SLDs that are deleted, such as when a registrar uses the 〈delete〉 EPP command, then enter the Redemption Grace Period (RdGP) (〈redemptionPeriod〉), with the exception of those deleted during the Add Grace Period (see above). The RdGP permits registrars to restore domains that were mistakenly deleted. The RdGP lasts for thirty (30) days. SRS-BE will first check for a clientDeleteProhibited or a serverDeleteProhibited prohibition before making the transition, and will not make the transition if those prohibitions exist.

Domains which enter this state become non-operational and are removed from the zone file and RDDS. The SRS-BE will accomplish this change by updating the DNS service. GSRS-BE will also set the status to "pendingDelete".

During the RdGP, the SRS-BE will reject all EPP requests other than 〈restore〉 . Registrars have 30 days to submit a 〈restore〉 request in order for the transaction to be accepted and the transaction cost credited back to the registrar. Registrars must provide a 〈report〉 that provides, among other things, a reason (〈resReason〉) and supporting information (〈statement〉) within 5 days (during which time the status will be Pending Restore or 〈pendingRestore〉). CRR will not process a 〈restore〉 without a 〈report〉 . If a 〈restore〉 request is not received or if a 〈report〉 is not received on time, GSRS-BE transitions the domain name to the Pending Delete state. Should a registrar reactivate the domain, SRS-BE will update the DNS zone file and RDDS. When complete, SRS-BE will update the state to Registered.

27.9. Pending Delete

This state is the final stage of the lifecycle prior to the domain again being made available. It lasts for 5 days. During this period, registrars shall not have the ability to reactivate the domain, but would have to wait to make a new request once the domain becomes available. During the Pending Delete phase, the SRS-BE will reject all requests to transform a domain name received through the EPP interface. The status of the domain name will be 〈pendingDelete〉 . After this stage, the domain shall be removed from the registry's database and once again made available for registration.

27.10. Released/Available

As noted above, at the conclusion of the Pending Delete state, GSRS-BE removes the domain name entirely from its database. It is now available for registrars. See 27.3 above for further details of "Available" state. The exception would be those domain names on the reserved list, which will instead return to the Reserved state after they are released.

27.11. Transfers

CRR and Google will adhere to the 15 March 2009 ICANN Policy on Transfer of Registrations (as well as its successor scheduled to take effect on 1 June 2012). Therefore, registrars are allowed to transfer domains between each other, provided that the states and status allow for it.

Transfer requires the following conditions:
- The domain must be in one of the following states: Add Grace Period, Registered, Renew Grace Period, Transfer Grace Period, or Auto Renew Grace Period.
- Neither a clientTransferProhibited nor a serverTransferProhibited status must be present.

Provided those two conditions are met, GSRS-BE will set the status to 〈pendingTransfer〉 while it performs its activities (during this period, the domain is considered to be in the Pending Transfer state). First, the registry will notify both registrars of the pending transfer. The registry will complete the transfer if it receives an 〈ACK〉 response from the Registrar of Record if received within the first five (5) days. If after five (5) days and the registry

has not received any message, the transfer will be automatically completed. If a 〈NACK〉 response is received from the Registrar of Record, the transfer will be rejected. A rejected transfer would result in the SRS-BE setting the state back to its previous value.

Upon completion of the transfer, CRR will update the zone file and RDDS and send another notification to both registrars. When a transfer is complete, the registration period for the SLD is extended by a year (but not to exceed ten (10) years from the date of the transfer) and the gaining registrar will be charged for submitting a 〈transfer〉 EPP request.

27.11.1. Transfer Grace Period (TGP)

The registry places the domain name into the Transfer Grace Period (〈transferPeriod〉) for the first 5 days after the completion of the 〈transfer〉 request. During this time, the Gaining registrar will receive a credit for the cost of the transfer if a 〈delete〉 EPP transaction is received. Provided the domain is not deleted, at the end of the 5 day period the domain will return to the Registered state. A transfer received during TGP would result in the domain moving to 〈pendingTransfer〉 as described above.

27.12. Resourcing

Google Inc. will implement these technical requirements using the teams and resources discussed below.

The cost of these services will generally be set at reasonable market rates per agreement between Charleston Road Registry and Google. The expected costs are discussed in Questions 46 and 47.

27.12.1. Registry Team

The Registry Team will be responsible for designing and implementing the SRS, EPP, and WHOIS systems, including details related to domain name lifecycle. They will also be responsible for creating tests and monitoring for these systems.

During initial implementation, this team will consist of at least 4-7 software engineers responsible for implementing the project. Additionally, Google plans to staff one software engineer who is responsible for engineering testing and monitoring for the registry, and one software engineer who is responsible for backup, restoration and escrow. In total, Google plans to implement the registry with a team of 6-9 software engineers.

After the registry is complete, Google expects to staff a team to support the ongoing operation of the registry. This team will consist of at least four engineers who will participate in on-call rotation, respond to alerts, provide support to ICANN and registrars for emergency escalations, and maintain responsibility for bug fixes and improvements. This team will continue maintenance throughout the life of the registry.

This team’s responsibilities will generally be limited to registry-specific components. The Registry Team will work closely with other relevant teams, including the Authoritative DNS support team, Storage Site Reliability Engineering team, network engineering and operations, and customer support teams. These other teams are described in more detail in Question 31 (Section 31.16), as well as the relevant sections throughout this application.

27.12.2. Customer Services Team

The Google Customer Services Team will be responsible for supporting customers and partners, including life cycle requests. Google has a very large existing customer service team of both internal staff as well as staff contracted through third parties, with many hundreds of dedicated staff members already in place. Since these teams and their management are already in place, no standalone implementation resources are needed.

To continue ongoing maintenance of CRR support needs, Google plans to add additional resources for capacity as needed. Google expects to add a total of approximately fifteen additional personnel (including both Google employees and outside vendors) to support all of CRR’s customers and partners. The individual staffing allocation to each TLD is described in Question 47.

27.13. Summary and Key Insights

- The registry will support a full registration lifecycle consistent with that offered by other major gTLDs. State changes are triggered by registrar commands via the EPP interface or by the SRS-BE, which manages changes triggered by the passage of time.

28. Abuse Prevention and Mitigation

Specifically, we will implement in our internal policies and in our Registry/Registrar and Registration Agreements that all registered domain names will be subject to a Domain Name Anti-Abuse Policy ("Abuse Policy"). The Abuse Policy will provide CRR with broad power to suspend, cancel, or transfer domain names that violate the Abuse Policy. We plan to post the Abuse Policy on a publicly facing website at nic.web/abuse, which will provide a reporting mechanism whereby violations of the policy can be reported by those who are impacted; an easy to find place to report policy violations; "plain language" definitions of what constitutes a "reportable" problem; and compliance processes to provide due process, and sanctions that will be applied, in the case of policy violations. The nic.web/abuse website will list CRR's Abuse Point of Contact. The Abuse Point of Contact shall consist of, at a minimum, a valid e-mail address dedicated solely to the handling of abuse complaints. CRR will ensure that this information is kept accurate and up to date and will be provided to ICANN if and when changes are made.The Abuse Point of Contact will review complaints regarding an alleged violation of the Abuse Policy.

28.1. Abuse Tracking

CRR also plans to catalog all abuse communications in Google's customer relationship management (CRM) software using a ticketing system and to maintain records of all abuse complaints for an appropriate amount of time. We shall only provide access to these records to third parties under limited circumstances, such as in response to a subpoena or other such court order or demonstrated official need by law enforcement.

The Abuse Policy will define abuse as an action that:
a. Causes actual and substantial harm, or is a material predicate of such harm; and
b. Is illegal or illegitimate, or is otherwise considered contrary to the intention and design of a stated legitimate purpose, if such purpose is disclosed.

28.2. Abuse Definitions

The Abuse Policy will also name and provide basic definitions as to what constitutes the abusive registration and/or use of domain names within the TLD. These will include, but not be limited to, the following activities:
1. Unqualified Applicant - not authorized to register domain name;
2. Child Pornography - Web sites that contain content that exploits children, such as child pornography (including cartoon child porn) or content that presents children in a sexual manner;
3. Fake renewal notices - Fake renewal notices are misleading correspondence sent to registrants from an individual or organization claiming to be or to represent the current registrar. These are sent for a variety of deceptive purposes, such as obtaining an unnecessary fee (fraud); getting a registrant to switch registrars unnecessarily ("slamming", or illegitimate market-based switching); or to obtain registrant credentials or authorization codes to facilitate theft of the domain;
4. Cross-TLD Registration Scam - a deceptive sales practice where an existing registrant is sent a notice that another party is interested in or is attempting to register the registrant's domain string in another TLD;
5. Domain kiting/tasting – Registrants may abuse an Add Grace Period through continual registration and deletion of domain names to test their monetization ("tasting"), and re-registration of the same names in order to avoid paying the registration fees ("kiting");
6. Phishing - a Web site fraudulently presenting itself as a trusted site (often a bank) in order to deceive Internet users into divulging sensitive information (e.g. online banking credentials, email passwords);

7. Spam - use of electronic messaging systems from email addresses from domains in the TLD to send unsolicited bulk e-mail;
8. Malware ⁄ Botnet Command-and-Control – Malware authors sometimes use domain names as a way to control and update botnets. Botnets are composed of thousands to millions of infected computers under the common control of a criminal. Botnets can be used to perpetrate many kinds of malicious activity, including distributed denial-of-service attacks (DDoS), spam, and fast-flux hosting of phishing sites;
9. Use of Stolen Credentials –such as stolen credit card numbers, to register domain names for malicious purposes;
10. Pharming - redirecting of unknowing users to fraudulent Web sites or services, typically through domain name system (DNS) hijacking or poisoning;
11. Fast flux hosting - use of fast-flux techniques to disguise the location of Web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fast-flux techniques use DNS to frequently change the location on the Internet to which the domain name of an Internet host or name server resolves. Fast flux hosting may be used only with prior permission of CRR;

28.3. Abuse Policy Rights Reserved

The Abuse Policy will state, at a minimum, that CRR reserves the right to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status, that it deems necessary, in its discretion: (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of CRR, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement or any agreement CRR has with any party; (5) to correct mistakes made by CRR, its registry services provider, or any registrar in connection with a domain name registration; (6) during resolution of any dispute regarding the domain; and (7) to remedy the abusive registration or use of any domain name.

28.4. Orphan Glue

We will remove orphan glue records for names removed from the zone when provided with evidence in written form to the Abuse Point of Contact that the glue is present in connection with malicious conduct according to Specification 6 of the New gTLD Registry Agreement. Google’s back-end systems will also periodically search for orphaned glue. We will inform its registrants that it removes glue if the covering zone is removed, and thus registrants should not reference it from outside the domain.

28.5. Resourcing

CRR and its affiliates will commit ample resources for the purpose of implementing its internal policies and its Registry⁄Registrar and Registration Agreements. As described herein, we will create an Internal Abuse Team, including an Abuse Point of Contact, whose responsibilities will include reviewing, responding, cataloging, and, if applicable, remedying complaints regarding alleged violations of the Abuse Policy. This team will be dedicated to manually reviewing abuse complaints. The roles and responsibilities of the team members are anticipated to include, but are not limited to, the following:
- Reviewing, responding, and if applicable, resolving complaints regarding alleged violations of the Abuse Policy
- Enforcing the Abuse Policy
- Monitoring productivity and efficiency of the manual review process
- Addressing high priority escalations from Law Enforcement quickly
- Collaborating with internal and external partners to drive issues to resolution
- Interface with the technical team to improve workflow, prioritize escalations, create tools for the manual review process

28.6. Anti-abuse Notice and Takedown Procedure

In order to reduce abusive registrations that affect the security of the TLD and its users, CRR plans to provide a domain anti-abuse notice and takedown procedure. Specifically, we will operate an anti-abuse website at the URI address nic.web⁄abuse that will provide the contact information for the Abuse Point of Contact. The nic.web⁄abuse website will prominently display

CRR's Abuse Policy and a fill-in section wherein the user will then be asked to fill in several fields, including the user's identity and contact information, and the identity and relevant information of the individual or organization that is making an abusive registration or use of a domain name within the TLD, and specific details on how, why, and when the complainant believes the registration or use of the domain name is abusive. The user will be asked to read the Abuse Policy before it submits a complaint and then click on a check box to indicate that the user has read and understands the Abuse Policy.

28.7. Abuse Response

CRR will then provide a targeted response time as to the decision regarding the complaint. We will review with the Internal Abuse Team and render a decision regarding the alleged abuse, and decide whether to deny, cancel, or transfer any registration or transaction, or place any domain(s) on registry lock, hold, or similar status that violates the Abuse Policy, if applicable. In accordance with the applicable terms of service, CRR reserves the right to terminate the accounts or domains of repeat abusers.

Specifically, the process is anticipated to occur as follows: an email containing the information relayed in the complaint will be sent to the Abuse Point of Contact. The Abuse Point of Contact will send an email to the complainant within twenty-four hours of receiving the complaint confirming receipt of the email. The Abuse Point of Contact will preliminarily review to determine whether the complaint reasonably falls within an abusive use as defined by the Abuse Policy. If the complaint does not, the Abuse Point of Contact will email the complainant within forty-eight business hours of the confirmation email to indicate that the subject of the complaint does not fall within the abusive uses as defined by the Abuse Policy, and that CRR considers the matter closed.

If the preliminary review does not resolve the matter, the Abuse Point of Contact will relay the complaint to CRR's Abuse Team.

All requests from law enforcement will be flagged for prompt review by the Internal Abuse Team. With the resources of Google's registry services team, CRR can meet its obligations under Section 2.8 of the Registry Agreement where required to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of its TLD.

In high-priority cases the Internal Abuse Team will seek to determine within forty-eight business hours whether the registration or use of the domain within the TLD is abusive as defined by the Abuse Policy. In all cases, the Internal Abuse Team will determine whether a domain is abusive within seven business days or sooner of receipt of the Complaint. If an abusive use is determined, the Internal Abuse Team may alert the registry services team to immediately suspend resolution of the domain name, as appropriate. Thereafter, if we decide to suspend resolution of the domain name at issue, the Abuse Point of Contact will immediately notify the abusive domain name registrant of such action, the nature of the complaint, and provide the registrant with the option to respond within ten days. All such actions will be ticketed in Google's CRM software to maintain accurate complaint processing records.

If the registrant responds within ten business days, the Internal Abuse Team will review the response to determine if the registration or use is not abusive. If the Internal Abuse Team is satisfied by the registrant's response, the Abuse Point of Contact will submit a request to the registry services team to reactivate the domain name. If the registrant does not respond within ten business days or the Internal Abuse Team is not satisfied by the registrant's response, the Abuse Point of Contact will notify the registry services team to continue the suspension, transfer or cancel the abusive domain name, as appropriate.

The anti-abuse procedure will not prejudice either party's election to pursue another dispute mechanism, such as the Uniform Rapid Suspension System (URS) or Uniform Domain-Name Dispute-Resolution Policy (UDRP). If CRR's registrar receives notice of a URS or UDRP complaint pertaining to a domain name within the TLD, the registrar will ensure that the domain name is locked within twenty-four hours of receipt of the complaint. The registrar will also notify CRR's Abuse Point of Contact and the registrant.

28.8. Abuse Prevention

In order to further minimize abusive domain name registrations and other activities that have a negative impact on Internet users, CRR will promote the ability to contact a domain registrant using information in WHOIS by providing accessibility in a reliable, consistent, and predictable fashion. CRR will adhere to port 43 WHOIS Service Level Agreements (SLA), which require that port 43 WHOIS service be highly accessible and fast.

CRR will either verify the email address or telephone number provided by the registrant or will require that the registrar do so as a part of registration.

CRR plans to establish policies and procedures to address domain names with inaccurate or incomplete WHOIS data.

As required by Specification 4 of the new gTLD Registry Agreement, CRR will offer thick WHOIS services, in which all authoritative WHOIS data is maintained at the registry. Through CRR's registrar and registry services team, we will maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing, and administrative contact information, identity of the registrar, domain name's expiration date, nameservers associated with the domain, and specified fields of data for the Registrant Contact, Administrative Contact, and Technical Contact.

CRR will employ query rate limiting and CAPTCHA procedures for its WHOIS database to minimize abuse of its features.

28.9. Summary and Key Insights

Abusive activity on the Internet has been a growing problem, creating security and stability issues for registrants, registrars and users of the Internet in general. CRR intends to address this issue across its TLDs by dedicating ample resources for the purpose of implementing its strict abuse policies and procedures.

29. Rights Protection Mechanisms

Abusive registrations and uses of domain names in the global top-level domain (gTLD) will not be tolerated. The nature of such abuses creates security and stability issues for the registry, registrars and registrants, as well as for users of the Internet in general. As set forth in prior responses, Charleston Road Registry (CRR) will employ a stringent verification process to establish that every prospective registrant meets the registration criteria. In addition to this verification process, the registry promises to incorporate the following Rights Protection Mechanisms.

29.1. Rights Protection Mechanisms – Sunrise Period

Subject to the Sunrise Eligibility Requirements (SERs) outlined herein, Charleston Road Registry (CRR) will offer a Sunrise Period of 60 days for owners of trademarks listed in the Trademark Clearinghouse to register domain names that contain a second level consisting of an identical match to their listed trademarks. In addition, CRR plans to implement a pricing structure to make it easy for brand owners to secure their trademarks and brand names within the gTLD. CRR's registrar will confirm all Sunrise and Registration eligibility. As an added measure of security for brand owners, CRR will staff an internal sunrise team (the "Sunrise Contact") which will review all Sunrise registrations to ensure Sunrise and registration eligibility.

The SERs, which will be verified by Clearinghouse data, will include the following: (i) proof of membership in eligible registrant class, (ii) ownership of a mark that is (a) nationally or regionally registered and for which proof of use, such as a declaration and a single specimen of current use – was submitted to, and validated by, the Trademark Clearinghouse; or (b) that have been court-validated; or (c) that are specifically protected by a statute or treaty currently in effect and that was in effect on or before 26 June 2008; (iii) representation that all provided information is true and correct; and (iv) provision of data sufficient to document rights in the trademark.

Upon submission of all of the required information and documentation, the registrar will review the submissions and verify the trademark and eligibility information and all contact information provided for registration. The registrar shall then send confirmation messages, listing any deficiencies regarding the trademark information provided with the application. If a registrant does not cure any eligibility deficiencies and/or respond by the means listed within one week, the registrar will release the name.

CRR will incorporate a Sunrise Dispute Resolution Policy (SDRP). The SDRP will allow challenges to Sunrise Registrations by third parties for a ten-day period after acceptance of the registration based on the following four grounds: (i) at the time the challenged domain name was registered, the registrant did not hold a trademark registration of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty; (ii) the domain name is not identical to the mark on which the registrant based its Sunrise registration; (iii) the trademark registration on which the registrant based its Sunrise registration is not of national or regional effect or the trademark had not been court-validated or protected by statute or treaty; or (iv) the trademark registration on which the domain name registrant based its Sunrise registration did not issue on or before the effective date of the Registry Agreement and was not applied for on or before ICANN announced the applications received.

After receiving a Sunrise Complaint, the Sunrise Contact will review the Complaint to see if the Complaint reasonably asserts a legitimate challenge as defined by the SDRP. If the Complaint does not, the Sunrise Contact will email the complainant within 36 hours of the complaint to indicate that the subject of the complaint does not fall within SDRP, and that CRR considers the matter closed.

If the domain name is not found to have adequately met the SERs, the Sunrise Contact may alert the registrar to immediately suspend resolution of the domain name, as appropriate. Thereafter, the Sunrise Contact will immediately notify the registrant of such action, the nature of the complaint, and provide the registrant with the option to respond within ten days to cure the SER deficiencies or the domain will be canceled. All such actions will be ticketed in Google’s customer relationship management (CRM) software to maintain accurate SDRP processing records.

If the registrant responds within ten business days, its response will be reviewed by the Sunrise Contact to determine if the SERs are met. If the Sunrise Contact is satisfied by the registrant’s response, it will submit a request by the registry services team to reactivate the domain name. The Sunrise Contact will then notify the Complainant that its complaint was ultimately denied and provide the reasons for the denial. If not, both the registrant and the complainant will be notified that the domain name will be released.

29.2. Rights Protection Mechanisms – Trademark Claims Service

CRR will offer a Trademark Claims Service during the Sunrise Period and plans to continue to offer the service for an indefinite period of time thereafter during general registration. CRR will staff an internal team that will be considered the Trademark Claims Contact. The registrar will verify whether any domain name requested to be registered in the gTLD is an identical match of a trademark that has been filed with the Trademark Clearinghouse. It is anticipated that a domain name will be considered an identical match when the domain name consists of the complete and identical textual elements of the mark, and includes domain names where (a) spaces contained within a mark that are either replaced by hyphens (and vice versa) or omitted; (b) certain special characters contained within a trademark are spelled out with appropriate words describing it (e.g., @ and &); and (c) punctuation or special characters contained within a mark that are unable to be used in a second-level domain name are either (i) omitted or (ii) replaced by hyphens or underscores.

If the registrar determines that a prospective domain name registration is identical to a mark registered in the Trademark Clearinghouse, the registrar will provide a “Trademark Claims Notice” (“Notice”) in English on the registrar’s website to the prospective registrant of the domain name. The Notice will provide the prospective registrant with access to the Trademark Clearinghouse Database information referenced in the Trademark Claims Notice to enhance its understanding of the Trademark rights being claimed by the trademark holder via a link. The Notice will be provided in real time without cost to the prospective registrant.

After receiving the Notice, the registrar will require the prospective registrant to click a link that specifically warrants that: (i) the prospective registrant has received notification that the mark(s) is included in the Clearinghouse; (ii) the prospective registrant has received and understood the Notice; and (iii) the registration and use of the requested domain name will not infringe on the rights that are the subject of the Notice.

CRR reserves the right to adopt other procedures and requirements for the Trademark Claims Service. At a minimum, it is anticipated that after the effectuation of a registration that is identical to a mark listed in the Trademark Clearinghouse, the registrar will then provide a clear notice to the trademark owner of the trademark with an email detailing the WHOIS information of the registered domain name. The trademark owner then has the option of filing a Complaint under the Uniform Domain Name Dispute Resolution Policy (UDRP) and/or the Uniform Rapid Suspension System (URS) against the domain name. As discussed in its right protection mechanisms, CRR will require in its domain name registration agreements that its registry operator and registrar providers, as well as all registrants, submit to the Uniform Domain Name Dispute Resolution Policy (UDRP) and the Uniform Rapid Suspension System (URS) procedures. CRR and its registrar(s) will abide by decisions rendered under the UDRP and URS on a timely and ongoing basis upon notification.

29.3. Rights Protection Mechanisms – URS

CRR will specify in the Registry Agreement, all Registry-Registrar Agreements, and all Registration Agreements used in connection with the gTLD that it will abide by all decisions made by panels in accordance with the Uniform Rapid Suspension System (URS). CRR's registrar will be tasked with receiving all URS Complaints and decisions. After receiving a URS complaint about a domain name within the gTLD, the registrar will ensure that the domain name is locked within twenty-four (24) hours of receipt of a URS complaint from the URS Provider and will notify CRR's Abuse Point of Contact and the registrant. In the event of a determination in favor of the complainant, the registrant will notify the Abuse Point of Contact and the registry services provider to ensure that the registry suspends the domain name in a timely fashion and has the website at that domain name is redirected to an informational web page provided by the URS Provider about the URS throughout the life of its registration. CRR's Abuse Point of Contact will oversee and monitor the status and resolution of all URS complaints and decisions.

29.4. Rights Protection Mechanisms – UDRP

CRR will specify in the Registry Agreement, all Registry-Registrar Agreements, and all Registration Agreements used in connection with the gTLD, that it will abide by all decisions made by panels in accordance with the Uniform Domain-Name Dispute-Resolution Policy (UDRP). CRR's registrar will be tasked with receiving all UDRP complaints and decisions. After receiving a UDRP complaint about a domain name within the gTLD, the registrar will ensure that the domain name is locked within twenty-four (24) hours of receipt of a UDRP complaint from the UDRP Provider and will notify CRR's Abuse Point of Contact and the registrant. In the event of a determination in favor of the complainant, the registrant will notify the Abuse Point of Contact and the registry services provider to ensure that the registry cancels or transfers the domain name in a timely fashion as provided for by the decision. CRR's Abuse Point of Contact will oversee and monitor the status and resolution of all UDRP complaints and decisions.

29.5. Rights Protection Mechanisms – Proven Registrars

CRR will contract with various ICANN-accredited registrars. CRR is committed to reducing abusive registrations, and will ensure that its registrar operates accordingly.

29.6. Rights Protection Mechanisms – Pre-Authorization and Authentication

CRR will either verify the email address or telephone number provided by the registrant or will require that the registrar do so as a part of registration. CRR will ensure proper access to domain functions by requiring multi-factor authentication from registrants to process update, transfer, and deletion requests.

No name will resolve until the registrant has been verified by the internal team as an eligible registrant.

29.7. Rights Protection Mechanisms – Grace Period

See Question 27 for a detailed discussion of CRR's policies with respect to Add Grace Periods.

29.8. Rights Protection Mechanisms – Domain Anti-Abuse Policy

CRR will implement in its internal policies and its Registry-Registrar and Registration agreements that all registered domain names will be subject to a Domain Name Anti-Abuse Policy ("Policy"). See Question 28 for a detailed discussion of CRR's Anti-Abuse Policy.

29.9. Resourcing

Google will implement these technical requirements using the teams and resources discussed below.

The cost of these services will generally be set at reasonable market rates per agreement between CRR and Google. The expected costs are discussed in Questions 46 and 47.

29.9.1. Registry Team

The Registry Team will be responsible for designing and implementing the SRS, EPP, and WHOIS systems, including implementation of the rights protection mechanisms. They will also be responsible for creating tests and monitoring for these systems.

During initial implementation, this team will consist of at least 4-7 software engineers responsible for implementing the project. Additionally, Google plans to staff one software engineer who is responsible for engineering testing and monitoring for the registry, and one software engineer who is responsible for backup, restoration and escrow. In total, Google plans to implement the registry with a team of 6-9 software engineers.

After the registry is complete, Google expects to staff a team to support the ongoing operation of the registry. This team will consist of at least four engineers who will participate in on-call rotation, respond to alerts, provide support to ICANN and registrars for emergency escalations, and maintain responsibility for bug fixes and improvements. This team will continue maintenance throughout the life of the registry.

This team's responsibilities will generally be limited to registry-specific components. The Registry Team will work closely with other relevant teams, including the Authoritative DNS support team, Storage Site Reliability Engineering team, network engineering and operations, and customer support teams. These other teams are described in more detail in Question 31 (Section 31.16), as well as the relevant sections throughout this application.

29.9.1. Customer Service Team

The Customer Services Team will be responsible for supporting customers and partners, including responding to abusive registrations. Google has a very large existing customer service team of both internal staff as well as staff contracted through third parties, with many hundreds of dedicated staff members already in place. Since these teams and their management are already in place, no standalone implementation resources are needed.

To continue ongoing maintenance of CRR support needs, Google plans to add additional resources for capacity as needed. Google expects to add a total of approximately fifteen additional personnel (including both Google employees and outside vendors) to support all of CRR's customers and partners. The individual staffing allocation to each gTLD is described in Question 47.

29.10. Summary and Key Insights

CRR is committed to implementing strong and integrated intellectual property rights protection mechanisms. Doing so is critical to Google's goals of model Internet citizenship and fostering Internet development, especially in emerging regions. Accordingly, CRR intends to offer a suite of rights protection measures which builds upon ICANN's required policies while fulfilling our commitment to encouraging innovation, competition, and choice on the Internet.

30(a). Security Policy: Summary of the security policy for the proposed registry

30.a. Security Policy

Google plans to use the same common secure infrastructure to support the proposed registry that we use for our other production networks and computing environments. Google currently provides best-in-class security technologies and processes to protect Google's products, services, infrastructure and user data. Google's common secure infrastructure supports some of the web's most widely-used services, such as Google Search YouTube, and Google Apps. These services are used by many millions of consumers, businesses and government customers for their daily operations. Google does not have any plan to support High Security Top Level Domain (HSTLD).

30.a.1. Google Security Policies

Google's security programs are governed through the Google Security Team. The Security Team is led by Google's Vice President of Security, who reports to Google Senior Leadership including the President of Technology and Chief Executive Officer. Google's VP of Security has approved the security policies that underpin Google's information security program.

Our Security Team is committed to:
- Control and maintain the confidentiality, integrity, and availability of information and information systems.
- Limit Google's exposure to the risks arising from loss, corruption or misuse of our information assets.
- Ensuring consistency, which is attained against legal, regulatory, policy and best practice requirements.

Google regularly reviews and updates the security policies that address purpose, scope, responsibilities, management commitment, coordination among organizational entities, and compliance.

To ensure the consistent implementation of security controls across the various layers of infrastructure and services, Google has documented the following security policies.

- Basic Security Policy: States the foundation and principles of Google's Security Policies.
- Physical Security Policy: States how the safety of people and property is protected at Google.
- Accounts Access and Administration Policy: States the kinds of internal accounts Google has and how to access, use, and administer them in a way that reduces risk and provides the ability to audit account activity.
- Data Security Policy: States how data should be handled at Google to help ensure its confidentiality, integrity, and availability.
- Corporate Services Security Policy: Informs Google employees of what to expect regarding access, monitoring, and other security considerations for communications and other data sent, received, or stored using Google's corporate services.
- Network and Computer Security Policy: States how to reduce the likelihood of compromise to Google's data and infrastructure from devices connected to Google networks.
- Applications, Systems, and Services Security Policy: Ensures that adequate attention is paid to security in the design, procurement, development, deployment, and maintenance of Applications, Systems, and Services.
- Change Management Policy: Describes the safeguards that protect Google from accidental or malicious changes to Google's systems.
- Information Security Incident Response Policy: States the minimal requirements for preparing for and responding to information security incidents.
- Datacenter Security Policy: Ensures that adequate attention is given to verifying that each datacenter hosting Google systems maintains security controls that provide protection appropriate to the criticality of those systems.

30.a.2. Independent Assessment Reports

Google regularly engages independent assessors to independently assess its information systems, infrastructure and security program and controls for compliance with the following:

- Federal Information Security Management Act (FISMA). Independent assessments conducted every two years. In 2011, Google received FISMA certification for Google Apps Cloud, another service that uses the same production network as the Google registry will use. Grant Thornton LLP performed independent assessment, and United States General Services and Administration (GSA) issued FISMA certification to Google based on this independent assessment.
- Statement on Standards for Attestation Engagements (SSAE16). Independent assessments conducted annually.
- Sarbanes-Oxley (SOX). Independent assessments conducted annually.
- Payment Card Industry (PCI). Independent assessments conducted annually.

Government agencies and Enterprise customers are currently using Google Apps Cloud Services. Google’s corporate and production networks were both in scope for FISMA and SSAE16 independent assessments. Google is also currently preparing for ISO 27001 certification of Google Apps Cloud.

30.a.3. Commitments made to Registrants

Google will make the following commitments to registrants.

- Google’s existing dedicated Security Organization will remain the focal point for ensuring implementation of adequate system security in order to prevent, detect, and recover from security breaches. Various teams in the security organization ensure that Google’s infrastructure and services are operated, used, maintained, and disposed of in accordance with internal security policies.
- Google will continue to contemplate threats from internal and external sources, and will exercise our existing incident response capability.
- Google will continue to perform quarterly scanning of our internal and external infrastructure to detect network, database, application, and OS vulnerabilities.
- Google will continue to maintain robust Logging, Monitoring and Auditing capabilities for its systems and networks. These policies are discussed further in Section 30b.
- Google’s externally facing network infrastructure will continue to enforce strict access control restrictions to deny all traffic and allow only authorized protocols to enter the Google network.
- Google has established background investigations for all Google employees in accordance with local laws and will continue to do background investigations for any new Google employees.

© Internet Corporation For Assigned Names and Numbers.

EXHIBIT JMR-14

JMR-14

New gTLD Application Submitted to ICANN by: Schlund Technologies GmbH

String: WEB

Originally Posted: 13 June 2012

Application ID: 1-1013-77165

Applicant Information

1. Full legal name

Schlund Technologies GmbH

2. Address of the principal place of business

Contact Informat on Redacted

3. Phone number

Con ac nforma ion Redac ed

4. Fax number

Contact nformation Redacted

5. If applicable, website or URL

http://www.schlundtech.com

Primary Contact

6(a). Name

John Kane

6(b). Title

Vice President, Corporate Services

6(c). Address

6(d). Phone Number

Contact nformation Redacted

6(e). Fax Number

6(f). Email Address

Contact Information Redacted

Secondary Contact

7(a). Name

Alex Howerton

7(b). Title

Account Manager

7(c). Address

7(d). Phone Number

Contact Information Redacted

7(e). Fax Number

7(f). Email Address

Contact Information Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

limited liability corporation (Gesellschaft mit beschränkter Haftung, GmbH)

8(b). State the specific national or other jursidiction that defines the type of entity identified in 8(a).

Germany

8(c). Attach evidence of the applicant's establishment.

Attachments are not displayed on this form.

9(a). If applying company is publicly traded, provide the exchange and symbol.

9(b). If the applying entity is a subsidiary, provide the parent company.

InterNetX GmbH

9(c). If the applying entity is a joint venture, list all joint venture partners.

not a joint venture

Applicant Background

11(a). Name(s) and position(s) of all directors

11(b). Name(s) and position(s) of all officers and partners

Thomas Mörz	CEO

11(c). Name(s) and position(s) of all shareholders holding at least 15% of shares

InterNetX GmbH	not applicable

11(d). For an applying entity that does not have directors, officers, partners, or shareholders: Name(s) and position(s) of all individuals having legal or executive responsibility

Applied-for gTLD string

13. Provide the applied-for gTLD string. If an IDN, provide the U-label.

WEB

14(a). If an IDN, provide the A-label (beginning with "xn--").

14(b). If an IDN, provide the meaning or restatement of the string in English, that is, a description of the literal meaning of the string in the opinion of the applicant.

14(c). If an IDN, provide the language of the label (in English).

14(c). If an IDN, provide the language of the label (as referenced by ISO-639-1).

14(d). If an IDN, provide the script of the label (in English).

14(d). If an IDN, provide the script of the label (as referenced by ISO 15924).

14(e). If an IDN, list all code points contained in the U-label according to Unicode form.

15(a). If an IDN, Attach IDN Tables for the proposed registry.

Attachments are not displayed on this form.

15(b). Describe the process used for development of the IDN tables submitted, including consultations and sources used.

15(c). List any variant strings to the applied-for gTLD string according to the relevant IDN tables.

16. Describe the applicant's efforts to ensure that there are no known operational or rendering problems concerning the applied-for gTLD string. If such issues are known, describe steps that will be taken to mitigate these issues in software and other applications.

Schlund Technologies GmbH, supported by Afilias, the back-end provider of registry services, anticipates the introduction of this TLD without operational or rendering problems. Based on a decade of experience launching and operating new TLDs, Afilias, the back-end provider of registry services for this TLD, is confident the launch and operation of this TLD presents no known challenges. The rationale for this opinion includes:
• The string is not complex and is represented in standard ASCII characters and follows relevant technical, operational and policy standards;
• The string length is within lengths currently supported in the root and by ubiquitous Internet programs such as web browsers and mail applications;
• There are no new standards required for the introduction of this TLD;
• No onerous requirements are being made on registrars, registrants or Internet users, and;
• The existing secure, stable and reliable Afilias SRS, DNS, WHOIS and supporting systems and staff are amply provisioned and prepared to meet the needs of this TLD.

17. (OPTIONAL) Provide a representation of the label according to the International Phonetic Alphabet (http://www.langsci.ucl.ac.uk/ipa/).

Mission/Purpose

18(a). Describe the mission/purpose of your proposed gTLD.

.WEB is intended to become one of the most common and easily accessible TLDs on the Internet, vastly expanding options for creating domains, and giving new opportunities to those who were unable to obtain a desired domain name under the existing TLD structure.

At the end of 2011, there were 95.5 million registered .com domain names and 220 million total registered domain names (Source: http://royal.pingdom.com/2012/01/17/internet-2011-in-numbers/). The interest and demand for new domains is only expected to grow. The .WEB TLD will help facilitate the expansion of those opportunities for Internet users, with a concise and memorable extension.

We expect that the demand to create and own new domains will drive the rapid expansion of the .WEB TLD. In conjunction with our branding and registrar promotion, we forecast 1,371,900 domains under management (DUMs) after three years.

18(b). How do you expect that your proposed gTLD will benefit registrants, Internet users, and others?

.WEB will quickly develop into one of the premier, open TLDs on the Internet.

i General goals
Schlund Technologies GmbH will engage in general marketing and branding, as well as outreach and marketing support to registrars to establish awareness of the .WEB TLD and its intended uses in the minds of the public. The anticipated popularity of this TLD will make it very attractive to registrars, incentivizing them to work with Schlund Technologies GmbH to make the TLD grow rapidly.

ii How .WEB adds to the current space
.WEB facilitates greatly expanded opportunities for domain creation and innovative use of the

Internet. Individuals and entities who have felt limited in their opportunities to obtain a desired domain name will have new options available to them.

With a TLD as concise and memorable as .WEB, Internet users will have a truly unburdened space to create an online entity devoid of associations with a commercial enterprise. Despite its broad use, the .com extension has a market perception of domains with a business or commercially focused purpose. With a .WEB domain, the average consumer has an option to create content, host mail servers or provide other services with a name that does not carry images of a business. For the online-only retailer, there will exist the opportunity to create a brand without a brick-and-mortar expectations. Overall, the vast and Internet-focused character of .WEB adds a universally understandable new home for domains.

iii User experience goals
Schlund Technologies GmbH intends for .WEB to be one of the most recognizable and useful TLDs on the Internet. .WEB will be positioned as not simply an alternative to existing generic gTLDS, but as an expanded option beyond existing opportunities to develop an Internet identity and presence. The explosion of new domain possibilities will foster innovation and creativity on the part of registrants, who will then create new and diverse user experiences for users. The competition among new registrants, as well as with established site operators, will improve the user experience.

iv Registry policies
.WEB will be an open TLD, generally available to all registrants (except in the Sunrise period).

In general, domains will be offered for periods of one to ten years, but no greater than ten years. Initial registrations made in the Sunrise period may have a minimum number of years required. For example, there may be a policy that all Sunrise names must be registered for an initial term of at least two years.

The roll-out of our TLD is anticipated to feature the following phases:
• Reservation of reserved names and premium names, which will be distributed through special mechanisms (detailed below).
• Sunrise – the required period for trademark owners to secure their domains before availability to the general public. This phase will feature applications for domain strings, verification of trademarks via Trademark Clearinghouse and a trademark verification agent, auctions between qualified parties who wish to secure the same string, and a Trademark Claims Service.
• General Availability period – real-time registrations, made on a first-come first-served basis. Trademark Claims Service will be in use at least for the first 60 days after General Availability applications open.
The registration of domain names in the .WEB TLD will follow the standard practices, procedures and policies Afilias, the back-end provider of registry services, currently has in place. This includes the following:
• Domain registration policies (for example, grace periods, transfer policies, etc.) are defined in response #27.
• Abuse prevention tools and policies, for example, measures to promote WHOIS accuracy and efforts to reduce phishing and pharming, are discussed in detail in our response #28.
• Rights protection mechanisms and dispute resolution mechanism policies (for example, UDRP, URS) are detailed in #29.

Other detailed policies for this domain include policies for reserved names.

Reserved names

There are two categories of reserved names for this TLD: registry reserved and premium names.
Registry reserved names

We will reserve the following classes of domain names, which will not be made generally available to registrants via the Sunrise or subsequent periods:
• All of the reserved names required in Specification 5 of the new gTLD Registry Agreement;
• The geographic names required in Specification 5 of the new gTLD Registry Agreement, and may

be released to the extent that Registry Operator reaches agreement with the government and country-code manager;
• The registry operator's own name and variations thereof, and registry operations names (such as registry.tld, and www.tld), for internal use;
• Names related to ICANN and Internet standards bodies (iana.tld, ietf.tld, w3c.tld, etc.), and may be released to the extent that Registry Operator reaches agreement with ICANN.

The list of reserved names will be published publicly before the Sunrise period begins, so that registrars and potential registrants will know which names have been set aside.

Premium names
The registry will also designate a set of premium domain names, set aside for distribution via special mechanisms. The list of premium names will be published publicly before the Sunrise period begins, so that registrars and potential registrants will know that these names are not available. Premium names may be distributed via mechanisms such as requests for proposals, contests, direct sales, and auctions.
For the auctioning of premium names, we intend to contract with an established auction provider that has successfully conducted domain auctions. This will ensure that there is a tested, trustworthy technical platform for the auctions, auditable records, and reliable collection mechanisms. With our chosen auction provider, we will create and post policies and procedures that ensure clear, fair, and ethical auctions. As an example of such a policy, all employees of the registry operator and its contractors will be strictly prohibited from bidding in auctions for domains in the TLD. We expect a comprehensive and robust set of auction rules to cover possible scenarios, such as how domains will be awarded if the winning bidder does not make payment.

v. Privacy and confidential information protection
As per the New gTLD Registry Agreement, we will make domain contact data (and other fields) freely and publicly available via a Web-based WHOIS server. This default set of fields includes the mandatory publication of registrant data. Our Registry-Registrar Agreement will require that registrants consent to this publication.

We shall notify each of our registrars regarding the purposes for which data about any identified or identifiable natural person ("Personal Data") submitted to the Registry Operator by such registrar is collected and used, and the intended recipients (or categories of recipients) of such Personal Data (the data in question is essentially the registrant and contact data required to be published in the WHOIS). We will require each registrar to obtain the consent of each registrant in the TLD for the collection and use of such Personal Data. The policies will be posted publicly on our TLD web site. As the registry operator, we shall not use or authorize the use of Personal Data in any way that is incompatible with the notice provided to registrars.

Our privacy and data use policies are as follows:
• As registry operator, we do not plan on selling bulk WHOIS data. We will not sell contact data in any way. We will not allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations.
• We may use registration data in the aggregate for marketing purposes.
• DNS query data will never be sold in a way that is personally identifiable.
• We may from time to time use the demographic data collected for statistical analysis, provided that this analysis will not disclose individual Personal Data and provided that such use is compatible with the notice provided to registrars regarding the purpose and procedures for such use.

As the registry operator we shall take significant steps to protect Personal Data collected from registrars from loss, misuse, unauthorized disclosure, alteration, or destruction. In our responses to Question 30 ("Security Policy") and Question 38 ("Escrow") we detail the security policies and procedures we will use to protect the registry system and the data contained therein from unauthorized access and loss.

Please see our response to Question 26 ("WHOIS") regarding "searchable WHOIS" and rate-limiting. That section contains details about how we will limit the mining of WHOIS data by spammers and other parties who abuse access to the WHOIS.

In order to acquire and maintain accreditation for our TLD, we will require registrars to adhere to certain information technology policies designed to help protect registrant data. These will include standards for access to the registry system and password management protocols. Our response to Question 30, “Security Policy” provides details of implementation.

We will allow the use of proxy and privacy services, which can protect the personal data of registrants from spammers and other parties that mine zone files and WHOIS data. We are aware that there are parties who may use privacy services to protect their free speech rights, or to avoid religious or political persecution.

18(c). What operating rules will you adopt to eliminate or minimize social costs?

Schlund Technologies GmbH, supported by Afilias, the back-end provider of registry services, has adopted the above-mentioned and other policies to ensure fair and equitable access and cost structures to the Internet community, including:
• no new burdens placed on the Internet community to resolve name disputes
• utilization of standard registration practices and policies (as detailed in responses to questions 27, 28, 29)
• protection of trademarks at launch and on-going operations (as detailed in the response to question 29)
• fair and reasonable wholesale prices
• fair and equitable treatment of registrars

As per the ICANN Registry Agreement, we will use only ICANN-accredited registrars, and will provide non-discriminatory access to registry services to those registrars.

Pricing Policies and Commitments

Pricing for domain names at General Availability will be €6 per domain year for the first year, then increase 5.0% per year in subsequent years for the next five years. Applicant reserves the right to reduce this pricing for promotional purposes in a manner available to all accredited registrars. Registry Operator reserves the right to work with ICANN to initiate an increase in the wholesale price of domains if required. Registry Operator will provide reasonable notice to the registrars of any approved price increase.

Community-based Designation

19. Is the application for a community-based TLD?

No

20(a). Provide the name and full description of the community that the applicant is committing to serve.

20(b). Explain the applicant's relationship to the community identified in 20(a).

20(c). Provide a description of the community-based purpose of the applied-for gTLD.

20(d). Explain the relationship between the applied-for gTLD string and the community identified in 20(a).

20(e). Provide a description of the applicant's intended registration policies in support of the community-based purpose of the applied-for gTLD.

20(f). Attach any written endorsements from institutions/groups representative of the community identified in 20(a).

Attachments are not displayed on this form.

Geographic Names

21(a). Is the application for a geographic name?

No

Protection of Geographic Names

22. Describe proposed measures for protection of geographic names at the second and other levels in the applied-for gTLD.

We will protect names with national or geographic significance by reserving the country and territory names at the second level and at all other levels within the TLD, as per the requirements in the New TLD Registry Agreement (Specification 5, paragraph 5).

We will employ a series of rules to translate the geographical names required to be reserved by Specification 5, paragraph 5 to a form consistent with the "host names" format used in domain names.

Considering the Governmental Advisory Committee (GAC) advice "Principles regarding new gTLDs", these domains will be blocked, at no cost to governments, public authorities, or IGOs,

before the TLD is introduced (Sunrise), so that no parties may apply for them. We will publish a list of these names before Sunrise, so our registrars and their prospective applicants can be aware that these names are reserved.

We will define a procedure so that governments can request the above reserved domain(s) if they would like to take possession of them. This procedure will be based on existing methodology developed for the release of country names in the .INFO TLD. For example, we will require a written request from the country's GAC representative, or a written request from the country's relevant Ministry or Department. We will allow the designated beneficiary (the Registrant) to register the name, with an accredited Afilias Registrar, possibly using an authorization number transmitted directly to the designated beneficiary in the country concerned.

As defined by Specification 5, paragraph 5, such geographic domains may be released to the extent that Registry Operator reaches agreement with the applicable government(s). Registry operator will work with respective GAC representatives of the country's relevant Ministry of Department to obtain their release of the names to the Registry Operator.

If internationalized domains names (IDNs) are introduced in the TLD in the future, we will also reserve the IDN versions of the country names in the relevant script(s) before IDNs become available to the public. If we find it advisable and practical, we will confer with relevant language authorities so that we can reserve the IDN domains properly along with their variants.

Regarding GAC advice regarding second-level domains not specified via Specification 5, paragraph 5: All domains awarded to registrants are subject to the Uniform Domain Name Dispute Resolution Policy (UDRP), and to any properly-situated court proceeding. We will ensure appropriate procedures to allow governments, public authorities or IGO's to challenge abuses of names with national or geographic significance at the second level. In its registry-registrar agreement, and flowing down to registrar-registrant agreements, the registry operator will institute a provision to suspend domains names in the event of a dispute. We may exercise that right in the case of a dispute over a geographic name.

Registry Services

23. Provide name and full description of all the Registry Services to be provided.

Throughout the technical portion (#23 - #44) of this application, answers are provided directly from Afilias, the back-end provider of registry services for this TLD. Schlund Technologies GmbH chose Afilias as its back-end provider because Afilias has more experience successfully applying to ICANN and launching new TLDs than any other provider. Afilias is the ICANN-contracted registry operator of the .INFO and .MOBI TLDs, and Afilias is the back-end registry services provider for other ICANN TLDs including .ORG, .ASIA, .AERO, and .XXX.

Registry services for this TLD will be performed by Afilias in the same responsible manner used to support 16 top level domains today. Afilias supports more ICANN-contracted TLDs (6) than any other provider currently. Afilias' primary corporate mission is to deliver secure, stable and reliable registry services. This TLD will utilize an existing, proven team and platform for registry services with:
• A stable and secure, state-of-the-art, EPP-based SRS with ample storage capacity, data security provisions and scalability that is proven with registrars who account for over 95% of all gTLD domain name registration activity (over 375 registrars);
• A reliable, 100% available DNS service (zone file generation, publication and dissemination) tested to withstand severe DDoS attacks and dramatic growth in Internet use;
• A WHOIS service that is flexible and standards compliant, with search capabilities to address both registrar and end-user needs; includes consideration for evolving standards, such

as RESTful, or draft-kucherawy-wierds;
• Experience introducing IDNs in the following languages: German (DE), Spanish (ES), Polish (PL), Swedish (SV), Danish (DA), Hungarian (HU), Icelandic (IS), Latvian (LV), Lithuanian (LT), Korean (KO), Simplified and Traditional Chinese (CN), Devanagari (HI-DEVA), Russian (RU), Belarusian (BE), Ukrainian (UK), Bosnian (BS), Serbian (SR), Macedonian (MK) and Bulgarian (BG) across the TLDs it serves;
• A registry platform that is both IPv6 and DNSSEC enabled;
• An experienced, respected team of professionals active in standards development of innovative services such as DNSSEC and IDN support;
• Methods to limit domain abuse, remove outdated and inaccurate data, and ensure the integrity of the SRS, and;
• Customer support and reporting capabilities to meet financial and administrative needs, e.g., 24x7 call center support, integration support, billing, and daily, weekly, and monthly reporting.

Afilias will support this TLD in accordance with the specific policies and procedures of Schlund Technologies GmbH (the “registry operator”), leveraging a proven registry infrastructure that is fully operational, staffed with professionals, massively provisioned, and immediately ready to launch and maintain this TLD.

The below response includes a description of the registry services to be provided for this TLD, additional services provided to support registry operations, and an overview of Afilias’ approach to registry management.

Registry services to be provided

To support this TLD, Schlund Technologies GmbH and Afilias will offer the following registry services, all in accordance with relevant technical standards and policies:
• Receipt of data from registrars concerning registration for domain names and nameservers, and provision to registrars of status information relating to the EPP-based domain services for registration, queries, updates, transfers, renewals, and other domain management functions. Please see our responses to questions #24, #25, and #27 for full details, which we request be incorporated here by reference.
• Operation of the registry DNS servers: The Afilias DNS system, run and managed by Afilias, is a massively provisioned DNS infrastructure that utilizes among the most sophisticated DNS architecture, hardware, software and redundant design created. Afilias’ industry-leading system works in a seamless way to incorporate nameservers from any number of other secondary DNS service vendors. Please see our response to question #35 for full details, which we request be incorporated here by reference.
• Dissemination of TLD zone files: Afilias’ distinctive architecture allows for real-time updates and maximum stability for zone file generation, publication and dissemination. Please see our response to question #34 for full details, which we request be incorporated here by reference.
• Dissemination of contact or other information concerning domain registrations: A port 43 WHOIS service with basic and expanded search capabilities with requisite measures to prevent abuse. Please see our response to question #26 for full details, which we request be incorporated here by reference.
• Internationalized Domain Names (IDNs): Ability to support all protocol valid Unicode characters at every level of the TLD, including alphabetic, ideographic and right-to-left scripts, in conformance with the ICANN IDN Guidelines. Please see our response to question #44 for full details, which we request be incorporated here by reference.
• DNS Security Extensions (DNSSEC): A fully DNSSEC-enabled registry, with a stable and efficient means of signing and managing zones. This includes the ability to safeguard keys and manage keys completely. Please see our response to question #43 for full details, which we request be incorporated here by reference.

Each service will meet or exceed the contract service level agreement. All registry services for this TLD will be provided in a standards-compliant manner.

Security
Afilias addresses security in every significant aspect – physical, data and network as well as process. Afilias’ approach to security permeates every aspect of the registry services

provided. A dedicated security function exists within the company to continually identify existing and potential threats, and to put in place comprehensive mitigation plans for each identified threat. In addition, a rapid security response plan exists to respond comprehensively to unknown or unidentified threats. The specific threats and Afilias mitigation plans are defined in our response to question #30(b); please see that response for complete information. In short, Afilias is committed to ensuring the confidentiality, integrity, and availability of all information.

New registry services

No new registry services are planned for the launch of this TLD.

Additional services to support registry operation

Numerous supporting services and functions facilitate effective management of the TLD. These support services are also supported by Afilias, including:
• Customer support: 24x7 live phone and e-mail support for customers to address any access, update or other issues they may encounter. This includes assisting the customer identification of the problem as well as solving it. Customers include registrars and the registry operator, but not registrants except in unusual circumstances. Customers have access to a web-based portal for a rapid and transparent view of the status of pending issues.
• Financial services: billing and account reconciliation for all registry services according to pricing established in respective agreements.

Reporting is an important component of supporting registry operations. Afilias will provide reporting to the registry operator and registrars, and financial reporting.

Reporting provided to registry operator
Afilias provides an extensive suite of reports to the registry operator, including daily, weekly and monthly reports with data at the transaction level that enable the registry operator to track and reconcile at whatever level of detail preferred. Afilias provides the exact data required by ICANN in the required format to enable the registry operator to meet its technical reporting requirements to ICANN.

In addition, Afilias offers access to a data warehouse capability that will enable near real-time data to be available 24x7. This can be arranged by informing the Afilias Account Manager regarding who should have access. Afilias' data warehouse capability enables drill-down analytics all the way to the transaction level.

Reporting available to registrars
Afilias provides an extensive suite of reporting to registrars and has been doing so in an exemplary manner for more than ten years. Specifically, Afilias provides daily, weekly and monthly reports with detail at the transaction level to enable registrars to track and reconcile at whatever level of detail they prefer.

Reports are provided in standard formats, facilitating import for use by virtually any registrar analytical tool. Registrar reports are available for download via a secure administrative interface. A given registrar will only have access to its own reports. These include the following:
• Daily Reports: Transaction Report, Billable Transactions Report, and Transfer Reports;
• Weekly: Domain Status and Nameserver Report, Weekly Nameserver Report, Domains Hosted by Nameserver Weekly Report, and;
• Monthly: Billing Report and Monthly Expiring Domains Report.

Weekly registrar reports are maintained for each registrar for four weeks. Weekly reports older than four weeks will be archived for a period of six months, after which they will be deleted.

Financial reporting
Registrar account balances are updated real-time when payments and withdrawals are posted to the registrars' accounts. In addition, the registrar account balances are updated as and when

they perform billable transactions at the registry level.

Afilias provides Deposit/Withdrawal Reports that are updated periodically to reflect payments received or credits and withdrawals posted to the registrar accounts.

The following reports are also available: a) Daily Billable Transaction Report, containing details of all the billable transactions performed by all the registrars in the SRS, b) daily e-mail reports containing the number of domains in the registry and a summary of the number and types of billable transactions performed by the registrars, and c) registry operator versions of most registrar reports (for example, a daily Transfer Report that details all transfer activity between all of the registrars in the SRS).

Afilias approach to registry support

Afilias, the back end registry services provider for this TLD, is dedicated to managing the technical operations and support of this TLD in a secure, stable and reliable manner. Afilias has worked closely with Schlund Technologies GmbH to review specific needs and objectives of this TLD. The resulting comprehensive plans are illustrated in technical responses #24-44, drafted by Afilias given Schlund Technologies GmbH requirements. Afilias and Schlund Technologies GmbH also worked together to provide financial responses for this application which demonstrate cost and technology consistent with the size and objectives of this TLD.

Afilias is the registry services provider for this and several other TLD applications. Over the past 11 years of providing services for gTLD and ccTLDs, Afilias has accumulated experience about resourcing levels necessary to provide high quality services with conformance to strict service requirements. Afilias currently supports over 20 million domain names, spread across 16 TLDs, with over 400 accredited registrars.

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

With over a decade of registry experience, Afilias has the depth and breadth of experience that ensure existing and new needs are addressed, all while meeting or exceeding service level requirements and customer expectations. This is evident in Afilias' participation in business, policy and technical organizations supporting registry and Internet technology within ICANN and related organizations. This allows Afilias to be at the forefront of security initiatives such as: DNSSEC, wherein Afilias worked with Public Interest Registry (PIR) to make the .ORG registry the first DNSSEC enabled gTLD and the largest TLD enabled at the time; in enhancing the Internet experience for users across the globe by leading development of IDNs; in pioneering the use of open-source technologies by its usage of PostgreSQL, and; being the first to offer near-real-time dissemination of DNS zone data.

The ability to observe tightening resources for critical functions and the capacity to add extra resources ahead of a threshold event are factors that Afilias is well versed in. Afilias' human resources team, along with well-established relationships with external organizations, enables it to fill both long-term and short-term resource needs expediently.

Afilias' growth from a few domains to serving 20 million domain names across 16 TLDs and 400 accredited registrars indicates that the relationship between the number of people required and the volume of domains supported is not linear. In other words, servicing 100 TLDs does not automatically require 6 times more staff than servicing 16 TLDs. Similarly, an increase in the number of domains under management does not require in a linear increase in resources. Afilias carefully tracks the relationship between resources deployed and domains to be serviced, and pro-actively reviews this metric in order to retain a safe margin of error. This enables

Afilias to add, train and prepare new staff well in advance of the need, allowing consistent delivery of high quality services.

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

Answers for this question (#24) are provided directly from Afilias, the back-end provider of registry services for this TLD.

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS (THE “〈” and “〉” CHARACTERS), WHICH ICANN INFORMS AFILIAS (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE FULL ANSWER TO THIS QUESTION IS ATTACHED AS A PDF FILE.

Afilias operates a state-of-the-art EPP-based Shared Registration System (SRS) that is secure, stable and reliable. The SRS is a critical component of registry operations that must balance the business requirements for the registry and its customers, such as numerous domain acquisition and management functions. The SRS meets or exceeds all ICANN requirements given that Afilias:
• Operates a secure, stable and reliable SRS which updates in real-time and in full compliance with Specification 6 of the new gTLD Registry Agreement;
• Is committed to continuously enhancing our SRS to meet existing and future needs;
• Currently exceeds contractual requirements and will perform in compliance with Specification 10 of the new gTLD Registry Agreement;
• Provides SRS functionality and staff, financial, and other resources to more than adequately meet the technical needs of this TLD, and;
• Manages the SRS with a team of experienced technical professionals who can seamlessly integrate this TLD into the Afilias registry platform and support the TLD in a secure, stable and reliable manner.

Description of operation of the SRS, including diagrams

Afilias’ SRS provides the same advanced functionality as that used in the .INFO and .ORG registries, as well as the fourteen other TLDs currently supported by Afilias. The Afilias registry system is standards-compliant and utilizes proven technology, ensuring global familiarity for registrars, and it is protected by our massively provisioned infrastructure that mitigates the risk of disaster.

EPP functionality is described fully in our response to question #25; please consider those answers incorporated here by reference. An abbreviated list of Afilias SRS functionality includes:
• Domain registration: Afilias provides registration of names in the TLD, in both ASCII and IDN forms, to accredited registrars via EPP and a web-based administration tool.
• Domain renewal: Afilias provides services that allow registrars the ability to renew domains under sponsorship at any time. Further, the registry performs the automated renewal of all domain names at the expiration of their term, and allows registrars to rescind automatic renewals within a specified number of days after the transaction for a full refund.
• Transfer: Afilias provides efficient and automated procedures to facilitate the transfer of sponsorship of a domain name between accredited registrars. Further, the registry enables bulk transfers of domains under the provisions of the Registry-Registrar Agreement.
• RGP and restoring deleted domain registrations: Afilias provides support for the Redemption Grace Period (RGP) as needed, enabling the restoration of deleted registrations.
• Other grace periods and conformance with ICANN guidelines: Afilias provides support for other grace periods that are evolving as standard practice inside the ICANN community. In addition, the Afilias registry system supports the evolving ICANN guidelines on IDNs.

Afilias also supports the basic check, delete, and modify commands.

As required for all new gTLDs, Afilias provides “thick” registry system functionality. In this model, all key contact details for each domain are stored in the registry. This allows better access to domain data and provides uniformity in storing the information.

Afilias’ SRS complies today and will continue to comply with global best practices including relevant RFCs, ICANN requirements, and this TLD’s respective domain policies. With over a decade of experience, Afilias has fully documented and tested policies and procedures, and our highly skilled team members are active participants of the major relevant technology and standards organizations, so ICANN can be assured that SRS performance and compliance are met. Full details regarding the SRS system and network architecture are provided in responses to questions #31 and #32; please consider those answers incorporated here by reference.

SRS servers and software

All applications and databases for this TLD will run in a virtual environment currently hosted by a cluster of servers equipped with the latest Intel Westmere multi-core processors. (It is possible that by the time this application is evaluated and systems deployed, Westmere processors may no longer be the “latest”; the Afilias policy is to use the most advanced, stable technology available at the time of deployment.) The data for the registry will be stored on storage arrays of solid state drives shared over a fast storage area network. The virtual environment allows the infrastructure to easily scale both vertically and horizontally to cater to changing demand. It also facilitates effective utilization of system resources, thus reducing energy consumption and carbon footprint.

The network firewalls, routers and switches support all applications and servers. Hardware traffic shapers are used to enforce an equitable access policy for connections coming from registrars. The registry system accommodates both IPv4 and IPv6 addresses. Hardware load balancers accelerate TLS/SSL handshaking and distribute load among a pool of application servers.

Each of the servers and network devices are equipped with redundant, hot-swappable components and multiple connections to ancillary systems. Additionally, 24x7 support agreements with a four-hour response time at all our data centers guarantee replacement of failed parts in the shortest time possible.

Examples of current system and network devices used are:
- Servers: Cisco UCS B230 blade servers
- SAN storage arrays: IBM Storwize V7000 with Solid State Drives
- SAN switches: Brocade 5100
- Firewalls: Cisco ASA 5585-X
- Load balancers: F5 Big-IP 6900
- Traffic shapers: Procera PacketLogic PL8720
- Routers: Juniper MX40 3D
- Network switches: Cisco Nexus 7010, Nexus 5548, Nexus 2232

These system components are upgraded and updated as required, and have usage and performance thresholds which trigger upgrade review points. In each data center, there is a minimum of two of each network component, a minimum of 25 servers, and a minimum of two storage arrays.

Technical components of the SRS include the following items, continually checked and upgraded as needed: SRS, WHOIS, web admin tool, DNS, DNS distributor, reporting, invoicing tools, and deferred revenue system (as needed).

All hardware is massively provisioned to ensure stability under all forecast volumes from launch through “normal” operations of average daily and peak capacities. Each and every system application, server, storage and network device is continuously monitored by the Afilias Network Operations Center for performance and availability. The data gathered is used by dynamic predictive analysis tools in real-time to raise alerts for unusual resource demands. Should any volumes exceed established thresholds, a capacity planning review is instituted which will address the need for additions well in advance of their actual need.

SRS diagram and interconnectivity description

As with all core registry services, the SRS is run from a global cluster of registry system data centers, located in geographic centers with high Internet bandwidth, power, redundancy and availability. All of the registry systems will be run in a 〈n+1〉 setup, with a primary data center and a secondary data center. For detailed site information, please see our responses to questions #32 and #35. Registrars access the SRS in real-time using EPP.

A sample of the Afilias SRS technical and operational capabilities (displayed in Figure 24-a) include:
• Geographically diverse redundant registry systems;
• Load balancing implemented for all registry services (e.g. EPP, WHOIS, web admin) ensuring equal experience for all customers and easy horizontal scalability;
• Disaster Recovery Point objective for the registry is within one minute of the loss of the primary system;
• Detailed and tested contingency plan, in case of primary site failure, and;
• Daily reports, with secure access for confidentiality protection.

As evidenced in Figure 24-a, the SRS contains several components of the registry system. The interconnectivity ensures near-real-time distribution of the data throughout the registry infrastructure, timely backups, and up-to-date billing information.

The WHOIS servers are directly connected to the registry database and provide real-time responses to queries using the most up-to-date information present in the registry.

Committed DNS-related EPP objects in the database are made available to the DNS Distributor via a dedicated set of connections. The DNS Distributor extracts committed DNS-related EPP objects in real time and immediately inserts them into the zone for dissemination.

The Afilias system is architected such that read-only database connections are executed on database replicas and connections to the database master (where write-access is executed) are carefully protected to ensure high availability.

This interconnectivity is monitored, as is the entire registry system, according to the plans detailed in our response to question #42.

Synchronization scheme

Registry databases are synchronized both within the same data center and in the backup data center using a database application called Slony. For further details, please see the responses to questions #33 and #37. Slony replication of transactions from the publisher (master) database to its subscribers (replicas) works continuously to ensure the publisher and its subscribers remain synchronized. When the publisher database completes a transaction the Slony replication system ensures that each replica also processes the transaction. When there are no transactions to process, Slony “sleeps” until a transaction arrives or for one minute, whichever comes first. Slony “wakes up” each minute to confirm with the publisher that there has not been a transaction and thus ensures subscribers are synchronized and the replication time lag is minimized. The typical replication time lag between the publisher and subscribers depends on the topology of the replication cluster, specifically the location of the subscribers relative to the publisher. Subscribers located in the same data center as the publisher are typically updated within a couple of seconds, and subscribers located in a secondary data center are typically updated in less than ten seconds. This ensures real-time or near-real-time synchronization between all databases, and in the case where the secondary data center needs to be activated, it can be done with minimal disruption to registrars.

SRS SLA performance compliance

Afilias has a ten-year record of delivering on the demanding ICANN SLAs, and will continue to provide secure, stable and reliable service in compliance with SLA requirements as specified in the new gTLD Registry Agreement, Specification 10, as presented in Figure 24-b.

The Afilias SRS currently handles over 200 million EPP transactions per month for just .INFO and .ORG. Overall, the Afilias SRS manages over 700 million EPP transactions per month for all TLDs under management.

Given this robust functionality, and more than a decade of experience supporting a thick TLD registry with a strong performance history, Afilias, on behalf of Schlund Technologies GmbH, will meet or exceed the performance metrics in Specification 10 of the new gTLD Registry Agreement. The Afilias services and infrastructure are designed to scale both vertically and horizontally without any downtime to provide consistent performance as this TLD grows. The Afilias architecture is also massively provisioned to meet seasonal demands and marketing campaigns. Afilias' experience also gives high confidence in the ability to scale and grow registry operations for this TLD in a secure, stable and reliable manner.

SRS resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

Over 100 Afilias team members contribute to the management of the SRS code and network that will support this TLD. The SRS team is composed of Software Engineers, Quality Assurance Analysts, Application Administrators, System Administrators, Storage Administrators, Network Administrators, Database Administrators, and Security Analysts located at three geographically separate Afilias facilities. The systems and services set up and administered by these team members are monitored 24x7 by skilled analysts at two NOCs located in Toronto, Ontario (Canada) and Horsham, Pennsylvania (USA). In addition to these team members, Afilias also utilizes trained project management staff to maintain various calendars, work breakdown schedules, utilization and resource schedules and other tools to support the technical and management staff. It is this team who will both deploy this TLD on the Afilias infrastructure, and maintain it. Together, the Afilias team has managed 11 registry transitions and six new TLD launches, which illustrate its ability to securely and reliably deliver regularly scheduled updates as well as a secure, stable and reliable SRS service for this TLD.

25. Extensible Provisioning Protocol (EPP)

Answers for this question (#25) are provided by Afilias, the back-end provider of registry services for this TLD.

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS (THE " 〈" and "〉 " CHARACTERS), WHICH ICANN INFORMS AFILIAS (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE FULL ANSWER TO THIS QUESTION IS ATTACHED AS A PDF FILE.

Afilias has been a pioneer and innovator in the use of EPP. .INFO was the first EPP-based gTLD registry and launched on EPP version 02⁄00. Afilias has a track record of supporting TLDs on standards-compliant versions of EPP. Afilias will operate the EPP registrar interface as well as a web-based interface for this TLD in accordance with RFCs and global best practices. In addition, Afilias will maintain a proper OT&E (Operational Testing and Evaluation) environment to facilitate registrar system development and testing.

Afilias' EPP technical performance meets or exceeds all ICANN requirements as demonstrated by:
• A completely functional, state-of-the-art, EPP-based SRS that currently meets the needs of various gTLDs and will meet this new TLD's needs;

• A track record of success in developing extensions to meet client and registrar business requirements such as multi-script support for IDNs;
• Supporting six ICANN gTLDs on EPP: .INFO, .ORG, .MOBI, .AERO, .ASIA and .XXX
• EPP software that is operating today and has been fully tested to be standards-compliant;
• Proven interoperability of existing EPP software with ICANN-accredited registrars, and;
• An SRS that currently processes over 200 million EPP transactions per month for both .INFO and .ORG. Overall, Afilias processes over 700 million EPP transactions per month for all 16 TLDs under management.

The EPP service is offered in accordance with the performance specifications defined in the new gTLD Registry Agreement, Specification 10.

EPP Standards

The Afilias registry system complies with the following revised versions of the RFCs and operates multiple ICANN TLDs on these standards, including .INFO, .ORG, .MOBI, .ASIA and .XXX. The systems have been tested by our Quality Assurance ("QA") team for RFC compliance, and have been used by registrars for an extended period of time:
• 3735 - Guidelines for Extending EPP
• 3915 - Domain Registry Grace Period Mapping
• 5730 - Extensible Provisioning Protocol (EPP)
• 5731 - Domain Name Mapping
• 5732 - Host Mapping
• 5733 - Contact Mapping
• 5734 - Transport Over TCP
• 5910 - Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)

This TLD will support all valid EPP commands. The following EPP commands are in operation today and will be made available for this TLD. See attachment #25a for the base set of EPP commands and copies of Afilias XSD schema files, which define all the rules of valid, RFC compliant EPP commands and responses that Afilias supports. Any customized EPP extensions, if necessary, will also conform to relevant RFCs.

Afilias staff members actively participated in the Internet Engineering Task Force (IETF) process that finalized the new standards for EPP. Afilias will continue to actively participate in the IETF and will stay abreast of any updates to the EPP standards.

EPP software interface and functionality

Afilias will provide all registrars with a free open-source EPP toolkit. Afilias provides this software for use with both Microsoft Windows and Unix/Linux operating systems. This software, which includes all relevant templates and schema defined in the RFCs, is available on sourceforge.net and will be available through the registry operator's website.

Afilias' SRS EPP software complies with all relevant RFCs and includes the following functionality:
• EPP Greeting: A response to a successful connection returns a greeting to the client. Information exchanged can include: name of server, server date and time in UTC, server features, e.g., protocol versions supported, languages for the text response supported, and one or more elements which identify the objects that the server is capable of managing;
• Session management controls: 〈login〉 to establish a connection with a server, and 〈logout〉 to end a session;
• EPP Objects: Domain, Host and Contact for respective mapping functions;
• EPP Object Query Commands: Info, Check, and Transfer (query) commands to retrieve object information, and;
• EPP Object Transform Commands: five commands to transform objects: 〈create〉 to create an instance of an object, 〈delete〉 to remove an instance of an object, 〈renew〉 to extend the validity period of an object, 〈update〉 to change information associated with an object, and 〈transfer〉 to manage changes in client sponsorship of a known object.

Currently, 100% of the top domain name registrars in the world have software that has already been tested and certified to be compatible with the Afilias SRS registry. In total, over 375 registrars, representing over 95% of all registration volume worldwide, operate software that has been certified compatible with the Afilias SRS registry. Afilias' EPP Registrar Acceptance Criteria are available in attachment #25b, EPP OT&E Criteria.

Free EPP software support
Afilias analyzes and diagnoses registrar EPP activity log files as needed and is available to assist registrars who may require technical guidance regarding how to fix repetitive errors or exceptions caused by misconfigured client software.

Registrars are responsible for acquiring a TLS/SSL certificate from an approved certificate authority, as the registry-registrar communication channel requires mutual authentication; Afilias will acquire and maintain the server-side TLS/SSL certificate. The registrar is responsible for developing support for TLS/SSL in their client application. Afilias will provide free guidance for registrars unfamiliar with this requirement.

Registrar data synchronization

There are two methods available for registrars to synchronize their data with the registry:
• Automated synchronization: Registrars can, at any time, use the EPP 〈info〉 command to obtain definitive data from the registry for a known object, including domains, hosts (nameservers) and contacts.
• Personalized synchronization: A registrar may contact technical support and request a data file containing all domains (and associated host (nameserver) and contact information) registered by that registrar, within a specified time interval. The data will be formatted as a comma separated values (CSV) file and made available for download using a secure server.

EPP modifications

There are no unique EPP modifications planned for this TLD.

All ICANN TLDs must offer a Sunrise as part of a rights protection program. Afilias uses EPP extensions that allow registrars to submit trademark and other intellectual property rights (IPR) data to the registry. These extensions are:
• An 〈ipr:name〉 element that indicates the name of Registered Mark.
• An 〈ipr:number〉 element that indicates the registration number of the IPR.
• An 〈ipr:ccLocality〉 element that indicates the origin for which the IPR is established (a national or international trademark registry).
• An 〈ipr:entitlement〉 element that indicates whether the applicant holds the trademark as the original "OWNER", "CO-OWNER" or "ASSIGNEE".
• An 〈ipr:appDate〉 element that indicates the date the Registered Mark was applied for.
• An 〈ipr:regDate〉 element that indicates the date the Registered Mark was issued and registered.
• An 〈ipr:class〉 element that indicates the class of the registered mark.
• An 〈ipr:type〉 element that indicates the Sunrise phase the application applies for.

Note that some of these extensions might be subject to change based on ICANN-developed requirements for the Trademark Clearinghouse.

EPP resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused

way.

108 Afilias team members directly contribute to the management and development of the EPP based registry systems. As previously noted, Afilias is an active member of IETF and has a long documented history developing and enhancing EPP. These contributors include 11 developers and 14 QA engineers focused on maintaining and enhancing EPP server side software. These engineers work directly with business staff to timely address existing needs and forecast registry/registrar needs to ensure the Afilias EPP software is effective today and into the future. A team of eight data analysts work with the EPP software system to ensure that the data flowing through EPP is securely and reliably stored in replicated database systems. In addition to the EPP developers, QA engineers, and data analysts, other EPP contributors at Afilias include: Technical Analysts, the Network Operations Center and Data Services team members.

26. Whois

Answers for this question (#26) are provided by Afilias, the back-end provider of registry services for this TLD.

Afilias operates the WHOIS (registration data directory service) infrastructure in accordance with RFCs and global best practices, as it does for the 16 TLDs it currently supports. Designed to be robust and scalable, Afilias' WHOIS service has exceeded all contractual requirements for over a decade. It has extended search capabilities, and methods of limiting abuse.

The WHOIS service operated by Afilias meets and exceeds ICANN's requirements. Specifically, Afilias will:
• Offer a WHOIS service made available on port 43 that is flexible and standards- compliant;
• Comply with all ICANN policies, and meeting or exceeding WHOIS performance requirements in Specification 10 of the new gTLD Registry Agreement;
• Enable a Searchable WHOIS with extensive search capabilities that offers ease of use while enforcing measures to mitigate access abuse, and;
• Employ a team with significant experience managing a compliant WHOIS service.

Such extensive knowledge and experience managing a WHOIS service enables Afilias to offer a comprehensive plan for this TLD that meets the needs of constituents of the domain name industry and Internet users. The service has been tested by our QA team for RFC compliance, and has been used by registrars and many other parties for an extended period of time. Afilias' WHOIS service currently serves almost 500 million WHOIS queries per month, with the capacity already built in to handle an order of magnitude increase in WHOIS queries, and the ability to smoothly scale should greater growth be needed.

WHOIS system description and diagram

The Afilias WHOIS system, depicted in figure 26-a, is designed with robustness, availability, compliance, and performance in mind. Additionally, the system has provisions for detecting abusive usage (e.g., excessive numbers of queries from one source). The WHOIS system is generally intended as a publicly available single object lookup system. Afilias uses an advanced, persistent caching system to ensure extremely fast query response times.

Afilias will develop restricted WHOIS functions based on specific domain policy and regulatory requirements as needed for operating the business (as long as they are standards compliant). It will also be possible for contact and registrant information to be returned according to regulatory requirements. The WHOIS database supports multiple string and field searching through a reliable, free, secure web-based interface.

Data objects, interfaces, access and lookups
Registrars can provide an input form on their public websites through which a visitor is able to perform WHOIS queries. The registry operator can also provide a Web-based search on its

site. The input form must accept the string to query, along with the necessary input elements to select the object type and interpretation controls. This input form sends its data to the Afilias port 43 WHOIS server. The results from the WHOIS query are returned by the server and displayed in the visitor's Web browser. The sole purpose of the Web interface is to provide a user-friendly interface for WHOIS queries.

Afilias will provide WHOIS output as per Specification 4 of the new gTLD Registry Agreement. The output for domain records generally consists of the following elements:
• The name of the domain registered and the sponsoring registrar;
• The names of the primary and secondary nameserver(s) for the registered domain name;
• The creation date, registration status and expiration date of the registration;
• The name, postal address, e-mail address, and telephone and fax numbers of the domain name holder;
• The name, postal address, e-mail address, and telephone and fax numbers of the technical contact for the domain name holder;
• The name, postal address, e-mail address, and telephone and fax numbers of the administrative contact for the domain name holder, and;
• The name, postal address, e-mail address, and telephone and fax numbers of the billing contact for the domain name holder.
The following additional features are also present in Afilias' WHOIS service:
• Support for IDNs, including the language tag and the Punycode representation of the IDN in addition to Unicode Hex and Unicode HTML formats;
• Enhanced support for privacy protection relative to the display of confidential information.

Afilias will also provide sophisticated WHOIS search functionality that includes the ability to conduct multiple string and field searches.

Query controls
For all WHOIS queries, a user is required to enter the character string representing the information for which they want to search. The object type and interpretation control parameters to limit the search may also be specified. If object type or interpretation control parameter is not specified, WHOIS will search for the character string in the Name field of the Domain object.

WHOIS queries are required to be either an "exact search" or a "partial search," both of which are insensitive to the case of the input string.

An exact search specifies the full string to search for in the database field. An exact match between the input string and the field value is required.

A partial search specifies the start of the string to search for in the database field. Every record with a search field that starts with the input string is considered a match. By default, if multiple matches are found for a query, then a summary containing up to 50 matching results is presented. A second query is required to retrieve the specific details of one of the matching records.

If only a single match is found, then full details will be provided. Full detail consists of the data in the matching object as well as the data in any associated objects. For example: a query that results in a domain object includes the data from the associated host and contact objects.

WHOIS query controls fall into two categories: those that specify the type of field, and those that modify the interpretation of the input or determine the level of output to provide. Each is described below.

The following keywords restrict a search to a specific object type:
• Domain: Searches only domain objects. The input string is searched in the Name field.
• Host: Searches only nameserver objects. The input string is searched in the Name field and the IP Address field.
• Contact: Searches only contact objects. The input string is searched in the ID field.
• Registrar: Searches only registrar objects. The input string is searched in the Name field.
By default, if no object type control is specified, then the Name field of the Domain object is searched.

In addition, Afilias WHOIS systems can perform and respond to WHOIS searches by registrant name, postal address and contact names. Deployment of these features is provided as an option to the registry operator, based upon registry policy and business decision making.

Figure 26-b presents the keywords that modify the interpretation of the input or determine the level of output to provide.

By default, if no interpretation control keywords are used, the output will include full details if a single match is found and a summary if multiple matches are found.

Unique TLD requirements

There are no unique WHOIS requirements for this TLD.

Sunrise WHOIS processes

All ICANN TLDs must offer a Sunrise as part of a rights protection program. Afilias uses EPP extensions that allow registrars to submit trademark and other intellectual property rights (IPR) data to the registry. The following corresponding data will be displayed in WHOIS for relevant domains:

• Trademark Name: element that indicates the name of the Registered Mark.
• Trademark Number: element that indicates the registration number of the IPR.
• Trademark Locality: element that indicates the origin for which the IPR is established (a national or international trademark registry).
• Trademark Entitlement: element that indicates whether the applicant holds the trademark as the original “OWNER”, “CO-OWNER” or “ASSIGNEE”.
• Trademark Application Date: element that indicates the date the Registered Mark was applied for.
• Trademark Registration Date: element that indicates the date the Registered Mark was issued and registered.
• Trademark Class: element that indicates the class of the Registered Mark.
• IPR Type: element that indicates the Sunrise phase the application applies for.

IT and infrastructure resources

All the applications and databases for this TLD will run in a virtual environment hosted by a cluster of servers equipped with the latest Intel Westmere multi-core processors (or a more advanced, stable technology available at the time of deployment). The registry data will be stored on storage arrays of solid-state drives shared over a fast storage area network. The virtual environment allows the infrastructure to easily scale both vertically and horizontally to cater to changing demand. It also facilitates effective utilization of system resources thus reducing energy consumption and carbon footprint.

The applications and servers are supported by network firewalls, routers and switches. The WHOIS system accommodates both IPv4 and IPv6 addresses.

Each of the servers and network devices are equipped with redundant hot-swappable components and multiple connections to ancillary systems. Additionally, 24x7 support agreements with our hardware vendor with a 4-hour response time at all our data centers guarantees replacement of failed parts in the shortest time possible.

Models of system and network devices used are:

• Servers: Cisco UCS B230 blade servers
• SAN storage arrays: IBM Storwize V7000 with Solid State Drives
• Firewalls: Cisco ASA 5585-X
• Load balancers: F5 Big-IP 6900
• Traffic shapers: Procera PacketLogic PL8720
• Routers: Juniper MX40 3D
• Network switches: Cisco Nexus 7010, Nexus 5548, Nexus 2232

There will be at least four virtual machines (VMs) offering WHOIS service. Each VM will run at least two WHOIS server instances - one for registrars and one for the public. All instances of the WHOIS service is made available to registrars and the public are rate limited to mitigate abusive behavior.

Frequency of synchronization between servers

Registration data records from the EPP publisher database will be replicated to the WHOIS system database on a near-real-time basis whenever an update occurs.

Specifications 4 and 10 compliance

The WHOIS service for this TLD will meet or exceed the performance requirements in the new gTLD Registry Agreement, Specification 10. Figure 26-c provides the exact measurements and commitments. Afilias has a 10 year track record of exceeding WHOIS performance and a skilled team to ensure this continues for all TLDs under management.

The WHOIS service for this TLD will meet or exceed the requirements in the new gTLD Registry Agreement, Specification 4.

RFC 3912 compliance
Afilias will operate the WHOIS infrastructure in compliance with RFCs and global best practices, as it does with the 16 TLDs Afilias currently supports.

Afilias maintains a registry-level centralized WHOIS database that contains information for every registered domain and for all host and contact objects. The WHOIS service will be available on the Internet standard WHOIS port (port 43) in compliance with RFC 3912. The WHOIS service contains data submitted by registrars during the registration process. Changes made to the data by a registrant are submitted to Afilias by the registrar and are reflected in the WHOIS database and service in near-real-time, by the instance running at the primary data center, and in under ten seconds by the instance running at the secondary data center, thus providing all interested parties with up-to-date information for every domain. This service is compliant with the new gTLD Registry Agreement, Specification 4.

The WHOIS service maintained by Afilias will be authoritative and complete, as this will be a “thick” registry (detailed domain contact WHOIS is all held at the registry); users do not have to query different registrars for WHOIS information, as there is one central WHOIS system. Additionally, visibility of different types of data is configurable to meet the registry operator’s needs.

Searchable WHOIS

Afilias offers a searchable WHOIS on a web-based Directory Service. Partial match capabilities are offered on the following fields: domain name, registrar ID, and IP address. In addition, Afilias WHOIS systems can perform and respond to WHOIS searches by registrant name, postal address and contact names.

Providing the ability to search important and high-value fields such as registrant name, address and contact names increases the probability of abusive behavior. An abusive user could script a set of queries to the WHOIS service and access contact data in order to create or sell a list of names and addresses of registrants in this TLD. Making the WHOIS machine readable, while preventing harvesting and mining of WHOIS data, is a key requirement integrated into the Afilias WHOIS systems. For instance, Afilias limits search returns to 50 records at a time. If bulk queries were ever necessary (e.g., to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process), Afilias makes such query responses available to carefully screened and limited staff members at the registry operator (and customer support staff) via an internal data warehouse. The Afilias WHOIS system accommodates anonymous access as well as pre-identified and profile-defined uses, with full audit and log capabilities.

The WHOIS service has the ability to tag query responses with labels such as “Do not redistribute” or “Special access granted”. This may allow for tiered response and reply scenarios. Further, the WHOIS service is configurable in parameters and fields returned, which allow for flexibility in compliance with various jurisdictions, regulations or laws.

Afilias offers exact-match capabilities on the following fields: registrar ID, nameserver name, and nameserver's IP address (only applies to IP addresses stored by the registry, i.e., glue records). Search capabilities are fully available, and results include domain names matching the search criteria (including IDN variants). Afilias manages abuse prevention through rate limiting and CAPTCHA (described below). Queries do not require specialized transformations of internationalized domain names or internationalized data fields

Please see "Query Controls" above for details about search options and capabilities.

Deterring WHOIS abuse

Afilias has adopted two best practices to prevent abuse of the WHOIS service: rate limiting and CAPTCHA.

Abuse of WHOIS services on port 43 and via the Web is subject to an automated rate-limiting system. This ensures that uniformity of service to users is unaffected by a few parties whose activities abuse or otherwise might threaten to overload the WHOIS system.

Abuse of web-based public WHOIS services is subject to the use of CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) technology. The use of CAPTCHA ensures that uniformity of service to users is unaffected by a few parties whose activities abuse or otherwise might threaten to overload the WHOIS system. The registry operator will adopt a CAPTCHA on its Web-based WHOIS.

Data mining of any sort on the WHOIS system is strictly prohibited, and this prohibition is published in WHOIS output and in terms of service.

For rate limiting on IPv4, there are configurable limits per IP and subnet. For IPv6, the traditional limitations do not apply. Whenever a unique IPv6 IP address exceeds the limit of WHOIS queries per minute, the same rate-limit for the given 64 bits of network prefix that the offending IPv6 IP address falls into will be applied. At the same time, a timer will start and rate-limit validation logic will identify if there are any other IPv6 address within the original 80-bit(/48) prefix. If another offending IPv6 address does fall into the /48 prefix then rate-limit validation logic will penalize any other IPv6 addresses that fall into that given 80-bit (/48) network. As a security precaution, Afilias will not disclose these limits.

Pre-identified and profile-driven role access allows greater granularity and configurability in both access to the WHOIS service, and in volume/frequency of responses returned for queries.

Afilias staff are key participants in the ICANN Security & Stability Advisory Committee's deliberations and outputs on WHOIS, including SAC003, SAC027, SAC033, SAC037, SAC040, and SAC051. Afilias staff are active participants in both technical and policy decision making in ICANN, aimed at restricting abusive behavior.

WHOIS staff resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

Within Afilias, there are 11 staff members who develop and maintain the compliant WHOIS systems. They keep pace with access requirements, thwart abuse, and continually develop software. Of these resources, approximately two staffers are typically required for WHOIS-related code customization. Other resources provide quality assurance, and operations

personnel maintain the WHOIS system itself. This team will be responsible for the implementation and on-going maintenance of the new TLD WHOIS service.

27. Registration Life Cycle

Answers for this question (#27) are provided by Afilias, the back-end provider of registry services for this TLD.

THE RESPONSE FOR THIS QUESTION USES ANGLE BRACKETS (THE “〈” and “〉” CHARACTERS), WHICH ICANN INFORMS AFILIAS (CASE ID 11027) CANNOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE FULL ANSWER TO THIS QUESTION IS ATTACHED AS A PDF FILE.

Afilias has had experience managing registrations for over a decade and supports comprehensive registration lifecycle services including the registration states, all standard grace periods, and can address any modifications required with the introduction of any new ICANN policies.

This TLD will follow the ICANN standard domain lifecycle, as is currently implemented in TLDs such as .ORG and .INFO. The below response includes: a diagram and description of the lifecycle of a domain name in this TLD, including domain creation, transfer protocols, grace period implementation and the respective time frames for each; and the existing resources to support the complete lifecycle of a domain.

As depicted in Figure 27-a, prior to the beginning of the Trademark Claims Service or Sunrise IP protection program, Afilias will support the reservation of names in accordance with the new gTLD Registry Agreement, Specification 5.

Registration period

After the IP protection programs and the general launch, eligible registrants may choose an accredited registrar to register a domain name. The registrar will check availability on the requested domain name and if available, will collect specific objects such as, the required contact and host information from the registrant. The registrar will then provision the information into the registry system using standard Extensible Provisioning Protocol (“EPP”) commands through a secure connection to the registry backend service provider.

When the domain is created, the standard five day Add Grace Period begins, the domain and contact information are available in WHOIS, and normal operating EPP domain statuses will apply. Other specifics regarding registration rules for an active domain include:
• The domain must be unique;
• Restricted or reserved domains cannot be registered;
• The domain can be registered from 1-10 years;
• The domain can be renewed at any time for 1-10 years, but cannot exceed 10 years;
• The domain can be explicitly deleted at any time;
• The domain can be transferred from one registrar to another except during the first 60 days following a successful registration or within 60 days following a transfer; and,
Contacts and hosts can be modified at any time.

The following describe the domain status values recognized in WHOIS when using the EPP protocol following RFC 5731.
• OK or Active: This is the normal status for a domain that has no pending operations or restrictions.
• Inactive: The domain has no delegated name servers.
• Locked: No action can be taken on the domain. The domain cannot be renewed, transferred, updated, or deleted. No objects such as contacts or hosts can be associated to, or disassociated from the domain. This status includes: Delete Prohibited ⁄ Server Delete Prohibited, Update Prohibited ⁄ Server Update Prohibited, Transfer Prohibited, Server Transfer Prohibited, Renew Prohibited, Server Renew Prohibited.
• Hold: The domain will not be included in the zone. This status includes: Client Hold, Server Hold.

• Transfer Prohibited: The domain cannot be transferred away from the sponsoring registrar. This status includes: Client Transfer Prohibited, Server Transfer Prohibited.

The following describe the registration operations that apply to the domain name during the registration period.

a. Domain modifications: This operation allows for modifications or updates to the domain attributes to include:
i. Registrant Contact
ii. Admin Contact
iii. Technical Contact
iv. Billing Contact
v. Host or nameservers
vi. Authorization information
vii. Associated status values

A domain with the EPP status of Client Update Prohibited or Server Update Prohibited may not be modified until the status is removed.

b. Domain renewals: This operation extends the registration period of a domain by changing the expiration date. The following rules apply:
i. A domain can be renewed at any time during its registration term,
ii. The registration term cannot exceed a total of 10 years.

A domain with the EPP status of Client Renew Prohibited or Server Renew Prohibited cannot be renewed.

c. Domain deletions: This operation deletes the domain from the Shared Registry Services (SRS). The following rules apply:
i. A domain can be deleted at any time during its registration term, f the domain is deleted during the Add Grace Period or the Renew⁄Extend Grace Period, the sponsoring registrar will receive a credit,
ii. A domain cannot be deleted if it has “child” nameservers that are associated to other domains.

A domain with the EPP status of Client Delete Prohibited or Server Delete Prohibited cannot be deleted.

d. Domain transfers: A transfer of the domain from one registrar to another is conducted by following the steps below.
i. The registrant must obtain the applicable 〈authInfo〉 code from the sponsoring (losing) registrar.
• Every domain name has an authInfo code as per EPP RFC 5731. The authInfo code is a six- to 16-character code assigned by the registrar at the time the name was created. Its purpose is to aid identification of the domain owner so proper authority can be established (it is the "password" to the domain).
• Under the Registry-Registrar Agreement, registrars will be required to provide a copy of the authInfo code to the domain registrant upon his or her request.
ii. The registrant must provide the authInfo code to the new (gaining) registrar, who will then initiate a domain transfer request. A transfer cannot be initiated without the authInfo code.
• Every EPP 〈transfer〉 command must contain the authInfo code or the request will fail. The authInfo code represents authority to the registry to initiate a transfer.
iii. Upon receipt of a valid transfer request, the registry automatically asks the sponsoring (losing) registrar to approve the request within five calendar days.
• When a registry receives a transfer request the domain cannot be modified, renewed or deleted until the request has been processed. This status must not be combined with either Client Transfer Prohibited or Server Transfer Prohibited status.
• If the sponsoring (losing) registrar rejects the transfer within five days, the transfer request is cancelled. A new domain transfer request will be required to reinitiate the process.
• If the sponsoring (losing) registrar does not approve or reject the transfer within five days, the registry automatically approves the request.

iv. After a successful transfer, it is strongly recommended that registrars change the authInfo code, so that the prior registrar or registrant cannot use it anymore.
v. Registrars must retain all transaction identifiers and codes associated with successful domain object transfers and protect them from disclosure.
vi. Once a domain is successfully transferred the status of TRANSFERPERIOD is added to the domain for a period of five days.
vii. Successful transfers will result in a one year term extension (resulting in a maximum total of 10 years), which will be charged to the gaining registrar.

e. Bulk transfer: Afilias, supports bulk transfer functionality within the SRS for situations where ICANN may request the registry to perform a transfer of some or all registered objects (includes domain, contact and host objects) from one registrar to another registrar. Once a bulk transfer has been executed, expiry dates for all domain objects remain the same, and all relevant states of each object type are preserved. In some cases the gaining and the losing registrar as well as the registry must approved bulk transfers. A detailed log is captured for each bulk transfer process and is archived for audit purposes.

Schlund Technologies GmbH will support ICANN’s Transfer Dispute Resolution Process. Schlund Technologies GmbH will work with Afilias to respond to Requests for Enforcement (law enforcement or court orders) and will follow that process.

1. Auto-renew grace period
The Auto-Renew Grace Period displays as AUTORENEWPERIOD in WHOIS. An auto-renew must be requested by the registrant through the sponsoring registrar and occurs if a domain name registration is not explicitly renewed or deleted by the expiration date and is set to a maximum of 45 calendar days. In this circumstance the registration will be automatically renewed by the registry system the first day after the expiration date. If a Delete, Extend, or Transfer occurs within the AUTORENEWPERIOD the following rules apply:
i. Delete. If a domain is deleted the sponsoring registrar at the time of the deletion receives a credit for the auto-renew fee. The domain then moves into the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.
ii. Renew/Extend. A domain can be renewed as long as the total term does not exceed 10 years. The account of the sponsoring registrar at the time of the extension will be charged for the additional number of years the registration is renewed.
iii. Transfer (other than ICANN-approved bulk transfer). If a domain is transferred, the losing registrar is credited for the auto-renew fee, and the year added by the operation is cancelled. As a result of the transfer, the expiration date of the domain is extended by minimum of one year as long as the total term does not exceed 10 years. The gaining registrar is charged for the additional transfer year(s) even in cases where a full year is not added because of the maximum 10 year registration restriction.

2. Redemption grace period
During this period, a domain name is placed in the PENDING DELETE RESTORABLE status when a registrar requests the deletion of a domain that is not within the Add Grace Period. A domain can remain in this state for up to 30 days and will not be included in the zone file. The only action a registrar can take on a domain is to request that it be restored. Any other registrar requests to modify or otherwise update the domain will be rejected. If the domain is restored it moves into PENDING RESTORE and then OK. After 30 days if the domain is not restored it moves into PENDING DELETE SCHEDULED FOR RELEASE before the domain is released back into the pool of available domains.

3. Pending delete
During this period, a domain name is placed in PENDING DELETE SCHEDULED FOR RELEASE status for five days, and all Internet services associated with the domain will remain disabled and domain cannot be restored. After five days the domain is released back into the pool of available domains.

Other grace periods

All ICANN required grace periods will be implemented in the registry backend service provider’s system including the Add Grace Period (AGP), Renew/Extend Grace Period (EGP), Transfer Grace Period (TGP), Auto-Renew Grace Period (ARGP), and Redemption Grace Period

(RGP). The lengths of grace periods are configurable in the registry system. At this time, the grace periods will be implemented following other gTLDs such as .ORG. More than one of these grace periods may be in effect at any one time. The following are accompanying grace periods to the registration lifecycle.

Add grace period

The Add Grace Period displays as ADDPERIOD in WHOIS and is set to five calendar days following the initial registration of a domain. If the domain is deleted by the registrar during this period, the registry provides a credit to the registrar for the cost of the registration. If a Delete, Renew/Extend, or Transfer operation occurs within the five calendar days, the following rules apply.

i. Delete. If a domain is deleted within this period the sponsoring registrar at the time of the deletion is credited for the amount of the registration. The domain is deleted from the registry backend service provider's database and is released back into the pool of available domains.

ii. Renew/Extend. If the domain is renewed within this period and then deleted, the sponsoring registrar will receive a credit for both the registration and the extended amounts. The account of the sponsoring registrar at the time of the renewal will be charged for the initial registration plus the number of years the registration is extended. The expiration date of the domain registration is extended by that number of years as long as the total term does not exceed 10 years.

iii. Transfer (other than ICANN-approved bulk transfer). Transfers under Part A of the ICANN Policy on Transfer of Registrations between registrars may not occur during the ADDPERIOD or at any other time within the first 60 days after the initial registration. Enforcement is the responsibility of the registrar sponsoring the domain name registration and is enforced by the SRS.

Renew / extend grace period

The Renew / Extend Grace Period displays as RENEWPERIOD in WHOIS and is set to five calendar days following an explicit renewal on the domain by the registrar. If a Delete, Extend, or Transfer occurs within the five calendar days, the following rules apply:

i. Delete. If a domain is deleted within this period the sponsoring registrar at the time of the deletion receives a credit for the renewal fee. The domain then moves into the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.

ii. Renew/Extend. A domain registration can be renewed within this period as long as the total term does not exceed 10 years. The account of the sponsoring registrar at the time of the extension will be charged for the additional number of years the registration is renewed.

iii. Transfer (other than ICANN-approved bulk transfer). If a domain is transferred within the Renew/Extend Grace Period, there is no credit to the losing registrar for the renewal fee. As a result of the transfer, the expiration date of the domain registration is extended by a minimum of one year as long as the total term for the domain does not exceed 10 years.

If a domain is auto-renewed, then extended, and then deleted within the Renew/Extend Grace Period, the registrar will be credited for any auto-renew fee charged and the number of years for the extension. The years that were added to the domain's expiration as a result of the auto-renewal and extension are removed. The deleted domain is moved to the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.

Transfer Grace Period

The Transfer Grace period displays as TRANSFERPERIOD in WHOIS and is set to five calendar days after the successful transfer of domain name registration from one registrar to another registrar. Transfers under Part A of the ICANN Policy on Transfer of Registrations between registrars may not occur during the TRANSFERPERIOD or within the first 60 days after the transfer. If a Delete or Renew/Extend occurs within that five calendar days, the following rules apply:

i. Delete. If the domain is deleted by the new sponsoring registrar during this period, the registry provides a credit to the registrar for the cost of the transfer. The domain then moves into the Redemption Grace Period with a status of PENDING DELETE RESTORABLE.

ii. Renew/Extend. If a domain registration is renewed within the Transfer Grace Period, there is no credit for the transfer. The registrar's account will be charged for the number of years the registration is renewed. The expiration date of the domain registration is extended by the

renewal years as long as the total term does not exceed 10 years.

Auction

This TLD will conduct an auction for certain domain names. Afilias will manage the domain name auction using existing technology. Upon the completion of the auction, any domain name acquired will then follow the standard lifecycle of a domain.

Registration lifecycle resources

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way. Virtually all Afilias resource are involved in the registration lifecycle of domains.

There are a few areas where registry staff devote resources to registration lifecycle issues:
a. Supporting Registrar Transfer Disputes. The registry operator will have a compliance staffer handle these disputes as they arise; they are very rare in the existing gTLDs.
b. Afilias has its development and quality assurance departments on hand to modify the grace period functionality as needed, if ICANN issues new Consensus Policies or the RFCs change.

Afilias has more than 30 staff members in these departments.

28. Abuse Prevention and Mitigation

Schlund Technologies GmbH, working with Afilias, will take the requisite operational and technical steps to promote WHOIS data accuracy, limit domain abuse, remove outdated and inaccurate data, and other security measures to ensure the integrity of the TLD. The specific measures include, but are not limited to:
• Posting a TLD Anti-Abuse Policy that clearly defines abuse, and provide point-of-contact information for reporting suspected abuse;
• Committing to rapid identification and resolution of abuse, including suspensions;
• Ensuring completeness of WHOIS information at the time of registration;
• Publishing and maintaining procedures for removing orphan glue records for names removed from the zone, and;
• Establishing measures to deter WHOIS abuse, including rate-limiting, determining data syntax validity, and implementing and enforcing requirements from the Registry-Registrar Agreement.

Abuse policy

The Anti-Abuse Policy stated below will be enacted under the contractual authority of the registry operator through the Registry-Registrar Agreement, and the obligations will be passed on to and made binding upon registrants. This policy will be posted on the TLD web site along with contact information for registrants or users to report suspected abuse.

The policy is designed to address the malicious use of domain names. The registry operator and its registrars will make reasonable attempts to limit significant harm to Internet users. This policy is not intended to take the place of the Uniform Domain Name Dispute Resolution Policy (UDRP) or the Uniform Rapid Suspension System (URS), and it is not to be used as an alternate form of dispute resolution or as a brand protection mechanism. Its intent is not to burden law-abiding or innocent registrants and domain users; rather, the intent is to deter those who use domain names maliciously by engaging in illegal or fraudulent activity.

Repeat violations of the abuse policy will result in a case-by-case review of the abuser(s), and the registry operator reserves the right to escalate the issue, with the intent of levying sanctions that are allowed under the TLD anti-abuse policy.

The below policy is a recent version of the policy that has been used by the .INFO registry since 2008, and the .ORG registry since 2009. It has proven to be an effective and flexible tool.

.WEB Anti-Abuse Policy

The following Anti-Abuse Policy is effective upon launch of the TLD. Malicious use of domain names will not be tolerated. The nature of such abuses creates security and stability issues for the registry, registrars, and registrants, as well as for users of the Internet in general. The registry operator definition of abusive use of a domain includes, without limitation, the following:

• Illegal or fraudulent actions;
• Spam: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to email spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of web sites and Internet forums;
• Phishing: The use of counterfeit web pages that are designed to trick recipients into divulging sensitive data such as personally identifying information, usernames, passwords, or financial data;
• Pharming: The redirecting of unknowing users to fraudulent sites or services, typically through, but not limited to, DNS hijacking or poisoning;
• Willful distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include, without limitation, computer viruses, worms, keyloggers, and Trojan horses.
• Malicious fast-flux hosting: Use of fast-flux techniques with a botnet to disguise the location of web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities.
• Botnet command and control: Services run on a domain name that are used to control a collection of compromised computers or "zombies," or to direct distributed denial-of-service attacks (DDoS attacks);
• Illegal Access to Other Computers or Networks: Illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).

Pursuant to the Registry-Registrar Agreement, registry operator reserves the right at its sole discretion to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status, that it deems necessary: (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of registry operator, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement and this Anti-Abuse Policy, or (5) to correct mistakes made by registry operator or any registrar in connection with a domain name registration. Registry operator also reserves the right to place upon registry lock, hold, or similar status a domain name during resolution of a dispute.

The policy stated above will be accompanied by notes about how to submit a report to the registry operator's abuse point of contact, and how to report an orphan glue record suspected of being used in connection with malicious conduct (see below).

Abuse point of contact and procedures for handling abuse complaints

The registry operator will establish an abuse point of contact. This contact will be a role-based e-mail address of the form "abuse@registry.WEB". This e-mail address will allow multiple staff members to monitor abuse reports on a 24x7 basis, and then work toward closure of cases as each situation calls for. For tracking purposes, the registry operator will have a ticketing system with which all complaints will be tracked internally. The reporter will be

provided with the ticket reference identifier for potential follow-up. Afilias will integrate its existing ticketing system with the registry operator's to ensure uniform tracking and handling of the complaint. This role-based approach has been used successfully by ISPs, e-mail service providers, and registrars for many years, and is considered a global best practice.

The registry operator's designated abuse handlers will then evaluate complaints received via the abuse system address. They will decide whether a particular issue is of concern, and decide what action, if any, is appropriate.

In general, the registry operator will find itself receiving abuse reports from a wide variety of parties, including security researchers and Internet security companies, financial institutions such as banks, Internet users, and law enforcement agencies among others. Some of these parties may provide good forensic data or supporting evidence of the malicious behavior. In other cases, the party reporting an issue may not be familiar with how to provide such data or proof of malicious behavior. It is expected that a percentage of abuse reports to the registry operator will not be actionable, because there will not be enough evidence to support the complaint (even after investigation), and because some reports or reporters will simply not be credible.

The security function includes a communication and outreach function, with information sharing with industry partners regarding malicious or abusive behavior, in order to ensure coordinated abuse mitigation across multiple TLDs.

Assessing abuse reports requires great care, and the registry operator will rely upon professional, trained investigators who are versed in such matters. The goals are accuracy, good record-keeping, and a zero false-positive rate so as not to harm innocent registrants.

Different types of malicious activities require different methods of investigation and documentation. Further, the registry operator expects to face unexpected or complex situations that call for professional advice, and will rely upon professional, trained investigators as needed.

In general, there are two types of domain abuse that must be addressed:
a) Compromised domains. These domains have been hacked or otherwise compromised by criminals, and the registrant is not responsible for the malicious activity taking place on the domain. For example, the majority of domain names that host phishing sites are compromised. The goal in such cases is to get word to the registrant (usually via the registrar) that there is a problem that needs attention with the expectation that the registrant will address the problem in a timely manner. Ideally such domains do not get suspended, since suspension would disrupt legitimate activity on the domain.
b) Malicious registrations. These domains are registered by malefactors for the purpose of abuse. Such domains are generally targets for suspension, since they have no legitimate use.

The standard procedure is that the registry operator will forward a credible alleged case of malicious domain name use to the domain's sponsoring registrar with a request that the registrar investigate the case and act appropriately. The registrar will be provided evidence collected as a result of the investigation conducted by the trained abuse handlers. As part of the investigation, if inaccurate or false WHOIS registrant information is detected, the registrar is notified about this. The registrar is the party with a direct relationship with—and a direct contract with—the registrant. The registrar will also have vital information that the registry operator will not, such as:
• Details about the domain purchase, such as the payment method used (credit card, PayPal, etc.);
• The identity of a proxy-protected registrant;
• The purchaser's IP address;
• Whether there is a reseller involved, and;
• The registrant's past sales history and purchases in other TLDs (insofar as the registrar can determine this).

Registrars do not share the above information with registry operators due to privacy and liability concerns, among others. Because they have more information with which to continue the investigation, and because they have a direct relationship with the registrant, the registrar is in the best position to evaluate alleged abuse. The registrar can determine if

the use violates the registrar's legal terms of service or the registry Anti-Abuse Policy, and can decide whether or not to take any action. While the language and terms vary, registrars will be expected to include language in their registrar-registrant contracts that indemnifies the registrar if it takes action, and allows the registrar to suspend or cancel a domain name; this will be in addition to the registry Anti-Abuse Policy. Generally, registrars can act if the registrant violates the registrar's terms of service, or violates ICANN policy, or if illegal activity is involved, or if the use violates the registry's Anti-Abuse Policy.

If a registrar does not take action within a time period indicated by the registry operator (usually 24 hours), the registry operator might then decide to take action itself. At all times, the registry operator reserves the right to act directly and immediately if the potential harm to Internet users seems significant or imminent, with or without notice to the sponsoring registrar.

The registry operator will be prepared to call upon relevant law enforcement bodies as needed. There are certain cases, for example, Illegal pharmacy domains, where the registry operator will contact the Law Enforcement Agencies to share information about these domains, provide all the evidence collected and work closely with them before any action will be taken for suspension. The specific action is often dependent upon the jurisdiction of which the registry operator, although the operator in all cases will adhere to applicable laws and regulations.

When valid court orders or seizure warrants are received from courts or law enforcement agencies of relevant jurisdiction, the registry operator will order execution in an expedited fashion. Compliance with these will be a top priority and will be completed as soon as possible and within the defined timelines of the order. There are certain cases where Law Enforcement Agencies request information about a domain including but not limited to:
• Registration information
• History of a domain, including recent updates made
• Other domains associated with a registrant's account
• Patterns of registrant portfolio

Requests for such information is handled on a priority basis and sent back to the requestor as soon as possible. Afilias sets a goal to respond to such requests within 24 hours.

The registry operator may also engage in proactive screening of its zone for malicious use of the domains in the TLD, and report problems to the sponsoring registrars. The registry operator could take advantage of a combination of the following resources, among others:
• Blocklists of domain names and nameservers published by organizations such as SURBL and Spamhaus.
• Anti-phishing feeds, which will provide URLs of compromised and maliciously registered domains being used for phishing.
• Analysis of registration or DNS query data [DNS query data received by the TLD nameservers.]

The registry operator will keep records and track metrics regarding abuse and abuse reports. These will include:
• Number of abuse reports received by the registry's abuse point of contact described above;
• Number of cases and domains referred to registrars for resolution;
• Number of cases and domains where the registry took direct action;
• Resolution times;
• Number of domains in the TLD that have been blacklisted by major anti-spam blocklist providers, and;
• Phishing site uptimes in the TLD.

Removal of orphan glue records

By definition, orphan glue records used to be glue records. Glue records are related to delegations and are necessary to guide iterative resolvers to delegated nameservers. A glue record becomes an orphan when its parent nameserver record is removed without also removing the corresponding glue record. (Please reference the ICANN SSAC paper SAC048 at: http://www.icann.org/en/committees/security/sac048.pdf.) Orphan glue records may be created when a domain (example.tld) is placed on EPP ServerHold or ClientHold status. When placed on Hold, the domain is removed from the zone and will stop resolving. However, any child

nameservers (now orphan glue) of that domain (e.g., ns1.example.tld) are left in the zone. It is important to keep these orphan glue records in the zone so that any innocent sites using that nameserver will continue to resolve. This use of Hold status is an essential tool for suspending malicious domains.

Afilias observes the following procedures, which are being followed by other registries and are generally accepted as DNS best practices. These procedures are also in keeping with ICANN SSAC recommendations.

When a request to delete a domain is received from a registrar, the registry first checks for the existence of glue records. If glue records exist, the registry will check to see if other domains in the registry are using the glue records. If other domains in the registry are using the glue records then the request to delete the domain will fail until no other domains are using the glue records. If no other domains in the registry are using the glue records then the glue records will be removed before the request to delete the domain is satisfied. If no glue records exist then the request to delete the domain will be satisfied.

If a registrar cannot delete a domain because of the existence of glue records that are being used by other domains, then the registrar may refer to the zone file or the “weekly domain hosted by nameserver report” to find out which domains are using the nameserver in question and attempt to contact the corresponding registrar to request that they stop using the nameserver in the glue record. The registry operator does not plan on performing mass updates of the associated DNS records.

The registry operator will accept, evaluate, and respond appropriately to complaints that orphan glue is being used maliciously. Such reports should be made in writing to the registry operator, and may be submitted to the registry’s abuse point-of-contact. If it is confirmed that an orphan glue record is being used in connection with malicious conduct, the registry operator will have the orphan glue record removed from the zone file. Afilias has the technical ability to execute such requests as needed.

Methods to promote WHOIS accuracy

The creation and maintenance of accurate WHOIS records is an important part of registry management. As described in our response to question #26, WHOIS, the registry operator will manage a secure, robust and searchable WHOIS service for this TLD.

WHOIS data accuracy

The registry operator will offer a “thick” registry system. In this model, all key contact details for each domain name will be stored in a central location by the registry. This allows better access to domain data, and provides uniformity in storing the information. The registry operator will ensure that the required fields for WHOIS data (as per the defined policies for the TLD) are enforced at the registry level. This ensures that the registrars are providing required domain registration data. Fields defined by the registry policy to be mandatory are documented as such and must be submitted by registrars. The Afilias registry system verifies formats for relevant individual data fields (e.g. e-mail, and phone/fax numbers). Only valid country codes are allowed as defined by the ISO 3166 code list. The Afilias WHOIS system is extensible, and is capable of using the VAULT system, described further below.

Similar to the centralized abuse point of contact described above, the registry operator can institute a contact email address which could be utilized by third parties to submit complaints for inaccurate or false WHOIS data detected. This information will be processed by Afilias’ support department and forwarded to the registrars. The registrars can work with the registrants of those domains to address these complaints. Afilias will audit registrars on a yearly basis to verify whether the complaints being forwarded are being addressed or not. This functionality, available to all registry operators, is activated based on the registry operator’s business policy.

Afilias also incorporates a spot-check verification system where a randomly selected set of domain names are checked periodically for accuracy of WHOIS data. Afilias’ .PRO registry system incorporates such a verification system whereby 1% of total registrations or 100 domains, whichever number is larger, are spot-checked every month to verify the domain name

registrant's critical information provided with the domain registration data. With both a highly qualified corps of engineers and a 24x7 staffed support function, Afilias has the capacity to integrate such spot-check functionality into this TLD, based on the registry operator's business policy. Note: This functionality will not work for proxy protected WHOIS information, where registrars or their resellers have the actual registrant data. The solution to that problem lies with either registry or registrar policy, or a change in the general marketplace practices with respect to proxy registrations.

Finally, Afilias' registry systems have a sophisticated set of billing and pricing functionality which aids registry operators who decide to provide a set of financial incentives to registrars for maintaining or improving WHOIS accuracy. For instance, it is conceivable that the registry operator may decide to provide a discount for the domain registration or renewal fees for validated registrants, or levy a larger cost for the domain registration or renewal of proxy domain names. The Afilias system has the capability to support such incentives on a configurable basis, towards the goal of promoting better WHOIS accuracy.

Role of registrars

As part of the RRA (Registry Registrar Agreement), the registry operator will require the registrar to be responsible for ensuring the input of accurate WHOIS data by their registrants. The Registrar⁄Registered Name Holder Agreement will include a specific clause to ensure accuracy of WHOIS data, and to give the registrar rights to cancel or suspend registrations if the Registered Name Holder fails to respond to the registrar's query regarding accuracy of data. ICANN's WHOIS Data Problem Reporting System (WDPRS) will be available to those who wish to file WHOIS inaccuracy reports, as per ICANN policy (http:⁄⁄wdprs.internic.net⁄).

Controls to ensure proper access to domain functions

Several measures are in place in the Afilias registry system to ensure proper access to domain functions, including authentication provisions in the RRA relative to notification and contact updates via use of AUTH-INFO codes.

IP address access control lists, TLS⁄SSL certificates and proper authentication are used to control access to the registry system. Registrars are only given access to perform operations on the objects they sponsor.

Every domain will have a unique AUTH-INFO code. The AUTH-INFO code is a 6- to 16-character code assigned by the registrar at the time the name is created. Its purpose is to aid identification of the domain owner so proper authority can be established. It is the "password" to the domain name. Registrars must use the domain's password in order to initiate a registrar-to-registrar transfer. It is used to ensure that domain updates (update contact information, transfer, or deletion) are undertaken by the proper registrant, and that this registrant is adequately notified of domain update activity. Only the sponsoring registrar of a domain has access to the domain's AUTH-INFO code stored in the registry, and this is accessible only via encrypted, password-protected channels.

Information about other registry security measures such as encryption and security of registrar channels are confidential to ensure the security of the registry system. The details can be found in the response to question #30b.

Validation and abuse mitigation mechanisms

Afilias has developed advanced validation and abuse mitigation mechanisms. These capabilities and mechanisms are described below. These services and capabilities are discretionary and may be utilized by the registry operator based on their policy and business need.

Afilias has the ability to analyze the registration data for known patterns at the time of registration. A database of these known patterns is developed from domains and other associated objects (e.g., contact information) which have been previously detected and suspended after being flagged as abusive. Any domains matching the defined criteria can be

flagged for investigation. Once analyzed and confirmed by the domain anti-abuse team members, these domains may be suspended. This provides proactive detection of abusive domains.

Provisions are available to enable the registry operator to only allow registrations by pre-authorized and verified contacts. These verified contacts are given a unique code that can be used for registration of new domains.

Registrant pre-verification and authentication

One of the systems that could be used for validity and identity authentication is VAULT (Validation and Authentication Universal Lookup). It utilizes information obtained from a series of trusted data sources with access to billions of records containing data about individuals for the purpose of providing independent age and id verification as well as the ability to incorporate additional public or private data sources as required. At present it has the following: US Residential Coverage - 90% of Adult Population and also International Coverage - Varies from Country to Country with a minimum of 80% coverage (24 countries, mostly European).

Various verification elements can be used. Examples might include applicant data such as name, address, phone, etc. Multiple methods could be used for verification include integrated solutions utilizing API (XML Application Programming Interface) or sending batches of requests.

• Verification and Authentication requirements would be based on TLD operator requirements or specific criteria.
• Based on required WHOIS Data; registrant contact details (name, address, phone)
• If address/ZIP can be validated by VAULT, the validation process can continue (North America +25 International countries)
• If in-line processing and registration and EPP/API call would go to the verification clearinghouse and return up to 4 challenge questions.
• If two-step registration is required, then registrants would get a link to complete the verification at a separate time. The link could be specific to a domain registration and pre-populated with data about the registrant.
• If WHOIS data is validated a token would be generated and could be given back to the registrar which registered the domain.
• WHOIS data would reflect the Validated Data or some subset, i.e., fields displayed could be first initial and last name, country of registrant and date validated. Other fields could be generic validation fields much like a “privacy service”.
• A “Validation Icon” customized script would be sent to the registrants email address. This could be displayed on the website and would be dynamically generated to avoid unauthorized use of the Icon. When clicked on the Icon would show limited WHOIS details i.e. Registrant: jdoe, Country: USA, Date Validated: March 29, 2011, as well as legal disclaimers.
• Validation would be annually renewed, and validation date displayed in the WHOIS.

Abuse prevention resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way. Abuse prevention and detection is a function that is staffed across the various groups inside Afilias, and requires a team effort when abuse is either well hidden or widespread, or both. While all of Afilias’ 200+ employees are charged with responsibility to report any detected abuse, the engineering and analysis teams, numbering over 30, provide specific support based on the type of abuse and volume and frequency of analysis required. The Afilias security and support teams have the authority to initiate mitigation.

Afilias has developed advanced validation and abuse mitigation mechanisms. These capabilities and mechanisms are described below. These services and capabilities are discretionary and may be utilized by the registry operator based on their policy and business need.

This TLD's anticipated volume of registrations in the first three years of operations is listed in response #46. Afilias and the registry operator's anti-abuse function anticipates the expected volume and type of registrations, and together will adequately cover the staffing needs for this TLD. The registry operator will maintain an abuse response team, which may be a combination of internal staff and outside specialty contractors, adjusting to the needs of the size and type of TLD. The team structure planned for this TLD is based on several years of experience responding to, mitigating, and managing abuse for TLDs of various sizes. The team will generally consist of abuse handlers (probably internal), a junior analyst, (either internal or external), and a senior security consultant (likely an external resource providing the registry operator with extra expertise as needed). These responders will be specially trained in the investigation of abuse complaints, and will have the latitude to act expeditiously to suspend domain names (or apply other remedies) when called for.

The exact resources required to maintain an abuse response team must change with the size and registration procedures of the TLD. An initial abuse handler is necessary as a point of contact for reports, even if a part-time responsibility. The abuse handlers monitor the abuse email address for complaints and evaluate incoming reports from a variety of sources. A large percentage of abuse reports to the registry operator may be unsolicited commercial email. The designated abuse handlers can identify legitimate reports and then decide what action is appropriate, either to act upon them, escalate to a security analyst for closer investigation, or refer them to registrars as per the above-described procedures. A TLD with rare cases of abuse would conform to this structure.

If multiple cases of abuse within the same week occur regularly, the registry operator will consider staffing internally a security analyst to investigate the complaints as they become more frequent. Training an abuse analyst requires 3-6 months and likely requires the active guidance of an experienced senior security analyst for guidance and verification of assessments and recommendations being made.

If this TLD were to regularly experience multiple cases of abuse within the same day, a full-time senior security analyst would likely be necessary. A senior security analyst capable of fulfilling this role should have several years of experience and able to manage and train the internal abuse response team.

The abuse response team will also maintain subscriptions for several security information services, including the blocklists from organizations like SURBL and Spamhaus and anti-phishing and other domain related abuse (malware, fast-flux etc.) feeds. The pricing structure of these services may depend on the size of the domain and some services will include a number of rapid suspension requests for use as needed.

For a large TLD, regular audits of the registry data are required to maintain control over abusive registrations. When a registrar with a significant number of registrations has been compromised or acted maliciously, the registry operator may need to analyze a set of registration or DNS query data. A scan of all the domains of a registrar is conducted only as needed. Scanning and analysis for a large registrar may require as much as a week of full-time effort for a dedicated machine and team.

29. Rights Protection Mechanisms

Rights protection is a core responsibility of the TLD operator, and is supported by a fully-developed plan for rights protection that includes:
• Establishing mechanisms to prevent unqualified registrations (e.g., registrations made in violation of the registry's eligibility restrictions or policies);
• Implementing a robust Sunrise program, utilizing the Trademark Clearinghouse, the services of one of ICANN's approved dispute resolution providers, a trademark validation agent, and drawing upon sunrise policies and rules used successfully in previous gTLD launches;

• Implementing a professional trademark claims program that utilizes the Trademark Clearinghouse, and drawing upon models of similar programs used successfully in previous TLD launches;
• Complying with the URS requirements;
• Complying with the UDRP;
• Complying with the PDDRP, and;
• Including all ICANN-mandated and independently developed rights protection mechanisms ("RPMs") in the registry-registrar agreement entered into by ICANN-accredited registrars authorized to register names in the TLD.

The response below details the rights protection mechanisms at the launch of the TLD (Sunrise and Trademark Claims Service) which comply with rights protection policies (URS, UDRP, PDDRP, and other ICANN RPMs), outlines additional provisions made for rights protection, and provides the resourcing plans.

Safeguards for rights protection at the launch of the TLD

The launch of this TLD will include the operation of a trademark claims service according to the defined ICANN processes for checking a registration request and alerting trademark holders of potential rights infringement.

The Sunrise Period will be an exclusive period of time, prior to the opening of public registration, when trademark and service mark holders will be able to reserve marks that are an identical match in the .WEB domain. Following the Sunrise Period, Schlund Technologies GmbH will open registration to qualified applicants.

The anticipated Rollout Schedule for the Sunrise Period will be approximately as follows:
• Launch of the TLD – Sunrise Period begins for trademark holders and service mark holders to submit registrations for their exact marks in the .WEB domain.
• Quiet Period – The Sunrise Period will close and will be followed by a Quiet Period for testing and evaluation.
• One month after close of Quiet Period – Registration in the .WEB domain will be opened to qualified applicants.

Sunrise Period Requirements & Restrictions

Those wishing to reserve their marks in the .WEB domain during the Sunrise Period must own a current trademark or service mark listed in the Trademark Clearinghouse.

Notice will be provided to all trademark holders in the Clearinghouse if someone is seeking a Sunrise registration. This notice will be provided to holders of marks in the Clearinghouse that are an Identical Match (as defined in the Trademark Clearing House) to the name to be registered during Sunrise.

Each Sunrise registration will require a minimum term, to be determined at a later date.

Schlund Technologies GmbH will establish the following Sunrise eligibility requirements (SERs) as minimum requirements, verified by Clearinghouse data, and incorporate a Sunrise Dispute Resolution Policy (SDRP). The SERs include: (i) ownership of a mark that satisfies the criteria set forth in section 7.2 of the Trademark Clearing House specifications, (ii) description of international class of goods or services covered by registration; (iii) representation that all provided information is true and correct; and (iv) provision of data sufficient to document rights in the trademark.

The SDRP will allow challenges based on the following four grounds: (i) at time the challenged domain name was registered, the registrants did not hold a trademark registration of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty; (ii) the domain name is not identical to the mark on which the registrant based its Sunrise registration; (iii) the trademark registration on which the registrant based its Sunrise registration is not of national effect (or regional effect) or the trademark had not been court-validated or protected by statute or treaty; or (iv) the trademark registration

on which the domain name registrant based its Sunrise registration did not issue on or before the effective date of the Registry Agreement and was not applied for on or before ICANN announced the applications received.

Ongoing rights protection mechanisms

Several mechanisms will be in place to protect rights in this TLD. As described in our responses to questions #27 and #28, measures are in place to ensure domain transfers and updates are only initiated by the appropriate domain holder, and an experienced team is available to respond to legal actions by law enforcement or court orders.

This TLD will conform to all ICANN RPMs including URS (defined below), UDRP, PDDRP, and all measures defined in Specification 7 of the new TLD agreement.

Uniform Rapid Suspension (URS)

Schlund Technologies GmbH will implement decisions rendered under the URS on an ongoing basis. Per the URS policy posted on ICANN's Web site as of this writing, the registry operator will receive notice of URS actions from the ICANN-approved URS providers. These emails will be directed immediately to the registry operator's support staff, which is on duty 24x7. The support staff will be responsible for creating a ticket for each case, and for executing the directives from the URS provider. All support staff will receive pertinent training.

As per ICANN's URS guidelines, within 24 hours of receipt of the notice of complaint from the URS provider, the registry operator shall "lock" the domain, meaning the registry shall restrict all changes to the registration data, including transfer and deletion of the domain names, but the name will remain in the TLD DNS zone file and will thus continue to resolve. The support staff will "lock" the domain by associating the following EPP statuses with the domain and relevant contact objects:

- ServerUpdateProhibited, with an EPP reason code of "URS"
- ServerDeleteProhibited, with an EPP reason code of "URS"
- ServerTransferProhibited, with an EPP reason code of "URS"
- The registry operator's support staff will then notify the URS provider immediately upon locking the domain name, via email.

The registry operator's support staff will retain all copies of emails from the URS providers, assign them a tracking or ticket number, and will track the status of each opened URS case through to resolution via spreadsheet or database.

The registry operator's support staff will execute further operations upon notice from the URS providers. The URS provider is required to specify the remedy and required actions of the registry operator, with notification to the registrant, the complainant, and the registrar.

As per the URS guidelines, if the complainant prevails, the registry operator shall suspend the domain name, which shall remain suspended for the balance of the registration period and would not resolve to the original web site. The nameservers shall be redirected to an informational web page provided by the URS provider about the URS. The WHOIS for the domain name shall continue to display all of the information of the original registrant except for the redirection of the nameservers. In addition, the WHOIS shall reflect that the domain name will not be able to be transferred, deleted or modified for the life of the registration."

Rights protection via the RRA

The following will be memorialized and be made binding via the Registry-Registrar and Registrar-Registrant Agreements:

- The registry may reject a registration request or a reservation request, or may delete, revoke, suspend, cancel, or transfer a registration or reservation under the following criteria:

a. to enforce registry policies and ICANN requirements; each as amended from time to time;
b. that is not accompanied by complete and accurate information as required by ICANN requirements and/or registry policies or where required information is not updated and/or corrected as required by ICANN requirements and/or registry policies;
c. to protect the integrity and stability of the registry, its operations, and the TLD system;

d. to comply with any applicable law, regulation, holding, order, or decision issued by a court, administrative authority, or dispute resolution service provider with jurisdiction over the registry;
e. to establish, assert, or defend the legal rights of the registry or a third party or to avoid any civil or criminal liability on the part of the registry and/or its affiliates, subsidiaries, officers, directors, representatives, employees, contractors, and stockholders;
f. to correct mistakes made by the registry or any accredited registrar in connection with a registration; or
g. as otherwise provided in the Registry-Registrar Agreement and/or the Registrar-Registrant Agreement.

Reducing opportunities for behaviors such as phishing or pharming

In our response to question #28, Schlund Technologies GmbH has described its anti-abuse program. Rather than repeating the policies and procedures here, please see our response to question #28 for full details.

In the case of this TLD, Schlund Technologies GmbH will apply an approach that addresses registered domain names (rather than potentially registered domains). This approach will not infringe upon the rights of eligible registrants to register domains, and allows Schlund Technologies GmbH internal controls, as well as community-developed UDRP and URS policies and procedures if needed, to deal with complaints, should there be any.

Afilias is a member of various security fora which provide access to lists of names in each TLD which may be used for malicious purposes. Such identified names will be subject to the TLD anti-abuse policy, including rapid suspensions after due process.

Rights protection resourcing plans

Since its founding, Afilias is focused on delivering secure, stable and reliable registry services. Several essential management and staff who designed and launched the Afilias registry in 2001 and expanded the number of TLDs supported, all while maintaining strict service levels over the past decade, are still in place today. This experiential continuity will endure for the implementation and on-going maintenance of this TLD. Afilias operates in a matrix structure, which allows its staff to be allocated to various critical functions in both a dedicated and a shared manner. With a team of specialists and generalists, the Afilias project management methodology allows efficient and effective use of our staff in a focused way.

Supporting RPMs requires several departments within the registry operator as well as within Afilias. The implementation of Sunrise and the Trademark Claims service and on-going RPM activities will pull from the 102 Afilias staff members of the engineering, product management, development, security and policy teams at Afilias, which is on duty 24x7, and the support staff of the registry operator. A trademark validator will also be assigned within the registry operator, whose responsibilities may require as much as 50% of full-time employment if the domains under management were to exceed several million. No additional hardware or software resources are required to support this as Afilias has fully-operational capabilities to manage abuse today.

30(a). Security Policy: Summary of the security policy for the proposed registry

The answer to question #30a is provided by Afilias, the back-end provider of registry services for this TLD.

Afilias aggressively and actively protects the registry system from known threats and vulnerabilities, and has deployed an extensive set of security protocols, policies and procedures to thwart compromise. Afilias' robust and detailed plans are continually updated and tested to ensure new threats are mitigated prior to becoming issues. Afilias will continue

these rigorous security measures, which include:
• Multiple layers of security and access controls throughout registry and support systems;
• 24x7 monitoring of all registry and DNS systems, support systems and facilities;
• Unique, proven registry design that ensures data integrity by granting only authorized access to the registry system, all while meeting performance requirements;
• Detailed incident and problem management processes for rapid review, communications, and problem resolution, and;
• Yearly external audits by independent, industry-leading firms, as well as twice-yearly internal audits.

Security policies and protocols

Afilias has included security in every element of its service, including facilities, hardware, equipment, connectivity/Internet services, systems, computer systems, organizational security, outage prevention, monitoring, disaster mitigation, and escrow/insurance, from the original design, through development, and finally as part of production deployment. Examples of threats and the confidential and proprietary mitigation procedures are detailed in our response to question #30(b).

There are several important aspects of the security policies and procedures to note:
• Afilias hosts domains in data centers around the world that meet or exceed global best practices.
• Afilias' DNS infrastructure is massively provisioned as part of its DDoS mitigation strategy, thus ensuring sufficient capacity and redundancy to support new gTLDs.
• Diversity is an integral part of all of our software and hardware stability and robustness plan, thus avoiding any single points of failure in our infrastructure.
• Access to any element of our service (applications, infrastructure and data) is only provided on an as-needed basis to employees and a limited set of others to fulfill their job functions. The principle of least privilege is applied.
• All registry components – critical and non-critical – are monitored 24x7 by staff at our NOCs, and the technical staff has detailed plans and procedures that have stood the test of time for addressing even the smallest anomaly. Well-documented incident management procedures are in place to quickly involve the on-call technical and management staff members to address any issues.

Afilias follows the guidelines from the ISO 27001 Information Security Standard (Reference: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103) for the management and implementation of its Information Security Management System. Afilias also utilizes the COBIT IT governance framework to facilitate policy development and enable controls for appropriate management of risk (Reference: http://www.isaca.org/cobit). Best practices defined in ISO 27002 are followed for defining the security controls within the organization. Afilias continually looks to improve the efficiency and effectiveness of our processes, and follows industry best practices as defined by the IT Infrastructure Library, or ITIL (Reference: http://www.itil-officialsite.com/).

The Afilias registry system is located within secure data centers that implement a multitude of security measures both to minimize any potential points of vulnerability and to limit any damage should there be a breach. The characteristics of these data centers are described fully in our response to question #30(b).

The Afilias registry system employs a number of multi-layered measures to prevent unauthorized access to its network and internal systems. Before reaching the registry network, all traffic is required to pass through a firewall system. Packets passing to and from the Internet are inspected, and unauthorized or unexpected attempts to connect to the registry servers are both logged and denied. Management processes are in place to ensure each request is tracked and documented, and regular firewall audits are performed to ensure proper operation. 24x7 monitoring is in place and, if potential malicious activity is detected, appropriate personnel are notified immediately.

Afilias employs a set of security procedures to ensure maximum security on each of its servers, including disabling all unnecessary services and processes and regular application of security-related patches to the operating system and critical system applications. Regular

external vulnerability scans are performed to verify that only services intended to be available are accessible.

Regular detailed audits of the server configuration are performed to verify that the configurations comply with current best security practices. Passwords and other access means are changed on a regular schedule and are revoked whenever a staff member's employment is terminated.

Access to registry system
Access to all production systems and software is strictly limited to authorized operations staff members. Access to technical support and network operations teams where necessary are read only and limited only to components required to help troubleshoot customer issues and perform routine checks. Strict change control procedures are in place and are followed each time a change is required to the production hardware/application. User rights are kept to a minimum at all times. In the event of a staff member's employment termination, all access is removed immediately.

Afilias applications use encrypted network communications. Access to the registry server is controlled. Afilias allows access to an authorized registrar only if each of the authentication factors matches the specific requirements of the requested authorization. These mechanisms are also used to secure any web-based tools that allow authorized registrars to access the registry. Additionally, all write transactions in the registry (whether conducted by authorized registrars or the registry's own personnel) are logged.

EPP connections are encrypted using TLS/SSL, and mutually authenticated using both certificate checks and login/password combinations. Web connections are encrypted using TLS/SSL for an encrypted tunnel to the browser, and authenticated to the EPP server using login/password combinations.

All systems are monitored for security breaches from within the data center and without, using both system-based and network-based testing tools. Operations staff also monitor systems for security-related performance anomalies. Triple-redundant continual monitoring ensures multiple detection paths for any potential incident or problem. Details are provided in our response to questions #30(b) and #42. Network Operations and Security Operations teams perform regular audits in search of any potential vulnerability.

To ensure that registrar hosts configured erroneously or maliciously cannot deny service to other registrars, Afilias uses traffic shaping technologies to prevent attacks from any single registrar account, IP address, or subnet. This additional layer of security reduces the likelihood of performance degradation for all registrars, even in the case of a security compromise at a subset of registrars.

There is a clear accountability policy that defines what behaviors are acceptable and unacceptable on the part of non-staff users, staff users, and management. Periodic audits of policies and procedures are performed to ensure that any weaknesses are discovered and addressed. Aggressive escalation procedures and well-defined Incident Response management procedures ensure that decision makers are involved at early stages of any event.

In short, security is a consideration in every aspect of business at Afilias, and this is evidenced in a track record of a decade of secure, stable and reliable service.

Independent assessment

Supporting operational excellence as an example of security practices, Afilias performs a number of internal and external security audits each year of the existing policies, procedures and practices for:
• Access control;
• Security policies;
• Production change control;
• Backups and restores;
• Batch monitoring;
• Intrusion detection, and

• Physical security.

Afilias has an annual Type 2 SSAE 16 audit performed by PricewaterhouseCoopers (PwC). Further, PwC performs testing of the general information technology controls in support of the financial statement audit. A Type 2 report opinion under SSAE 16 covers whether the controls were properly designed, were in place, and operating effectively during the audit period (calendar year). This SSAE 16 audit includes testing of internal controls relevant to Afilias' domain registry system and processes. The report includes testing of key controls related to the following control objectives:
• Controls provide reasonable assurance that registrar account balances and changes to the registrar account balances are authorized, complete, accurate and timely.
• Controls provide reasonable assurance that billable transactions are recorded in the Shared Registry System (SRS) in a complete, accurate and timely manner.
• Controls provide reasonable assurance that revenue is systemically calculated by the Deferred Revenue System (DRS) in a complete, accurate and timely manner.
• Controls provide reasonable assurance that the summary and detail reports, invoices, statements, registrar and registry billing data files, and ICANN transactional reports provided to registry operator(s) are complete, accurate and timely.
• Controls provide reasonable assurance that new applications and changes to existing applications are authorized, tested, approved, properly implemented and documented.
• Controls provide reasonable assurance that changes to existing system software and implementation of new system software are authorized, tested, approved, properly implemented and documented.
• Controls provide reasonable assurance that physical access to data centers is restricted to properly authorized individuals.
• Controls provide reasonable assurance that logical access to system resources is restricted to properly authorized individuals.
• Controls provide reasonable assurance that processing and backups are appropriately authorized and scheduled and that deviations from scheduled processing and backups are identified and resolved.

The last Type 2 report issued was for the year 2010, and it was unqualified, i.e., all systems were evaluated with no material problems found.

During each year, Afilias monitors the key controls related to the SSAE controls. Changes or additions to the control objectives or activities can result due to deployment of new services, software enhancements, infrastructure changes or process enhancements. These are noted and after internal review and approval, adjustments are made for the next review.

In addition to the PricewaterhouseCoopers engagement, Afilias performs internal security audits twice a year. These assessments are constantly being expanded based on risk assessments and changes in business or technology.

Additionally, Afilias engages an independent third-party security organization, PivotPoint Security, to perform external vulnerability assessments and penetration tests on the sites hosting and managing the Registry infrastructure. These assessments are performed with major infrastructure changes, release of new services or major software enhancements. These independent assessments are performed at least annually. A report from a recent assessment is attached with our response to question #30(b).

Afilias has engaged with security companies specializing in application and web security testing to ensure the security of web-based applications offered by Afilias, such as the Web Admin Tool (WAT) for registrars and registry operators.

Finally, Afilias has engaged IBM's Security services division to perform ISO 27002 gap assessment studies so as to review alignment of Afilias' procedures and policies with the ISO 27002 standard. Afilias has since made adjustments to its security procedures and policies based on the recommendations by IBM.

Special TLD considerations

Afilias' rigorous security practices are regularly reviewed; if there is a need to alter or

augment procedures for this TLD, they will be done so in a planned and deliberate manner.

Commitments to registrant protection

With over a decade of experience protecting domain registration data, Afilias understands registrant security concerns. Afilias supports a “thick” registry system in which data for all objects are stored in the registry database that is the centralized authoritative source of information. As an active member of IETF (Internet Engineering Task Force), ICANN’s SSAC (Security & Stability Advisory Committee), APWG (Anti-Phishing Working Group), MAAWG (Messaging Anti-Abuse Working Group), USENIX, and ISACA (Information Systems Audits and Controls Association), the Afilias team is highly attuned to the potential threats and leading tools and procedures for mitigating threats. As such, registrants should be confident that:
• Any confidential information stored within the registry will remain confidential;
• The interaction between their registrar and Afilias is secure;
• The Afilias DNS system will be reliable and accessible from any location;
• The registry system will abide by all polices, including those that address registrant data;
• Afilias will not introduce any features or implement technologies that compromise access to the registry system or that compromise registrant security.

Afilias has directly contributed to the development of the documents listed below and we have implemented them where appropriate. All of these have helped improve registrants’ ability to protect their domains name(s) during the domain name lifecycle.
• [SAC049]: SSAC Report on DNS Zone Risk Assessment and Management (03 June 2011)
• [SAC044]: A Registrant’s Guide to Protecting Domain Name Registration Accounts (05 November 2010)
• [SAC040]: Measures to Protect Domain Registration Services Against Exploitation or Misuse (19 August 2009)
• [SAC028]: SSAC Advisory on Registrar Impersonation Phishing Attacks (26 May 2008)
• [SAC024]: Report on Domain Name Front Running (February 2008)
• [SAC022]: Domain Name Front Running (SAC022, SAC024) (20 October 2007)
• [SAC011]: Problems caused by the non-renewal of a domain name associated with a DNS Name Server (7 July 2006)
• [SAC010]: Renewal Considerations for Domain Name Registrants (29 June 2006)
• [SAC007]: Domain Name Hijacking Report (SAC007) (12 July 2005)

To protect any unauthorized modification of registrant data, Afilias mandates TLS/SSL transport (per RFC 5246) and authentication methodologies for access to the registry applications. Authorized registrars are required to supply a list of specific individuals (five to ten people) who are authorized to contact the registry. Each such individual is assigned a pass phrase. Any support requests made by an authorized registrar to registry customer service are authenticated by registry customer service. All failed authentications are logged and reviewed regularly for potential malicious activity. This prevents unauthorized changes or access to registrant data by individuals posing to be registrars or their authorized contacts.

These items reflect an understanding of the importance of balancing data privacy and access for registrants, both individually and as a collective, worldwide user base.

The Afilias 24/7 Customer Service Center consists of highly trained staff who collectively are proficient in 15 languages, and who are capable of responding to queries from registrants whose domain name security has been compromised – for example, a victim of domain name hijacking. Afilias provides specialized registrant assistance guides, including specific hand-holding and follow-through in these kinds of commonly occurring circumstances, which can be highly distressing to registrants

Security resourcing plans

Please refer to our response to question #30b for security resourcing plans.

© Internet Corporation For Assigned Names and Numbers.

EXHIBIT JMR-15

New gTLD Application Submitted to ICANN by: NU DOT CO LLC

String: WEB

Originally Posted: 13 June 2012

Application ID: 1-1296-36138

Applicant Information

1. Full legal name

NU DOT CO LLC

2. Address of the principal place of business

Contact information Redacted

3. Phone number

Contact information Redacted

4. Fax number

Contact information Redacted

5. If applicable, website or URL

Primary Contact

6(a). Name

Jose Ignacio Rasco

6(b). Title

Manager

6(c). Address

6(d). Phone Number

Contact nformation Redacted

6(e). Fax Number

6(f). Email Address

Contact Information Redacted

Secondary Contact

7(a). Name

Mr. Nicolai Bezsonoff

7(b). Title

Manager

7(c). Address

7(d). Phone Number

Con ac nforma ion Redac ed

7(e). Fax Number

7(f). Email Address

Contact Information Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

Limited liability company

8(b). State the specific national or other jursidiction that defines the type of entity identified in 8(a).

NU DOTCO LLC is a UNITED STATES entity, registered in the STATE of DELAWARE as a limited liability company.

8(c). Attach evidence of the applicant's establishment.

Attachments are not displayed on this form.

9(a). If applying company is publicly traded, provide the exchange and symbol.

9(b). If the applying entity is a subsidiary, provide the parent company.

9(c). If the applying entity is a joint venture, list all joint venture partners.

Applicant Background

11(a). Name(s) and position(s) of all directors

Jose Ignacio Rasco III	Manager
Juan Diego Calle	Manager
Nicolai Bezsonoff	Manager

11(b). Name(s) and position(s) of all officers and partners

Jose Ignacio Rasco III	CFO
Juan Diego Calle	CEO
Nicolai Bezsonoff	COO

11(c). Name(s) and position(s) of all shareholders holding at least 15% of shares

Domain Marketing Holdings, LLC	Not Applicable
NUCO LP, LLC	Not Applicable

11(d). For an applying entity that does not have directors, officers, partners, or shareholders: Name(s) and position(s) of all individuals having legal or executive responsibility

Applied-for gTLD string

13. Provide the applied-for gTLD string. If an IDN, provide the U-label.

WEB

14(a). If an IDN, provide the A-label (beginning with "xn--").

14(b). If an IDN, provide the meaning or restatement of the string in English, that is, a description of the literal meaning of the string in the opinion of the applicant.

14(c). If an IDN, provide the language of the label (in English).

14(c). If an IDN, provide the language of the label (as referenced by ISO-639-1).

14(d). If an IDN, provide the script of the label (in English).

14(d). If an IDN, provide the script of the label (as referenced by ISO 15924).

14(e). If an IDN, list all code points contained in the U-label according to Unicode form.

15(a). If an IDN, Attach IDN Tables for the proposed registry.

Attachments are not displayed on this form.

15(b). Describe the process used for development of the IDN tables submitted, including consultations and sources used.

15(c). List any variant strings to the applied-for gTLD string according to the relevant IDN tables.

16. Describe the applicant's efforts to ensure that there are no known operational or rendering problems concerning the applied-for gTLD string. If such issues are known, describe steps that will be taken to mitigate these issues in software and other applications.

NU DOTCO, LLC ("NU.CO") foresees no known rendering issues in connection with the proposed .LAW TLD which it is seeking to apply for as a gTLD. This answer is based upon consultation with NU.CO's backend provider, Neustar, which has successfully launched a number of new gTLDs over the last decade. In reaching this determination, the following data points were analyzed: • ICANN's Security Stability Advisory Committee (SSAC) entitled Alternative TLD Name Systems and Roots: Conflict, Control and Consequences (SAC009); • IAB - RFC3696 "Application Techniques for Checking and Transformation of Names" • Known software issues which Neustar has encountered during the last decade launching new gTLDs; • Character type and length; • ICANN supplemental notes to Question 16; and • ICANN's presentation during its Costa Rica regional meeting on TLD Universal Acceptance;

17. (OPTIONAL) Provide a representation of the label according to the International Phonetic Alphabet (http://www.langsci.ucl.ac.uk/ipa/).

Mission/Purpose

18(a). Describe the mission/purpose of your proposed gTLD.

18.1 Mission/purpose of .WEB
The mission of .WEB is to provide the internet community at-large with an alternative "home domain" for their online presence. We envision that through strategic marketing campaigns designed to brand the domain, it will become a premium online namespace for a variety of businesses and websites. This general domain will provide new registrants with better, more relevant alternatives to the limited options remaining for current commercial TLD names.

18(b). How do you expect that your proposed gTLD will benefit registrants, Internet users, and others?

18.2 How will .WEB benefit registrants, Internet users, and others?
.WEB seeks to offer registrants and the broader internet community, with a reliable, trusted, and secure top level domain (TLD). Congestion in the current availability of commercial TLD names fundamentally advantages older incumbent players. Providing access to additional high-value second level domain names (i.e. shorter and more memorable) will provide an opportunity for new entrants to compete effectively for internet users' finite attention. The domain's coherent and consistent branding will assist registrants in developing meaningful emotional connection with users, allowing them to further differentiate themselves as premium destinations. These marketing efforts along with the initial adoption of key industry players, should reinforce the implicit attribution of "cutting-edge" and "innovativeness" upon its registrants. Prospective users benefit from the long-term commitment of a proven executive team that has a track-record of building and successfully marketing affinity TLD's (e.g., .CO targeting innovative businesses and entrepreneurs).

The demand for having an online presence continues to grow worldwide, especially as more people and businesses become active internet users, enjoying the increases in productivity and promotional effectiveness that the internet offers. A clear example of this is the number of worldwide internet users, which has grown at an average18% annual rate over the past decade, and domain registrations which have experienced similar adoption rates having grown from approximately 25mm in 2000 to over 225mm today.

In particular for small businesses and entrepreneurs, the Internet offers an incredibly useful way to promote themselves to a wider audience, both locally and globally. Moreover, it allows them to cost-effective offer their products and services directly to consumers, leveling the playing field with larger and more established competitors. A number of new and innovative business models have been established that were not possible prior to the Internet, creating substantial value for society.

However, until a few years ago it was difficult and costly for individuals and small businesses to establish an internet presence. This has changed as prices decreased dramatically and offerings became more accessible and intuitive. This is the result of having many retailers (i.e. registrars or resellers) that compete amongst each other on price, along with product and service differentiation. Differentiation has mainly centered around higher value-add services ancillary to the domain registration itself, such as hosting, web-site builders, SSL, e-mail, etc. The basic product (a domain) has not changed much, and until now, there have been few feasible alternatives to the commercial TLDs. The proposed new TLDs will provide users with more relevant and customized

options. Just as ICANN opened up the market for the distribution and registration of domains and created the Registrar industry, which ultimately benefitted hundreds of millions of people and businesses worldwide, we expect that the introduction of new TLDs will yield similar benefits.

The experienced team behind this application initially launched and currently operates the .CO ccTLD. The intention is for .WEB to be added to .CO's product portfolio, where it can benefit from economies of scale along with the firm's experience and expertise in marketing and branding TLD properties. Their successful track record proves that properly branded affinity domains can help sites form deeper emotional connections with their users, providing significant value-add. The .CO re-launch is a great illustration of how a new option in TLDs can address the unmet needs an affinity group (e.g., small businesses and start-ups), and we continue to firmly believe that the new .WEB domain will provide better, more relevant solutions for registrants .

Since its launch, .CO's marketing has primarily focused on developing a worldwide ecosystem of innovative small businesses and entrepreneurs. To date, the .CO registry, .CO Internet S.A.S, has reached close to 1.3 million domains under management, with more than one million individual new Registrations in the first year alone and a renewal rate for domains purchased during launch of nearly 70% and a current average renewal rate of 65%. The renewal rate is one of the highest amongst the industry and especially high considering it has not yet reached the multiple year expiration dates, where it's expected to climb even higher. In addition, .CO has become the standard secondary option to .COM for the leading global registrars, having the most conversions when presented with a non-.COM option. Further, .CO has secured a strong position with the tech startup community by securing such high profile users as Twitter (t.co), Google (g.co), tech influencers like Angel list (angel.co) and 500 Startups (500.co), and entrepreneurship organizations like Startup America (s.co).

.CO has differentiated itself from other existing TLDs by combining innovative branding with the highest standards in trademark protection, unprecedented marketing campaigns, and pro-active security monitoring. We plan to implement a very similar strategy for .WEB in its launch, operation, promotion and growth.

We plan to target a similar community of entrepreneurs, startups, and progressive corporate entities that are looking for an online presence with a suitable domain name. We anticipate the addressable community will continue to grow as traditional businesses choose to launch an online presence for their pre-existing operations and as entrepreneurs launch new start-ups. The domain's marketing strategy will utilize a 3 pillar framework, similar to that used with .CO:

- Awareness: We plan to launch marketing campaigns to both the small businesses and entrepreneurs promoting .WEB via a combination of:
o Media placements online and offline
o Social media campaigns
o Events
o Sponsorships
o Endorsements
o PR efforts
o Direct marketing
o Channel marketing

- Usage: We plan to foster the community of users of .WEB via a combination community engagement and outreach, use-case development and direct marketing to base.

- Distribution: The distribution will be done through the existing ICANN accredited registrar channel and will include marketing at the point of sale, packages and bundles, campaigns, etc.

The marketing plans will evolve depending on market conditions, but using .CO as an example, we implemented an awareness and branding strategy that included the creation of a brand identity and logo; mass media placements including 2 super-bowl commercials with one of our partners plus many TV placements; billboards and other outdoors campaigns; several online media campaigns including networks, re-targeting and videos; ongoing Twitter, Facebook engagements; sponsorship and presence in a variety of events for TMs (INTA), Tech startups (SxSW, Web 2.0, Internetweek, etc.), Startups (Task Rabbit TR.co), Community (ICANN, LACTLD, etc.), etc. We also implemented for .CO a strong usage promotion of the domain by creating and fostering a community of .CO users and case studies. We achieved this through a combination of events, sponsorships, and partnerships with different entities like Angel.co, 500.co, Startup America (s.co), founders institute (fi.co), etc. We also cultivated many case studies of successful .CO users, remaining in close contact with them. Finally, we implemented a rigorous channel marketing and sales plan that included marketing placements at the

point of purchase plus co-marketing and community outreach.

While we do plan to follow a similar strategy to achieve widespread awareness, usage and distribution, the budget and actual placements for promoting .WEB will be scaled down accordingly, as neither its volume of registrations or revenues is expected to be in line with that of .CO.

By launching the .WEB domain we expect to provide more descriptive/ relevant options for end-users, including access to desirable second level domain names which are unavailable or occupied by current general TLD's. As illustrated with .CO, the rapid growth to 1.3 million domains is evidence of pent up demand in the marketplace for good, descriptive domain names. We expect that our marketing strategies will result in a new branded and available option that will emotionally connect with potential users and allow them to differentiate themselves through the use of a branded premium domain.

We will also follow the same ICANN rules and distribution methods of major gTLDs thereby ensuring Registrars and Resellers do not have to change their systems to distribute the .WEB domain. As our systems are already integrated with largest registrars in the world and we have implemented industry best practices, the transition to delegation and launch should be seamless to the registrar channel as well as consumers.

We will also implement a thick whois and adopt any ICANN recommendations or requirements in the future. In order to protect the privacy of our users, we will allow the use of Privacy or Proxy registrations by reputable registrars that comply with applicable policies specified by ICANN. We find this service is highly valuable for registrants that want to ensure their information is not available online and would like to maintain a higher level privacy.

18(c). What operating rules will you adopt to eliminate or minimize social costs?

18.3 .WEB operating rules to benefit consumers
We plan to follow all ICANN policies, including the best practices and recommendations for gTLDs. This will allow us to ensure end-users, have an easy way to register/purchase, administer, and use their domains. Adopting these policies will also prevent malicious behavior by third parties and ensure a smooth operation of the domain. The plans for the launch will be similar to the launch process used in .CO, which included:

- Gradual Offering Plan: The .CO launch included a very comprehensive gradual opening plan that both protected trademarks and provided transparency to end users. The launch was lauded by ICANN for its comprehensiveness and management. For the launch of .WEB we will follow ICANN's policies especially as it relates to the Trademark Clearinghouse which was similar to the process we used for .CO:
-
o Sunrise: Provide a period of a few weeks to allow the TM and IP community to register their .WEB domains prior to the opening to the public. Trademark validations will be done by the Trademark Clearinghouse or as specified by ICANN in their policies. If there are multiple validated applications, these would go to auction and allocated based on these results.
o Landrush: Provide a period of a few weeks to allow domain investors and others that are interested in premium domains to apply for these domains. Once the period of the Landrush phase is over, a process to check the applications will determine if these were unique or if there were multiple applicants. If single applicants, then the domain is awarded at that time. If multiple applicants then the domain would go to an auction in which all applicants would be able to participate. For .CO this process included close to 30,000 applications and the resulting auctions were managed by Pool.com. The process was very successful managing to allocate very efficiently domains according to their perceived value by applicants and bidders at the resulting auctions.

- General Availability: For .CO we had 100k registrations in the first 10 minutes and we didn't have a single issue nor service degradation through the launch or afterwards. We achieved this through a combination of strong planning between our partners, especially Neustar our back-end provider; communication with our Registrars prior and during the launch in a very structured way; strong infrastructure planning and provisioning; and effective load, contingency, and disaster recovery planning. We plan to use similar methods for the launch of .WEB.
o First come first serve during GA and afterwards, which we believe is the best mechanism to ensure a fair allocation of domains once the domain has been launched.
o Use of UDRP and any other best-practices in rights protection mechanisms

o Highly managed General Availability launch
- Premium Domains: We will keep some domains for premium sales and these will be restricted prior to the Gradual Offering Plan begins, but can be applied for during the Sunrise phase. These premium domains will be brokered or sold via auction directly or through an accredited 3rd party. With .CO we used this mechanism as a way to allocate high value domains and also to promote the usage of the domain by high profile companies including Twitter with t.co, Google with g.co, Startup America with s.co, as well as a myriad of smaller startups and other endorsements.

Community-based Designation

19. Is the application for a community-based TLD?

No

20(a). Provide the name and full description of the community that the applicant is committing to serve.

20(b). Explain the applicant's relationship to the community identified in 20(a).

20(c). Provide a description of the community-based purpose of the applied-for gTLD.

20(d). Explain the relationship between the applied-for gTLD string and the community identified in 20(a).

20(e). Provide a description of the applicant's intended registration policies in support of the community-based purpose of the applied-for gTLD.

20(f). Attach any written endorsements from institutions/groups representative of the community identified in 20(a).

Attachments are not displayed on this form.

Geographic Names

21(a). Is the application for a geographic name?

No

Protection of Geographic Names

22. Describe proposed measures for protection of geographic names at the second and other levels in the applied-for gTLD.

In preparation for answering this question, NU DOTCO, LLC (NU.CO) reviewed the following relevant background material regarding the protection of geographic names in the DNS, including:

- ICANN Board Resolution 01-92 regarding the methodology developed for the reservation and release of country names in the .INFO top-level domain (see http://www.icann.org/en/minutes/minutes-10sep01.htm);

- ICANN's Proposed Action Plan on .INFO Country Names (see http://www.icann.org/en/meetings/montevideo/action-plan-country-names-09oct01.htm);

- "Report of the Second WIPO Internet Domain Name Process: The Recognition and Rights and the Use of Names in the Internet Domain Name System," Section 6, Geographical Identifiers (see http://www.wipo.int/amc/en/processes/process²/report/html/report.html);

- ICANN's Governmental Advisory Committee (GAC) Principles Regarding New gTLDs, (see https://gacweb.icann.org/download/attachments/1540128/gTLD_principles_0.pdf?version=1&modificationDate=1312358178000); and

- ICANN's Generic Names Supporting Organization (GNSO) Reserved Names Working Group – Final Report (see http://gnso.icann.org/issues/new-gtlds/final-report-rn-wg-23may07.htm).

Initial Reservation of Country and Territory Names

NU.CO is committed to initially reserving the country and territory names contained in the internationally recognized lists described in Article 5 of Specification 5 attached to the New gTLD Applicant Guidebook at the second level and at all other levels within the .WEB gTLD at which domain name registrations will be provided. Specifically, NU.CO will reserve:

- The short form (in English) of all country and territory names contained on the ISO 3166- 1 list, as updated from time to time, including the European Union, which is exceptionally reserved on the ISO 3166-1 list, and its scope extended in August 1999 to any application needing to represent the name European Union (see http://www.iso.org/iso/support/country_codes/iso_3166_code_lists/iso-3166-1_decoding_table.htm#EU);

- The United Nations Group of Experts on Geographical Names, Technical Reference Manual for the Standardization of Geographical Names, Part III Names of Countries of the World; and

- The list of United Nations member states in six official United Nations languages prepared by the Working Group on Country Names of the United Nations Conference on the Standardization of Geographical Names.

Potential Future Release of Two Character Names

While NU.CO foresees no immediate need for plans to make use of these initially reserved country names at the second level within the .WEB namespace, NU.CO recognizes that there has been several successful and non-misleading use of country names by new gTLD operators as evidenced below:

AUSTRALIA.COOP – Is operated by Co-operatives Australia the national body for State Co-operative Federations and provides a valuable resource about cooperatives within Australia.

UK.COOP – Is operated by Co-operatives UK the national trade body that campaigns for co-operation and works to promote, develop and unite co-operative enterprises within the United Kingdom.

NZ.COOP – Is operated by the New Zealand Cooperatives Association which brings together the country's cooperative mutual business in a not-for-profit incorporated society.

USA.JOBS - Is operated by DirectEmployers Association (DE). While Employ Media the registry operator of the .JOBS gTLD is currently in a dispute with ICANN regarding the allocation of this and other domain names. Direct Employers has a series of partnerships and programs with the United States Department of Labor, the National Association of State Workforce Agencies and Facebook to help unemployed workers find jobs.

MALDIVIAN.AERO - Is the dominant domestic air carrier in Maldives, and provides a range of commercial and leisure air transport services.

The more likely request by NU.CO will come in connection with the un-reservation and allocation of two-letter .WEB domain names, e.g. US.WEB, UK.WEB, etc. If NU.CO should decide in the future to attempt and allocate these domain names, it would submit the proper Registry Service Evaluation Processes (RSEP) with ICANN. In evaluating similar RSEP requests that have been submitted to ICANN by other gTLD registry operators, NU.CO believes that its request would be favorably granted.

Creation and Updating the Policies

NU.CO is committed to continually reviewing and updating when necessary its policies in this area. Consistent with this commitment, NU.CO intends to remain an active participant in any ongoing ICANN policy discussion regarding the protection of geographic names within the DNS.

Registry Services

23. Provide name and full description of all the Registry Services to be provided.

23.1 Introduction

NU DOTCO LLC has elected to partner with NeuStar, Inc ("Neustar") to provide back-end services for the .WEB registry. In making this decision, NU DOTCO LLC recognized that Neustar already possesses a production-proven registry system that can be quickly deployed and smoothly operated over its robust, flexible, and scalable world-class infrastructure. The existing registry services will be leveraged for the .WEB registry. The following section describes the registry services to be provided.

23.2 Standard Technical and Business Components

Neustar will provide the highest level of service while delivering a secure, stable and comprehensive registry platform. NU DOTCO LLC will use Neustar's Registry Services platform to deploy the .WEB registry, by providing the following Registry Services (none of these services are offered in a manner that is unique to .WEB):

-Registry-Registrar Shared Registration Service (SRS)
-Extensible Provisioning Protocol (EPP)
-Domain Name System (DNS)
-WHOIS
-DNSSEC
-Data Escrow
-Dissemination of Zone Files using Dynamic Updates
-Access to Bulk Zone Files

-Dynamic WHOIS Updates
-IPv6 Support
-Rights Protection Mechanisms
-Internationalized Domain Names (IDN)

The following is a description of each of the services.

23.2.1 SRS

Neustar's secure and stable SRS is a production-proven, standards-based, highly reliable, and high-performance domain name registration and management system. The SRS includes an EPP interface for receiving data from registrars for the purpose of provisioning and managing domain names and name servers. The response to Question 24 provides specific SRS information.

23.2.2 EPP

The .WEB registry will use the Extensible Provisioning Protocol (EPP) for the provisioning of domain names. The EPP implementation will be fully compliant with all RFCs. Registrars are provided with access via an EPP API and an EPP based Web GUI. With more than 10 gTLD, ccTLD, and private TLDs implementations, Neustar has extensive experience building EPP-based registries. Additional discussion on the EPP approach is presented in the response to Question 25.

23.2.3 DNS

NU DOTCO LLC will leverage Neustar's world-class DNS network of geographically distributed nameserver sites to provide the highest level of DNS service. The service utilizes "Anycast" routing technology, and supports both IPv4 and IPv6. The DNS network is highly proven, and currently provides service to over 20 TLDs and thousands of enterprise companies. Additional information on the DNS solution is presented in the response to Questions 35.

23.2.4 WHOIS

Neustar's existing standard WHOIS solution will be used for the .WEB. The service provides supports for near real-time dynamic updates. The design and construction is agnostic with regard to data display policy is flexible enough to accommodate any data model. In addition, a searchable WHOIS service that complies with all ICANN requirements will be provided. The following WHOIS options will be provided:

Standard WHOIS (Port 43)
Standard WHOIS (Web)
Searchable WHOIS (Web)

23.2.5 DNSSEC

An RFC compliant DNSSEC implementation will be provided using existing DNSSEC capabilities. Neustar is an experienced provider of DNSSEC services, and currently manages signed zones for three large top level domains: .biz, .us, and .co. Registrars are provided with the ability to submit and manage DS records using EPP, or through a web GUI. Additional information on DNSSEC, including the management of security extensions is found in the response to Question 43.

23.2.6 Data Escrow

Data escrow will be performed in compliance with all ICANN requirements in conjunction with an approved data escrow provider. The data escrow service will:

-Protect against data loss
-Follow industry best practices
-Ensure easy, accurate, and timely retrieval and restore capability in the event of a hardware failure
-Minimizes the impact of software or business failure.

Additional information on the Data Escrow service is provided in the response to Question 38.

23.2.7 Dissemination of Zone Files using Dynamic Updates

Dissemination of zone files will be provided through a dynamic, near real-time process. Updates will be performed within the specified performance levels. The proven technology ensures that updates pushed to all nodes within a few minutes of the changes being received by the SRS. Additional information on the DNS updates may be found in the response to Question 35.

23.2.8 Access to Bulk Zone Files

NU DOTCO LLC will provide third party access to the bulk zone file in accordance with specification 4, Section 2 of the Registry Agreement. Credentialing and dissemination of the zone files will be facilitated through the Central Zone Data Access Provider.

23.2.9 Dynamic WHOIS Updates

Updates to records in the WHOIS database will be provided via dynamic, near real-time updates. Guaranteed delivery message oriented middleware is used to ensure each individual WHOIS server is refreshed with dynamic updates. This component ensures that all WHOIS servers are kept current as changes occur in the SRS, while also decoupling WHOIS from the SRS. Additional information on WHOIS updates is presented in response to Question 26.

23.2.10 IPv6 Support

The .WEB registry will provide IPv6 support in the following registry services: SRS, WHOIS, and DNS/DNSSEC. In addition, the registry supports the provisioning of IPv6 AAAA records. A detailed description on IPv6 is presented in the response to Question 36.

23.2.11 Required Rights Protection Mechanisms

NU DOTCO LLC, will provide all ICANN required Rights Mechanisms, including:

-Trademark Claims Service
-Trademark Post-Delegation Dispute Resolution Procedure (PDDRP)
-Registration Restriction Dispute Resolution Procedure (RRDRP)
-UDRP
-URS
-Sunrise service.
More information is presented in the response to Question 29.

23.2.12 Internationalized Domain Names (IDN)

IDN registrations are provided in full compliance with the IDNA protocol. Neustar possesses extensive experience offering IDN registrations in numerous TLDs, and its IDN implementation uses advanced technology to accommodate the unique bundling needs of certain languages. Character mappings are easily constructed to block out characters that may be deemed as confusing to users. A detailed description of the IDN implementation is presented in response to Question 44.

23.3 Unique Services

NU DOTCO LLC will not be offering services that are unique to .WEB.

23.4 Security or Stability Concerns

All services offered are standard registry services that have no known security or stability concerns. Neustar has demonstrated a strong track record of security and stability within the industry.

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

24.1 Introduction

NU DOTCO LLC has partnered with NeuStar, Inc ("Neustar"), an experienced TLD registry operator, for the operation of the .WEB Registry. The applicant is confident that the plan in place for the operation of a robust and reliable Shared Registration System (SRS) as currently provided by Neustar will satisfy the criterion established by ICANN.

Neustar built its SRS from the ground up as an EPP based platform and has been operating it reliably and at scale since 2001. The software currently provides registry services to five TLDs (.BIZ, .US, TEL, .CO and .TRAVEL) and is used to provide gateway services to the .CN and .TW registries. Neustar's state of the art registry has a proven track record of being secure, stable, and robust. It manages more than 6 million domains, and has over 300 registrars connected today.
The following describes a detailed plan for a robust and reliable SRS that meets all ICANN requirements including compliance with Specifications 6 and 10.

24.2 The Plan for Operation of a Robust and Reliable SRS

24.2.1 High-level SRS System Description

The SRS to be used for .WEB will leverage a production-proven, standards-based, highly reliable and high-performance domain name registration and management system that fully meets or exceeds the requirements as identified in the new gTLD Application Guidebook.

The SRS is the central component of any registry implementation and its quality, reliability and capabilities are essential to the overall stability of the TLD. Neustar has a documented history of deploying SRS implementations with proven and verifiable performance, reliability and availability. The SRS adheres to all industry standards and protocols. By leveraging an existing SRS platform, NU DOTCO LLC is mitigating the significant risks and costs associated with the development of a new system. Highlights of the SRS include:

-State-of-the-art, production proven multi-layer design
-Ability to rapidly and easily scale from low to high volume as a TLD grows
-Fully redundant architecture at two sites
-Support for IDN registrations in compliance with all standards
-Use by over 300 Registrars
-EPP connectivity over IPv6
-Performance being measured using 100% of all production transactions (not sampling).

24.2.2 SRS Systems, Software, Hardware, and Interoperability

The systems and software that the registry operates on are a critical element to providing a high quality of service. If the systems are of poor quality, if they are difficult to maintain and operate, or if the registry personnel are unfamiliar with them, the registry will be prone to outages. Neustar has a decade of experience operating registry infrastructure to extremely high service level requirements. The infrastructure is designed using best of breed systems and software. Much of the application software that performs registry-specific operations was developed by the current engineering team and a result the team is intimately familiar with its operations.

The architecture is highly scalable and provides the same high level of availability and performance as volumes increase. It combines load balancing technology with scalable server technology to provide a cost effective and efficient method for scaling.

The Registry is able to limit the ability of any one registrar from adversely impacting other registrars by consuming too many resources due to excessive EPP transactions. The system uses network layer 2 level packet shaping to limit the number of simultaneous connections registrars can open to the protocol layer.

All interaction with the Registry is recorded in log files. Log files are generated at each layer of the system. These log files record at a minimum:

-The IP address of the client
-Timestamp
-Transaction Details
-Processing Time.

In addition to logging of each and every transaction with the SRS Neustar maintains audit records, in the database, of all transformational transactions. These audit records allow the Registry, in support of the applicant, to produce a complete history of changes for any domain name.

24.2.3 SRS Design

The SRS incorporates a multi-layer architecture that is designed to mitigate risks and easily scale as volumes increase. The three layers of the SRS are:

-Protocol Layer
-Business Policy Layer
-Database.

Each of the layers is described below.

24.2.4 Protocol Layer

The first layer is the protocol layer, which includes the EPP interface to registrars. It consists of a high availability farm of load-balanced EPP servers. The servers are designed to be fast processors of transactions. The servers perform basic validations and then feed information to the business policy engines as described below. The protocol layer is horizontally scalable as dictated by volume.

The EPP servers authenticate against a series of security controls before granting service, as follows:

-The registrar's host exchanges keys to initiates a TLS handshake session with the EPP server.
-The registrar's host must provide credentials to determine proper access levels.
-The registrar's IP address must be preregistered in the network firewalls and traffic-shapers.

24.2.5 Business Policy Layer

The Business Policy Layer is the "brain" of the registry system. Within this layer, the policy engine servers perform rules-based processing as defined through configurable attributes. This process takes individual transactions, applies various validation and policy rules, persists data and dispatches notification through the central database in order to publish to various external systems. External systems fed by the Business Policy Layer include backend processes such as dynamic update of DNS, WHOIS and Billing.

Similar to the EPP protocol farm, the SRS consists of a farm of application servers within this layer. This design ensures that there is sufficient capacity to process every transaction in a manner that meets or exceeds all service level requirements. Some registries couple the business logic layer directly in the protocol layer or within the database. This architecture limits the ability to scale the registry. Using a decoupled architecture enables the load to be distributed among farms of inexpensive servers that can be scaled up or down as demand changes.

The SRS today processes over 30 million EPP transactions daily.

24.2.6 Database

The database is the third core components of the SRS. The primary function of the SRS database is to provide highly reliable, persistent storage for all registry information required for domain registration services. The database is highly secure, with access limited to transactions from authenticated registrars, trusted application-server processes, and highly restricted access by the registry database administrators. A full description of the database can be found in response to Question 33.

Figure 24-1 attached depicts the overall SRS architecture including network components.

24.2.7 Number of Servers

As depicted in the SRS architecture diagram above Neustar operates a high availability architecture where at each level of the stack there are no single points of failures. Each of the network level devices run with dual pairs as do the databases. For the .WEB registry, the SRS will operate with 8 protocol servers and 6 policy engine servers. These expand horizontally as volume increases due to additional TLDs, increased load, and through organic growth. In addition to the SRS servers described

above, there are multiple backend servers for services such as DNS and WHOIS. These are discussed in detail within those respective response sections.

24.2.8 Description of Interconnectivity with Other Registry Systems

The core SRS service interfaces with other external systems via Neustar's external systems layer. The services that the SRS interfaces with include:

-WHOIS
-DNS
-Billing
-Data Warehouse (Reporting and Data Escrow).

Other external interfaces may be deployed to meet the unique needs of a TLD. At this time there are no additional interfaces planned for .WEB.

The SRS includes an "external notifier" concept in its business policy engine as a message dispatcher. This design allows time-consuming backend processing to be decoupled from critical online registrar transactions. Using an external notifier solution, the registry can utilize "control levers" that allow it to tune or to disable processes to ensure optimal performance at all times. For example, during the early minutes of a TLD launch, when unusually high volumes of transactions are expected, the registry can elect to suspend processing of one or more back end systems in order to ensure that greater processing power is available to handle the increased load requirements. This proven architecture has been used with numerous TLD launches, some of which have involved the processing of over tens of millions of transactions in the opening hours. The following are the standard three external notifiers used the SRS:

24.2.9 WHOIS External Notifier

The WHOIS external notifier dispatches a work item for any EPP transaction that may potentially have an impact on WHOIS. It is important to note that, while the WHOIS external notifier feeds the WHOIS system, it intentionally does not have visibility into the actual contents of the WHOIS system. The WHOIS external notifier serves just as a tool to send a signal to the WHOIS system that a change is ready to occur. The WHOIS system possesses the intelligence and data visibility to know exactly what needs to change in WHOIS. See response to Question 26 for greater detail.

24.2.10 DNS External Notifier

The DNS external notifier dispatches a work item for any EPP transaction that may potentially have an impact on DNS. Like the WHOIS external notifier, the DNS external notifier does not have visibility into the actual contents of the DNS zones. The work items that are generated by the notifier indicate to the dynamic DNS update sub-system that a change occurred that may impact DNS. That DNS system has the ability to decide what actual changes must be propagated out to the DNS constellation. See response to Question 35 for greater detail.

24.2.11 Billing External Notifier

The billing external notifier is responsible for sending all billable transactions to the downstream financial systems for billing and collection. This external notifier contains the necessary logic to determine what types of transactions are billable. The financial systems use this information to apply appropriate debits and credits based on registrar.

24.2.12 Data Warehouse

The data warehouse is responsible for managing reporting services, including registrar reports, business intelligence dashboards, and the processing of data escrow files. The Reporting Database is used to create both internal and external reports, primarily to support registrar billing and contractual reporting requirement. The data warehouse databases are updated on a daily basis with full copies of the production SRS data.

24.2.13 Frequency of Synchronization between Servers

The external notifiers discussed above perform updates in near real-time, well within the prescribed service level requirements. As transactions from registrars update the core SRS, update notifications are pushed to the external systems such as DNS and WHOIS. These updates are typically live in the

external system within 2-3 minutes.

24.2.14 Synchronization Scheme (e.g., hot standby, cold standby)

Neustar operates two hot databases within the data center that is operating in primary mode. These two databases are kept in sync via synchronous replication. Additionally, there are two databases in the secondary data center. These databases are updated real time through asynchronous replication. This model allows for high performance while also ensuring protection of data. See response to Question 33 for greater detail.

24.2.15 Compliance with Specification 6 Section 1.2

The SRS implementation for .WEB is fully compliant with Specification 6, including section 1.2. EPP Standards are described and embodied in a number of IETF RFCs, ICANN contracts and practices, and registry-registrar agreements. Extensible Provisioning Protocol or EPP is defined by a core set of RFCs that standardize the interface that make up the registry-registrar model. The SRS interface supports EPP 1.0 as defined in the following RFCs shown in Table 24-1 attached.

Additional information on the EPP implementation and compliance with RFCs can be found in the response to Question 25.

24.2.16 Compliance with Specification 10

Specification 10 of the New TLD Agreement defines the performance specifications of the TLD, including service level requirements related to DNS, RDDS (WHOIS), and EPP. The requirements include both availability and transaction response time measurements. As an experienced registry operator, Neustar has a long and verifiable track record of providing registry services that consistently exceed the performance specifications stipulated in ICANN agreements. This same high level of service will be provided for the .WEB Registry. The following section describes Neustar's experience and its capabilities to meet the requirements in the new agreement.

To properly measure the technical performance and progress of TLDs, Neustar collects data on key essential operating metrics. These measurements are key indicators of the performance and health of the registry. Neustar's current .biz SLA commitments are among the most stringent in the industry today, and exceed the requirements for new TLDs. Table 24-2 compares the current SRS performance levels compared to the requirements for new TLDs, and clearly demonstrates the ability of the SRS to exceed those requirements.

Their ability to commit and meet such high performance standards is a direct result of their philosophy towards operational excellence. See response to Question 31 for a full description of their philosophy for building and managing for performance.

24.3 Resourcing Plans

The development, customization, and on-going support of the SRS are the responsibility of a combination of technical and operational teams, including:

-Development/Engineering
-Database Administration
-Systems Administration
-Network Engineering.

Additionally, if customization or modifications are required, the Product Management and Quality Assurance teams will be involved in the design and testing. Finally, the Network Operations and Information Security play an important role in ensuring the systems involved are operating securely and reliably.

The necessary resources will be pulled from the pool of operational resources described in detail in the response to Question 31. Neustar's SRS implementation is very mature, and has been in production for over 10 years. As such, very little new development related to the SRS will be required for the implementation of the .WEB registry. The following resources are available from those teams:

-Development/Engineering – 19 employees
-Database Administration- 10 employees
-Systems Administration – 24 employees

-Network Engineering – 5 employees

The resources are more than adequate to support the SRS needs of all the TLDs operated by Neustar, including the .WEB registry.

25. Extensible Provisioning Protocol (EPP)

25.1 Introduction

NU DOTCO LLC's back-end registry operator, Neustar, has over 10 years of experience operating EPP based registries. They deployed one of the first EPP regis

EXHIBIT JMR-16

New gTLD Application Submitted to ICANN by: Web.com Group, Inc.

String: web

Originally Posted: 13 June 2012

Application ID: 1-1009-97005

Applicant Information

1. Full legal name

Web.com Group, Inc.

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact Informat on Redacted

4. Fax number

Contact Informat on Redacted

5. If applicable, website or URL

http://www.web.com

Primary Contact

6(a). Name

Mr. Robert Conant Wiegand

6(b). Title

Senior Vice President

6(c). Address

6(d). Phone Number

Contact Information Redacted

6(e). Fax Number

6(f). Email Address

Contact Information Redacted

Secondary Contact

7(a). Name

Mr. Matthew Patrick McClure

7(b). Title

Chief Legal Officer

7(c). Address

7(d). Phone Number

Contact Informat on Redacted

7(e). Fax Number

7(f). Email Address

Contact Information Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

Corporation

8(b). State the specific national or other jursidiction that defines the type of entity identified in 8(a).

General Corporation Law of the State of Delaware

8(c). Attach evidence of the applicant's establishment.

Attachments are not displayed on this form.

9(a). If applying company is publicly traded, provide the exchange and symbol.

NASDAQ;WWWW

9(b). If the applying entity is a subsidiary, provide the parent company.

9(c). If the applying entity is a joint venture, list all joint venture partners.

Applicant Background

11(a). Name(s) and position(s) of all directors

Anton J. Levy	Director
David L. Brown	Chairman of the Board
Deborah H. Quazzo	Director
Hugh M. Durden	Director
Phillip J. Facchina	Director
Robert S. McCoy	Director
Timothy I. Maudlin	Director

11(b). Name(s) and position(s) of all officers and partners

David L. Brown	CEO & President
Jason M. Teichman	EVP and Chief Marketing Officer
Kevin M. Carney	EVP and Chief Financial Officer
Matthew P. McClure	Chief Legal Officer & Secretary
Roseann Duran	EVP and Chief People Officer

11(c). Name(s) and position(s) of all shareholders holding at least 15% of shares

NWS Holdings	Not Applicable

11(d). For an applying entity that does not have directors, officers, partners, or shareholders: Name(s) and position(s) of all individuals having legal or executive responsibility

Applied-for gTLD string

13. Provide the applied-for gTLD string. If an IDN, provide the U-label.

web

14(a). If an IDN, provide the A-label (beginning with "xn--").

14(b). If an IDN, provide the meaning or restatement of the string in English, that is, a description of the literal meaning of the string in the opinion of the applicant.

14(c). If an IDN, provide the language of the label (in English).

14(c). If an IDN, provide the language of the label (as referenced by ISO-639-1).

14(d). If an IDN, provide the script of the label (in English).

14(d). If an IDN, provide the script of the label (as referenced by ISO 15924).

14(e). If an IDN, list all code points contained in the U-label according to Unicode form.

15(a). If an IDN, Attach IDN Tables for the proposed registry.

Attachments are not displayed on this form.

15(b). Describe the process used for development of the IDN tables submitted, including consultations and sources used.

15(c). List any variant strings to the applied-for gTLD string according to the relevant IDN tables.

16. Describe the applicant's efforts to ensure that there are no known operational or rendering problems concerning the applied-for gTLD string. If such issues are known, describe steps that will be taken to mitigate these issues in software and other applications.

Web.com Group, Inc. (”Web.com”) has taken a number of steps, including consulting with Verisign, our registry services provider to ensure that there are no known operational or rendering problems concerning the .web gTLD string.

Many software applications conduct software validity checks. Applications like web browsers and desktop software will validate the use of URLs either by a validation of the known gTLDs and/or the length of the string. The gTLDs delegated during the 2004 round experienced universal acceptance issues that for the most part are resolved today.

Upon delegation of .web, Web.com intends to conduct thorough integration testing with all major software applications. Further, Web.com intends to assist customers of the .web gTLD as issues arise. Web.com understands that these items cannot be remedied alone, but Web.com will collaborate with software vendors about issues as they are discovered to ensure seamless adoption.

17. (OPTIONAL) Provide a representation of the label according to the International Phonetic Alphabet (http://www.langsci.ucl.ac.uk/ipa/).

Mission/Purpose

18(a). Describe the mission/purpose of your proposed gTLD.

18(a). Describe the mission/purpose of your proposed gTLD.

Web.com Group, Inc (“Web.com”) has been in the business of helping our customers establish their online presence for over 15 years. Following our acquisition of Register.com in July 2010 and the subsequent acquisition of Network Solutions, LLC, the oldest ICANN accredited registrar, in October 2011, we have become one of the largest domain name registrars in the world with approximately 3 million customers. Web.com offers a variety of TLDs and a full suite of domain-name services, including registration, management, renewal, expiration protection and privacy services.

The creation of a .web gTLD will help to fulfill ICANN’s mission of providing more competition in the online marketplace and Web.com is the perfect candidate for operating

.web given its experience, global reach, and brand recognition.

Why .web?

Web.com knows from years of experience that the .com gTLD has played a revolutionary role in the advancement of global commerce and culture. In addition, the .com gTLD has had a powerful and democratizing impact, providing avenues for anyone to participate in online discourse and a growing market. There are, however, a finite number of useful second-level domains that can be applied for in .com, as ICANN knows and understands. Often other gTLDs, such as .org, .info, .biz and others either are unavailable or are not a good fit for a potential second-level domain.

In looking to expand the gTLD landscape beyond the existing robustness of gTLD offerings, an easy-to-remember and intuitively logical gTLD such as .web is a relevant addition. Consumers will instantly understand that a .web domain is an Internet website thereby ensuring quick adoption by users. Due to its ubiquitous nature, .web will compete directly with all gTLDs, both existing ones and others to be approved by ICANN. It has universal appeal to anyone looking to operate on the World Wide Web. Not only will .web introduce a new and previously unavailable range of domain choices to businesses and individuals around the world but it could also serve as a platform for a number of innovative domain-based services.

The .web gTLD will help customers launch and leverage their presence on the Internet. As a leading global provider of online marketing services to small businesses, Web.com recognizes that finding a relevant and memorable domain name can be challenging. Since many keywords and descriptive phrases associated with existing TLDs have already been registered, it is often difficult to pinpoint a domain name which contains an acceptable number of characters. Consequently, prospective registrants are many times unable to secure a unique and adequate name.

The availability of .web domains will spark competition across all industries engaging customers online by providing more opportunities for registrants to secure easily found domains. Consumer choice will increase, and in doing so, online operators will seek ways to differentiate themselves from their competition with proactive steps to build consumer trust and confidence.

Introducing .web as a gTLD choice also will inject additional inventory into the domain name marketplace. As such, it will increase competition within the Internet registry space, as well as provide avenues for increased registrar competition.

Why Web.com?

As the sole owner of the Web.com® Trademark--issued by the U.S. Patent and Trademark Office-- Web.com seeks to be the sole registry operator for the .web gTLD. Historically, Web.com has offered and will continue to provide pre-registration service for the .web gTLD through www.register.web.com. We remain committed to promoting .web as a new gTLD and to expanding the competitive landscape that permeates the Internet.

Founded in 1997 as Atlantic Teleservices, Web.com has evolved to become a leading provider of Internet services for small- to medium-sized businesses (“SMBs”). Web.com is the parent company of two global domain name registrars, and further meets the Internet needs of consumers and businesses throughout their lifecycle with affordable value-added services. These services include domain-name registration; website design; search engine optimization; search engine marketing; social media and mobile products; local sales leads; ecommerce solutions; and call center services.

Headquartered in Jacksonville, FL, USA, Web.com is a publicly traded company (Nasdaq: WWWW) serving nearly three million customers, with more than 1,700 global employees in fourteen locations in North America, South America and the United Kingdom. In recognition of its rapid progress, Web.com has appeared on Deloitte’s Technology Fast 500™ list in each of the past two years.

One of our primary corporate goals is to provide a broad range of online services and products that enable SMBs to establish, maintain, promote, and optimize their web presence. By providing a comprehensive and best-in-class suite of services, we are able to deliver

solutions that enable small and medium-sized businesses to compete and succeed online. Customers can choose to purchase ‘a la carte’ solutions for specific issues, or subscribe to bundled products that meet a variety of needs.

Web.com brings a wealth of experience in providing a seamless process for customers from the first point of registration through the growth of their Internet properties. Following our acquisition of Register.com in July 2010 and the subsequent acquisition of Network Solutions in October 2011, we have become one of the largest domain name registrars in the world. Web.com offers a variety of TLDs and a full suite of domain-name services, including registration, management, renewal, expiration protection and privacy services. Web.com is also a prominent player in the Internet community through participation in numerous working groups and organizations including the Certificate Authentication Board, Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet standards development community.

Additionally, since the .web gTLD mirrors the Web.com brand, trademarks, and the character string associated with our corporate website address (www.web.com), we believe that Web.com should be the sole operator and administrator of the .web gTLD. The issuance of the .web gTLD to anyone other than Web.com would infringe on the trademark rights in Web.com and be confusingly similar to domains currently in use by Web.com such as www.register.web.com and www.dot.web.com.

18(b). How do you expect that your proposed gTLD will benefit registrants, Internet users, and others?

18(b). How proposed gTLD will benefit registrants, Internet users, and others.

The .web gTLD will benefit registrants, Internet users, and others in a number of ways:

- Increase the domain-name extension inventory: An expanding global population results in more Internet users, coupled with increasing demand for domain name choices. The .web gTLD provides alternatives in every possible imagining of a website, from ecommerce to promotion of free expression.

- Increased availability of generic word domain names. For the first time in decades, generic names that have been locked down by registrants in existing gTLDs will be available in a new and easy-to-remember gTLD, which increases competition and benefits Internet users.

- Increase online innovation: New online properties with the .web gTLD will spur competitors to innovate in ways that will empower consumers, enabling communication instantaneously with others in their own communities and worldwide, at a low cost relative to traditional forms of media. The Internet’s unique attributes create new opportunities to collaborate, exchange ideas, and promote scientific, cultural, and economic progress. These opportunities will increase when .web is introduced by ICANN and implemented and operated by Web.com.

Web.com is committed to providing best-in-class service to customers by maintaining our position as an industry leader. Our goal is to enable online users to expand their web presence and we are committed to offering a greater choice in top level domain extensions.

18(b)(i) What is the goal of your proposed TLD in terms of areas of specialty, service levels, of reputation?

Many gTLDs introduced by ICANN will, by their nature, appeal only to certain segments of the online population, whether those communities are industries, ethnicities, or other collections of like-minded individuals and organizations. We are hopeful that the .web gTLD will have the same popularity as that of .com.

Web.com has the scalability and processes required to meet the challenges anticipated with the .web gTLD. Today we manage over 8 million domain names across hundreds of TLDs. We

are committed to servicing and/or providing domain-name resolution services that adhere to industry standards. Following our existing standards of industry benchmark performance, we will continuously monitor and proactively defend the .web infrastructure and associated services in order to provide reliable services for each registrant in areas of specialty, service levels, and reputation:

• Specialty: As the first domain-name ICANN-accredited registrar, Web.com's Network Solutions subsidiary brings an unprecedented 25 years of domain industry experience to the community as a whole. The .web gTLD will be the baseline by which customers can incorporate new generation web-based technologies, enabling their web presence to be a highly efficient and effective communication mechanism. The experience and trust associated with Web.com will help ensure that outcome.

• Service Levels: Web.com has a long history of succeeding in its mission of providing world-class domain registration services. Our longstanding commitment to the highest service levels will be replicated with .web. Furthermore, we will meet or exceed the service levels mandated within the Registry Agreement enforced by ICANN as it pertains, but not limited, to the registration and resolution of the .web gTLD zone. Web.com is pleased to be working with Verisign, one of the leading Internet infrastructure companies, to launch .web. Verisign's unmatched performance in the operation of existing TLDs will ensure a high degree of service, stability and reliability.

• Reputation: Given our success over the course of the last 15 years, we are confident that Web.com will continue to serve customers with the best in class service as it pertains to the .web gTLD. Given the proactive safeguards we incorporate, and will continue to incorporate within the .web gTLD, we believe potential customers will register a .web gTLD in order to be associated with a secure, reliable and scalable gTLD. At Web.com, we believe that a website is only as good as the services and support behind it. With the .web gTLD, we have the opportunity to bring this same level of commitment to a gTLD.

18(b)(ii) What do you anticipate your proposed TLD will add to the current space, in terms of competition, differentiation, or innovation?

As stated in 18(a) above, the .web gTLD will have a dramatic impact by increasing competition, providing more differentiation for customers and consumers, while driving innovation.

• Competition: The addition of a .web gTLD will increase competition across all vertical online platforms. Registrars will compete to offer .web and meet the high demand for .web second-level TLDs. Vendors in the online marketplace will seek to expand their existing footprint or pioneer new products and services with a fresh .web website. The universal appeal of a .web URL will provide competition to every TLD, both broad-based existing ones--such as .com, .org, .biz and .info--as well as others that will be approved by ICANN, whether broad-based or narrowly targeted. Internet users will benefit from the dramatically accelerated competitive environment resulting from ICANN's adoption of .web operated by Web.com.

• Differentiation: The .web gTLD will quickly become as ubiquitous as .com. The .web gTLD will be the most versatile gTLD on the World Wide Web. A brand name company might choose .com; a non-profit .org; a start-up .biz; a resource site .info; and so on. But every one of those organizations' sites would be perfectly compatible with a .web second-level domain. More narrow gTLDs will provide differentiation in certain niches and markets; .web will do so in every conceivable area on the Internet, from commerce to information to community-building. The introduction of generics under a new gTLD also will provide differentiated approaches to reaching Internet users.

• Innovation: There is little room for continued innovation by .com registrants seeking to compete with and differentiate themselves from other .com registrants. That is not a negative reflection on .com, but rather the fact that there are a finite number of short and memorable second-level domains. With many keywords and descriptive phrases already registered, incentives to innovate decrease with each year. A land rush of .web addresses will reverse that decline and drive new innovation in web delivery and customer service.

18(b)(iii) What goals does your proposed TLD have in terms of user experience?

Web.com will provide rewarding user experiences on two levels:

- Registrants: Web.com will incorporate the ability to allow various segments of the market to take advantage of registering the desired .web domain name. This includes providing the IP community with the ability to secure the .web domains affiliated or associated with their brands during a proposed Sunrise period, prior to making registrations publicly available to all. This registrant service is a natural extension of decades of experience on the part of Web.com and its holdings. Web.com may also enable registrants who have already purchased domains in other gTLDs the ability to register those domains in the .web gTLD. For registrants who are looking to improve their domain name or looking to purchase a new one, having .web will open up a new swath of choices in a gTLD that is new, fresh and directly tied to their goals of establishing their web presence. Upon enabling registrations to the general public, Web.com will incorporate a Go to Market Launch plan that will focus on ease of use, perspective registrant outreach program, and proactive communication associated with turn-key customer service. We intend to maintain our leading position that includes the lowest churn rates in the industry, which will be critical to the rollout of .web and its long-term success as a vibrant gTLD.

- Internet users: For users of .web gTLD websites, our enhanced efforts to prevent abusive behavior to protect the rights of others will result in a user experience that is more stable and secure than what they currently experience in other gTLDs. We fully recognize that eliminating abusive and fraudulent behavior is a difficult challenge but it is one that we will stress as we develop our plans to launch .web. Web.com plans to vigorously enforce all provisions we have outlined in the responses to Questions 28 and 29 to ensure a positive experience for all users of the .web gTLD.

18(b)(iv) Provide a complete description of the applicant’s intended registration policies in support of the goals listed above.

Web.com takes its responsibilities in the operation of the .web gTLD very seriously. We have implemented a series of measures that, when taken together, will ensure that registrants have the ability to register names of their choice while ensuring that policies are in place to prevent and mitigate abusive behavior as well as protect the rights of others.

These registration policies include:

- An Acceptable Use Policy (AUP) that clearly defines what is considered abuse and what registrants may and may not do with their .web domain names

- A name selection policy that ensures compliance with ICANN mandated restrictions on second level domains

- Support for Uniform Rapid Suspension (URS) and Uniform Domain-Name Dispute-Resolution Policy (UDRP) to mitigate trademark infringement

The gTLD will be launched in multiple phases, ensuring a stable, secure, and controlled introduction:

- Sunrise A: This initial phase will allow the trademark community the ability to secure the .web domains associated with their brands for a 60-day period - double the ICANN minimum.

- Possible Sunrise B: We are also considering a second phase which might be available for previously registered names in other gTLDs.

- Landrush: Following the Sunrise phases, this phase will allow domain registrants to register domains at a premium price point. Multiple submissions will be auctioned, with the auction provider to be named at a later date.

- General Availability: This final phase will be open to the general public. Domains may be registered on a first-come/first-serve basis.

18(b)(v) Will your proposed TLD impose any measures for protecting the privacy or confidential information of registrants or users? If so, please describe any such measures.

Web.com respects the privacy of its customers and the visitors and users of its websites. The .web gTLD will be governed by a strict Privacy Policy to ensure the privacy of information for registrants as well as users. Web.com is an industry leader in providing transparent and rigorous policies on how sensitive information will be used, as well as preventing unauthorized access to information through vigilant use of the latest technological innovations. We will continue our commitment to privacy for our customers and website users by publicly posting our privacy policies on the registry website. Web.com will ensure compliance with all laws and regulations that govern privacy issues.

18(b)(vi) Describe whether and in what ways outreach and communications will help to achieve your projected benefits.

Web.com enables regular dialogue with its registrants by establishing and maintaining clear and secure channels of communication. Web.com has every incentive to ensure that potential and existing .web registrants understand privacy and security measures to protect their information and to assist in their adherence to the AUP in their efforts to protect Internet users.

No other registry is better equipped to deal with the communication challenges inherent in the rollout and maintenance of a gTLD with the appeal and anticipated popularity of .web.

To ensure the success of the .web launch, the company will undertake a global marketing and advertising campaign to create customer awareness and interest in the features and benefits of the .web gTLD.

18(c). What operating rules will you adopt to eliminate or minimize social costs?

18(c) What operating rules will you adopt to minimize social costs (e.g., time or financial resources costs, as well as various types of consumer vulnerabilities? What other steps will you take to minimize negative consequences/costs imposed upon consumers?

As stated earlier, we take our responsibilities in this area very seriously. To demonstrate our commitment to make the .web gTLD more resistant to abusive behavior than other gTLDs that currently exist, Web.com has explored various mechanisms to help prevent abusive registrations. We were particularly impressed with the set of 31 Proposed Security, Stability and Resiliency Requirements for Financial TLDs that were developed by the Security Standards Working Group (SSWG) under the guidance of the financial services industry. Following their recommendation that all potential applicants look at these standards for their own TLDs, Web.com has completed a thorough review to determine which ones might enhance the .web gTLD experience. While not all of the proposed standards are applicable to the .web gTLD, we will endeavor to implement several of them to aid in our efforts to prevent and mitigate abusive registrations. In addition to the mechanisms described in 18 (b)(iv), we will undertake the following efforts:

- An Acceptable Use policy that clearly defines what is considered abuse and what registrants may and may not do with their domain names
- A seasoned abuse mitigation team that has years of experience in dealing with these issues
- Technological measures for removal of orphan glue records
- Efforts and measures to promote accurate and complete ‘Whois’
- Requirements for .web accredited registrars to enact measures in support of these efforts
- Extended Sunrise services
- Extended trademark claims service
- Name Selection Policy
- Acceptable Use Policy

- Support for URS and UDRP
- PDDRP
- Rapid takedown or suspension where necessary
- Anti-Abuse Process
- Enhanced Authentication
- Malware Code Identification
- DNSSEC signing service
- Biannual‘WHOIS’ Verification
- Participation in anti-abuse community activities

18(c)(i) How will multiple applications for a particular domain name be resolved, for example, by auction or on a first-come/first-serve basis?

Web.com will launch the .web gTLD in the following phases:

- Sunrise A: This initial phase will allow the trademark community the ability to secure the .web domains associated with their brands for a 60-day period.

- Possible Sunrise B: This second phase could be available for previously registered names in other gTLDs.

- Landrush: Following the Sunrise phases, Landrush will allow registrants to register domains at a premium price point. Multiple submissions for the same domain name will be resolved through auction, with an auction provider to be named at a later date.

- General Availability: This final phase will be open to the general public. Domains may be registered on a first-come/first-serve basis.

18(c)(ii) Explain any cost benefits for registrants you intend to implement (e.g., advantageous pricing, introductory discounts, bulk registration discounts).

Web.com, like ICANN, has every incentive to see the .web gTLD become a ubiquitous online presence, serving Internet users globally and spurring online innovation. As such, we will institute necessary incentives to encourage rapid rollout and growing adoption of the .web gTLD, with policies to be developed and adopted in the future as necessary.

18(c)(iii) Note that the Registry Agreement requires that registrars be offered the option to obtain initial domain name registrations for periods of one to ten years at the discretion of the registrar, but no greater than ten years. Additionally, the Registry Agreement requires advance written notice of price increases. Do you intend to make contractual commitments to registrants regarding the magnitude of price escalation? If so, please describe your plans.

Web.com intends to price its domains competitively to maximize sales, while at the same time ensuring profitable, secure, and sustainable operations. It is premature to elaborate on specific policies at this stage in the process, but we intend to be responsive to market demands and share ICANN’s desire to ensure a rapid spread and adoption of .web. Web.com will fully comply with all necessary and recommended notification requirements in the event that price increases are necessary.

Community-based Designation

19. Is the application for a community-based TLD?

No

20(a). Provide the name and full description of the community that the applicant is committing to serve.

20(b). Explain the applicant's relationship to the community identified in 20(a).

20(c). Provide a description of the community-based purpose of the applied-for gTLD.

20(d). Explain the relationship between the applied-for gTLD string and the community identified in 20(a).

20(e). Provide a description of the applicant's intended registration policies in support of the community-based purpose of the applied-for gTLD.

20(f). Attach any written endorsements from institutions/groups representative of the community identified in 20(a).

Attachments are not displayed on this form.

Geographic Names

21(a). Is the application for a geographic name?

No

Protection of Geographic Names

22. Describe proposed measures for protection of geographic names at the second and other levels in the applied-for gTLD.

In order to comply with ICANN requirements and GAC recommendations regarding the protection of geographic names, Web.com Group, Inc. (”Web.com”) has developed and will implement the following measures to protect geographical names at the second and all other levels in the .web gTLD:

1. Rules for Reserving Geographical Names

Web.com will comply with Specification 5 ”Schedule of Reserved Names at the Second Level in gTLD Registries” Section 5 titled ”Country and Territory Names.” The country and territory names contained in the following internationally recognized lists shall be initially reserved at the second level and at all other levels within the .web gTLD at which the Web.com provides for registrations:

a. the short form (in English) of all country and territory names contained on the ISO 3166-1 list, as updated from time to time, including the European Union, which is exceptionally reserved on the ISO 3166-1 list, and its scope extended in August 1999 to any application needing to represent the name European Union;
b. the United Nations Group of Experts on Geographical Names, Technical Reference Manual for the Standardization of Geographical Names, Part III Names of Countries of the World; and
c. the list of United Nations member states in 6 official United Nations languages prepared by the Working Group on Country Names of the United Nations Conference on the Standardization of Geographical Names.

2. Incorporation of GAC recommendation regarding second level geographic domains

Web.com will review and seriously consider suggestions from global government entities, public authorities and the IGO’s regarding additional names with national or geographic significant at the second level.

Web.com will consider any claims of abuse, including abuse of names with national or geographic significance as serious offenses. The Abuse Prevention and Mitigation Procedures for the .web gTLD will ensure that governments, public authorities or IGO’s have the ability to raise cases of concern.

3. Rules for registration and employment of geographical names.

If a decision is made by Web.com to release names reserved in Section 1 above, Web.com will follow the policy and procedures outlined in Specification 5 of the Registry agreement and will work effectively to reach agreement with the applicable government(s), provided, further, that Web.com may also propose release of these reservations, subject to review by ICANN’s Governmental Advisory Committee and approval by ICANN.

Registry Services

23. Provide name and full description of all the Registry Services to be provided.

1 CUSTOMARY REGISTRY SERVICES

Please note; all figures, tables and diagrams referenced in the following response can be found in attachment titled “Attachment dot web Q23.”

As Web.com Group, Inc.’s (”Web.com”) selected provider of backend registry services, Verisign provides a comprehensive system and physical security solution that is designed to ensure a TLD is protected from unauthorized disclosure, alteration, insertion, or destruction of registry data. Verisign’s system addresses all areas of security including

information and policies, security procedures, the systems development lifecycle, physical security, system hacks, break-ins, data tampering, and other disruptions to operations. Verisign's operational environments not only meet the security criteria specified in its customer contractual agreements, thereby preventing unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with applicable standards, but also are subject to multiple independent assessments as detailed in the response to Question 30, Security Policy. Verisign's physical and system security methodology follows a mature, ongoing lifecycle that was developed and implemented many years before the development of the industry standards with which Verisign currently complies. Please see the response to Question 30, Security Policy, for details of the security features of Verisign's registry services.

Verisign's registry services fully comply with relevant standards and best current practice RFCs published by the Internet Engineering Task Force (IETF), including all successor standards, modifications, or additions relating to the DNS and name server operations including without limitation RFCs 1034, 1035, 1982, 2181, 2182, 2671, 3226, 3596, 3597, 3901, 4343, and 4472. Moreover, Verisign's Shared Registration System (SRS) supports the following IETF Extensible Provisioning Protocol (EPP) specifications, where the Extensible Markup Language (XML) templates and XML schemas are defined in RFC 3915, 5730, 5731, 5732, 5733, and 5734. By strictly adhering to these RFCs, Verisign helps to ensure its registry services do not create a condition that adversely affects the throughput, response time, consistency, or coherence of responses to Internet servers or end systems. Besides its leadership in authoring RFCs for EPP, Domain Name System Security Extensions (DNSSEC), and other DNS services, Verisign has created and contributed to several now well-established IETF standards and is a regular and long-standing participant in key Internet standards forums.

Figure 23-1 summarizes the technical and business components of those registry services, customarily offered by a registry operator (i.e., Verisign), that support this application. These services are currently operational and support both large and small Verisign-managed registries. Customary registry services are provided in the same manner as Verisign provides these services for its existing gTLDs.

Through these established registry services, Verisign has proven its ability to operate a reliable and low-risk registry that supports millions of transactions per day. Verisign is unaware of any potential security or stability concern related to any of these services.

Registry services defined by this application are not intended to be offered in a manner unique to the new generic top-level domain (gTLD) nor are any proposed services unique to this application's registry.

As further evidence of Verisign's compliance with ICANN mandated security and stability requirements, Verisign allocates the applicable RFCs to each of the five customary registry services (items A – E above). For each registry service, Verisign also provides evidence in Figure 23-2 of Verisign's RFC compliance and includes relevant ICANN prior-service approval actions.

1.1 Critical Operations of the Registry

i. Receipt of Data from Registrars Concerning Registration of Domain Names and Name Servers
See Item A in Figure 23-1 and Figure 23-2.

ii. Provision to Registrars Status Information Relating to the Zone Servers

Verisign is Web.com's selected provider of backend registry services. Verisign registry services provisions to registrars status information relating to zone servers for the gTLD. The services also allow a domain name to be updated with clientHold, serverHold status, which removes the domain name server details from zone files. This ensures that DNS queries of the domain name are not resolved temporarily. When these hold statuses are removed, the name server details are written back to zone files and DNS queries are again resolved. Figure 23-3 describes the domain name status information and zone insertion indicator provided to registrars. The zone insertion indicator determines whether the name server details of the domain name exist in the zone file for a given domain name status. Verisign also has the capability to withdraw domain names from the zone file in near real time by changing the domain name statuses upon request by customers, courts, or legal authorities

as required.

iii. Dissemination of TLD Zone Files
See Item B in Figure 23-1 and Figure 23-2.

iv. Operation of the Registry Zone Servers
Verisign is Web.com’s selected provider of backend registry services. Verisign, as a company, operates zone servers and serves DNS resolution from 76 geographically distributed resolution sites located in North America, South America, Africa, Europe, Asia, and Australia. Currently, 17 DNS locations are designated primary sites, offering greater capacity than smaller sites comprising the remainder of the Verisign constellation. Verisign also uses Anycast techniques and regional Internet resolution sites to expand coverage, accommodate emergency or surge capacity, and support system availability during maintenance procedures. Verisign plans to operate Web.com’s .web gTLD from a minimum of eight of its primary sites (two on the East Coast of the United States, two on the West Coast of the United States, two in Europe, and two in Asia) and expand resolution sites based on traffic volume and patterns. Further details of the geographic diversity of Verisign’s zone servers are provided in the response to Question 34, Geographic Diversity. Moreover, additional details of Verisign’s zone servers are provided in the response to Question 32, Architecture and the response to Question 35, DNS Service.

v. Dissemination of Contact and Other Information Concerning Domain Name Server Registrations
See Item C in Figure 23-1 and Figure 23-2.

2 OTHER PRODUCTS OR SERVICES THE REGISTRY OPERATOR IS REQUIRED TO PROVIDE BECAUSE OF THE ESTABLISHMENT OF A CONSENSUS POLICY
Verisign, Web.com’s selected provider of backend registry services, is a proven supporter of ICANN’s consensus-driven, bottom-up policy development process whereby community members identify a problem, initiate policy discussions, and generate a solution that produces effective and sustained results. Verisign currently provides all of the products or services (collectively referred to as services) that the registry operator is required to provide because of the establishment of a Consensus Policy. For the .web gTLD, Verisign implements these services using the same proven processes and procedures currently in-place for all registries under Verisign’s management. Furthermore, Verisign executes these services on computing platforms comparable to those of other registries under Verisign’s management. Verisign’s extensive experience with consensus policy required services and its proven processes to implement these services greatly minimize any potential risk to Internet security or stability. Details of these services are provided in the following subsections. It shall be noted that consensus policy services required of registrars (e.g., Whois Reminder, Expired Domain) are not included in this response. This exclusion is in accordance with the direction provided in the question’s Notes column to address registry operator services.

2.1 Inter-Registrar Transfer Policy (IRTP)
Technical Component: In compliance with the IRTP consensus policy, Verisign, Web.com’s selected provider of backend registry services, has designed its registration systems to systematically restrict the transfer of domain names within 60 days of the initial create date. In addition, Verisign has implemented EPP and “AuthInfo” code functionality, which is used to further authenticate transfer requests. The registration system has been designed to enable compliance with the five-day transfer grace period and includes the following functionality:

- Allows the losing registrar to proactively ‘ACK’ or acknowledge a transfer prior to the expiration of the five-day transfer grace period
- Allows the losing registrar to proactively ‘NACK’ or not acknowledge a transfer prior to the expiration of the five-day transfer grace period
- Allows the system to automatically ACK the transfer request once the five-day transfer grace period has passed if the losing registrar has not proactively ACK’d or NACK’d the transfer request.

Business Component: All requests to transfer a domain name to a new registrar are handled according to the procedures detailed in the IRTP. Dispute proceedings arising from a registrar’s alleged failure to abide by this policy may be initiated by any ICANN-accredited registrar under the Transfer Dispute Resolution Policy. Web.com’s compliance

office serves as the first level dispute resolution provider pursuant to the associated Transfer Dispute Resolution Policy. As needed Verisign is available to offer policy guidance as issues arise.

Security and Stability Concerns: Verisign is unaware of any impact caused by the service on throughput, response time, consistency, or coherence of the responses to Internet servers or end-user systems. By implementing the IRTP in accordance with ICANN policy, security is enhanced as all transfer commands are authenticated using the AuthInfo code prior to processing.

ICANN Prior Approval: Verisign has been in compliance with the IRTP since November 2004 and is available to support Web.com in a consulting capacity as needed.

Unique to the TLD: This service is not provided in a manner unique to the .web gTLD.

2.2 Add Grace Period (AGP) Limits Policy

Technical Component: Verisign's registry system monitors registrars' Add grace period deletion activity and provides reporting that permits Web.com to assess registration fees upon registrars that have exceeded the AGP thresholds stipulated in the AGP Limits Policy. Further, Web.com accepts and evaluates all exemption requests received from registrars and determines whether the exemption request meets the exemption criteria. Web.com maintains all AGP Limits Policy exemption request activity so that this material may be included within Web.com's Monthly Registry Operator Report to ICANN.

Registrars that exceed the limits established by the policy may submit exemption requests to Web.com for consideration. Web.com's compliance office reviews these exemption requests in accordance with the AGP Limits Policy and renders a decision. Upon request, Web.com submits associated reporting on exemption request activity to support reporting in accordance with established ICANN requirements.

Business Component: The Add grace period (AGP) is restricted for any gTLD operator that has implemented an AGP. Specifically, for each operator:

- During any given month, an operator may not offer any refund to an ICANN-accredited registrar for any domain names deleted during the AGP that exceed (i) 10% of that registrar's net new registrations (calculated as the total number of net adds of one-year through ten-year registrations as defined in the monthly reporting requirement of Operator Agreements) in that month, or (ii) fifty (50) domain names, whichever is greater, unless an exemption has been granted by an operator.

- Upon the documented demonstration of extraordinary circumstances, a registrar may seek from an operator an exemption from such restrictions in a specific month. The registrar must confirm in writing to the operator how, at the time the names were deleted, these extraordinary circumstances were not known, reasonably could not have been known, and were outside the registrar's control. Acceptance of any exemption will be at the sole and reasonable discretion of the operator; however "extraordinary circumstances" that reoccur regularly for the same registrar will not be deemed extraordinary.

In addition to all other reporting requirements to ICANN, Web.com identifies each registrar that has sought an exemption, along with a brief description of the type of extraordinary circumstance and the action, approval, or denial taken by the operator.

Security and Stability Concerns: Verisign is unaware of any impact, caused by the policy, on throughput, response time, consistency, or coherence of the responses to Internet servers or end-user systems.

ICANN Prior Approval: Verisign, Web.com's backend registry services provider, has had experience with this policy since its implementation in April 2009 and is available to support Web.com in a consulting capacity as needed.

Unique to the TLD: This service is not provided in a manner unique to the .web gTLD.

2.3 Registry Services Evaluation Policy (RSEP)

Technical Component: Verisign, Web.com's selected provider of backend registry services, adheres to all RSEP submission requirements. Verisign has followed the process many times

and is fully aware of the submission procedures, the type of documentation required, and the evaluation process that ICANN adheres to.

Business Component: In accordance with ICANN procedures detailed on the ICANN RSEP website (http://www.icann.org/en/registries/rsep/), all gTLD registry operators are required to follow this policy when submitting a request for new registry services.

Security and Stability Concerns: As part of the RSEP submission process, Verisign, Web.com's backend registry services provider, identifies any potential security and stability concerns in accordance with RSEP stability and security requirements. Verisign never launches services without satisfactory completion of the RSEP process and resulting approval.

ICANN Prior Approval: Not applicable.

Unique to the TLD: gTLD RSEP procedures are not implemented in a manner unique to the .web gTLD.

3 PRODUCTS OR SERVICES ONLY A REGISTRY OPERATOR IS CAPABLE OF PROVIDING BY REASON OF ITS DESIGNATION AS THE REGISTRY OPERATOR

Web.com plans to implement a Premium Name Service as part of launch plans for the .web gTLD. Work is still proceeding on this effort but it will be modeled after similar offerings during recent TLD launches and the reserved Premium Domain Name list will comply with all necessary ICANN regulations related to such efforts. This list will be authoritative and these names will not be available during Sunrise A&B or Landrush.

Verisign, Web.com's selected backend registry services provider, has developed a Registry-Registrar Two-Factor Authentication Service that complements traditional registration and resolution registry services. In accordance with direction provided in Question 23, Verisign details below the technical and business components of the service, identifies any potential threat to registry security or stability, and lists previous interactions with ICANN to approve the operation of the service. The Two-Factor Authentication Service is currently operational, supporting multiple registries under ICANN's purview.

Web.com is unaware of any competition issue that may require the registry service(s) listed in this response to be referred to the appropriate governmental competition authority or authorities with applicable jurisdiction. ICANN previously approved the service(s), at which time it was determined that either the service(s) raised no competitive concerns or any applicable concerns related to competition were satisfactorily addressed.

3.1 Two-Factor Authentication Service

Technical Component: The Registry-Registrar Two-Factor Authentication Service is designed to improve domain name security and assist registrars in protecting the accounts they manage. As part of the service, dynamic one-time passwords augment the user names and passwords currently used to process update, transfer, and/or deletion requests. These one-time passwords enable transaction processing to be based on requests that are validated both by "what users know" (i.e., their user name and password) and "what users have" (i.e., a two-factor authentication credential with a one-time-password).

Registrars can use the one-time-password when communicating directly with Verisign's Customer Service department as well as when using the registrar portal to make manual updates, transfers, and/or deletion transactions. The Two-Factor Authentication Service is an optional service offered to registrars that execute the Registry-Registrar Two-Factor Authentication Service Agreement.

Business Component: There is no charge for the Registry-Registrar Two-Factor Authentication Service. It is enabled only for registrars that wish to take advantage of the added security provided by the service.

Security and Stability Concerns: Verisign is unaware of any impact, caused by the service, on throughput, response time, consistency, or coherence of the responses to Internet servers or end-user systems. The service is intended to enhance domain name security, resulting in increased confidence and trust by registrants.

ICANN Prior Approval: ICANN approved the same Two-Factor Authentication Service for Verisign's use on .com and .net on 10 July 2009 (RSEP Proposal 2009004) and for .name on 16 February 2011 (RSEP Proposal 2011001).

Unique to the TLD: This service is not provided in a manner unique to the .web gTLD.

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

1 ROBUST PLAN FOR OPERATING A RELIABLE SRS

Please note; all figures, tables and diagrams referenced in the following response can be found in attachment titled "Attachment dot web Q24."

1.1 High-Level Shared Registration System (SRS) System Description
Verisign, Web.com Group, Inc.'s ("Web.com") selected provider of backend registry services, provides and operates a robust and reliable SRS that enables multiple registrars to provide domain name registration services in the top-level domain (TLD). Verisign's proven reliable SRS serves approximately 915 registrars, and Verisign, as a company, has averaged more than 140 million registration transactions per day. The SRS provides a scalable, fault-tolerant platform for the delivery of gTLDs through the use of a central customer database, a web interface, a standard provisioning protocol (i.e., Extensible Provisioning Protocol, EPP), and a transport protocol (i.e., Secure Sockets Layer, SSL).

The SRS components include:

- Web Interface: Allows customers to access the authoritative database for accounts, contacts, users, authorization groups, product catalog, product subscriptions, and customer notification messages.
- EPP Interface: Provides an interface to the SRS that enables registrars to use EPP to register and manage domains, hosts, and contacts.
- Authentication Provider: A Verisign developed application, specific to the SRS, that authenticates a user based on a login name, password, and the SSL certificate common name and client IP address.

The SRS is designed to be scalable and fault tolerant by incorporating clustering in multiple tiers of the platform. New nodes can be added to a cluster within a single tier to scale a specific tier, and if one node fails within a single tier, the services will still be available. The SRS allows registrars to manage the .web gTLD domain names in a single architecture. To flexibly accommodate the scale of its transaction volumes, as well as new technologies, Verisign employs the following design practices:
- Scale for Growth: Scale to handle current volumes and projected growth.
- Scale for Peaks: Scale to twice base capacity to withstand "registration add attacks" from a compromised registrar system.
- Limit Database CPU Utilization: Limit utilization to no more than 50 percent during peak loads.
- Limit Database Memory Utilization: Each user's login process that connects to the database allocates a small segment of memory to perform connection overhead, sorting, and data caching. Verisign's standards mandate that no more than 40 percent of the total available physical memory on the database server will be allocated for these functions.

Verisign's SRS is built upon a three-tier architecture as illustrated in Figure 24-1 and detailed here:
- Gateway Layer: The first tier, the gateway servers, uses EPP to communicate with registrars. These gateway servers then interact with application servers, which comprise the second tier.
- Application Layer: The application servers contain business logic for managing and

maintaining the registry business. The business logic is particular to each TLD's business rules and requirements. The flexible internal design of the application servers allows Verisign to easily leverage existing business rules to apply to the .web gTLD. The application servers store Web.com's data in the registry database, which comprises the third and final tier. This simple, industry-standard design has been highly effective with other customers for whom Verisign provides backend registry services.

- Database Layer: The database is the heart of this architecture. It stores all the essential information provisioned from registrars through the gateway servers. Separate servers query the database, extract updated zone and Whois information, validate that information, and distribute it around the clock to Verisign's worldwide domain name resolution sites.

Scalability and Performance. Verisign, Web.com's selected backend registry services provider, implements its scalable SRS on a supportable infrastructure that achieves the availability requirements in Specification 10. Verisign employs the design patterns of simplicity and parallelism in both its software and systems, based on its experience that these factors contribute most significantly to scalability and reliable performance. Going counter to feature-rich development patterns, Verisign intentionally minimizes the number of lines of code between the end user and the data delivered. The result is a network of restorable components that provide rapid, accurate updates. Figure 24-2 depicts EPP traffic flows and local redundancy in Verisign's SRS provisioning architecture. As detailed in the figure, local redundancy is maintained for each layer as well as each piece of equipment. This built-in redundancy enhances operational performance while enabling the future system scaling necessary to meet additional demand created by the .web gTLD.

Besides improving scalability and reliability, local SRS redundancy enables Verisign to take down individual system components for maintenance and upgrades, with little to no performance impact. With Verisign's redundant design, Verisign can perform routine maintenance while the remainder of the system remains online and unaffected. For the .web gTLD registry, this flexibility minimizes unplanned downtime and provides a more consistent end-user experience.

1.2 Representative Network Diagrams

Figure 24-3 provides a summary network diagram of Web.com's selected backend registry services provider's (Verisign's) SRS. This configuration at both the primary and alternate-primary Verisign data centers provides a highly reliable backup capability. Data is continuously replicated between both sites to ensure failover to the alternate-primary site can be implemented expeditiously to support both planned and unplanned outages.

1.3 Number of Servers

As Web.com's selected provider of backend registry services, Verisign continually reviews its server deployments for all aspects of its registry service. Verisign evaluates usage based on peak performance objectives as well as current transaction volumes, which drive the quantity of servers in its implementations. Verisign's scaling is based on the following factors:

- Server configuration is based on CPU, memory, disk IO, total disk, and network throughput projections.
- Server quantity is determined through statistical modeling to fulfill overall performance objectives as defined by both the service availability and the server configuration.
- To ensure continuity of operations for the .web gTLD, Verisign uses a minimum of 100 dedicated servers per SRS site. These servers are virtualized to meet demand.

1.4 Description of Interconnectivity with Other Registry Systems

Figure 24-4 provides a technical overview of the Web.com's selected backend registry services provider's (Verisign's) SRS, showing how the SRS component fits into this larger system and interconnects with other system components.

1.5 Frequency of Synchronization Between Servers

As Web.com's selected provider of backend registry services, Verisign uses synchronous replication to keep the Verisign SRS continuously in sync between the two data centers. This synchronization is performed in near-real time, thereby supporting rapid failover should a failure occur or a planned maintenance outage be required.

1.6 Synchronization Scheme

Verisign uses synchronous replication to keep the Verisign SRS continuously in sync between the two data centers. Because the alternate-primary site is continuously up, and built using an identical design to the primary data center, it is classified as a "hot standby."

2 SCALABILITY AND PERFORMANCE ARE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

Verisign is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign's scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the .web gTLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain this gTLD. Verisign's pricing for the backend registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

3 TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

Verisign, Web.com's selected provider of backend registry services, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services provided to Web.com fully accounts for this personnel-related cost, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support SRS performance:

- Application Engineers: 19
- Database Administrators: 8
- Database Engineers: 3
- Network Administrators: 11
- Network Architects: 4
- Project Managers: 25
- Quality Assurance Engineers: 11
- SRS System Administrators: 13
- Storage Administrators: 4
- Systems Architects: 9

To implement and manage the .web gTLD as described in this application, Verisign, Web.com's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each

technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only the .web gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

4 EVIDENCE OF COMPLIANCE WITH SPECIFICATION 6 AND 10 TO THE REGISTRY AGREEMENT
Section 1.2 (EPP) of Specification 6, Registry Interoperability and Continuity Specifications. Verisign, Web.com's selected backend registry services provider, provides these services using its SRS, which complies fully with Specification 6, Section 1.2 of the Registry Agreement. In using its SRS to provide backend registry services, Verisign implements and complies with relevant existing RFCs (i.e., 5730, 5731, 5732, 5733, 5734, and 5910) and intends to comply with RFCs that may be published in the future by the Internet Engineering Task Force (IETF), including successor standards, modifications, or additions thereto relating to the provisioning and management of domain names that use EPP. In addition, Verisign's SRS includes a Registry Grace Period (RGP) and thus complies with RFC 3915 and its successors. Details of the Verisign SRS' compliance with RFC SRS/EPP are provided in the response to Question 25, Extensible Provisioning Protocol. Verisign does not use functionality outside the base EPP RFCs, although proprietary EPP extensions are documented in Internet-Draft format following the guidelines described in RFC 3735 within the response to Question 25. Moreover, prior to deployment, Web.com will provide to ICANN updated documentation of all the EPP objects and extensions supported in accordance with Specification 6, Section 1.2.

Specification 10, EPP Registry Performance Specifications. Verisign's SRS meets all EPP Registry Performance Specifications detailed in Specification 10, Section 2. Evidence of this performance can be verified by a review of the .com and .net Registry Operator's Monthly Reports, which Verisign files with ICANN. These reports detail Verisign's operational status of the .com and .net registries, which use an SRS design and approach comparable to the one proposed for the .web gTLD. These reports provide evidence of Verisign's ability to meet registry operation service level agreements (SLAs) comparable to those detailed in Specification 10. The reports are accessible at the following URL: http://www.icann.org/en/tlds/monthly-reports/.

In accordance with EPP Registry Performance Specifications detailed in Specification 10, Verisign's SRS meets the following performance attributes:
- EPP service availability: 〈= 864 minutes of downtime (˜98%)
- EPP session-command round trip time (RTT): 〈=4000 milliseconds (ms), for at least 90 percent of the commands
- EPP query-command RTT: 〈=2000 ms, for at least 90 percent of the commands
- EPP transform-command RTT: 〈=4000 ms, for at least 90 percent of the commands

25. Extensible Provisioning Protocol (EPP)

1 COMPLETE KNOWLEDGE AND UNDERSTANDING OF THIS ASPECT OF REGISTRY TECHNICAL REQUIREMENTS

Please note; all figures, tables and diagrams referenced in the following response can be found in the attachment titled "Attachment dot web Q25." All EPP schemas can be found in the attachment titled "Attachment dot web Q25 EPP schemas."

Verisign, Web.com Group, Inc.'s ("Web.com") selected backend registry services provider, has used Extensible Provisioning Protocol (EPP) since its inception and possesses complete

knowledge and understanding of EPP registry systems. Its first EPP implementation– for a thick registry for the .name generic top-level domain (gTLD)–was in 2002. Since then Verisign has continued its RFC-compliant use of EPP in multiple TLDs, as detailed in Figure 25-1.

Verisign's understanding of EPP and its ability to implement code that complies with the applicable RFCs is unparalleled. Mr. Scott Hollenbeck, Verisign's director of software development, authored the Extensible Provisioning Protocol and continues to be fully engaged in its refinement and enhancement (U.S. Patent Number 7299299 – Shared registration system for registering domain names). Verisign has also developed numerous new object mappings and object extensions following the guidelines in RFC 3735 (Guidelines for Extending the Extensible Provisioning Protocol). Mr. James Gould, a principal engineer at Verisign, led and co-authored the most recent EPP Domain Name System Security Extensions (DNSSEC) RFC effort (RFC 5910).

All registry systems for which Verisign is the registry operator or provides backend registry services use EPP. Upon approval of this application, Verisign will use EPP to provide the backend registry services for this gTLD. The .com, .net, and .name registries for which Verisign is the registry operator use an SRS design and approach comparable to the one proposed for this gTLD. Approximately 915 registrars use the Verisign EPP service, and the registry system performs more than 140 million EPP transactions daily without performance issues or restrictive maintenance windows. The processing time service level agreement (SLA) requirements for the Verisign-operated .net gTLD are the strictest of the current Verisign managed gTLDs. All processing times for Verisign-operated gTLDs can be found in ICANN's Registry Operator's Monthly Reports at http://www.icann.org/en/tlds/monthly-reports/.

Verisign has also been active on the Internet Engineering Task Force (IETF) Provisioning Registry Protocol (provreg) working group and mailing list since work started on the EPP protocol in 2000. This working group provided a forum for members of the Internet community to comment on Mr. Scott Hollenbeck's initial EPP drafts, which Mr. Hollenbeck refined based on input and discussions with representatives from registries, registrars, and other interested parties. The working group has since concluded, but the mailing list is still active to enable discussion of different aspects of EPP.

1.1 EPP Interface with Registrars

Verisign, Web.com's selected backend registry services provider, fully supports the features defined in the EPP specifications and provides a set of software development kits (SDK) and tools to help registrars build secure and stable interfaces. Verisign's SDKs give registrars the option of either fully writing their own EPP client software to integrate with the Shared Registration System (SRS), or using the Verisign-provided SDKs to aid them in the integration effort. Registrars can download the Verisign EPP SDKs and tools from the registrar website (http://www.Verisign.com/domain-name-services/current-registrars/epp-sdk/index.html).

The EPP SDKs provide a host of features including connection pooling, Secure Sockets Layer (SSL), and a test server (stub server) to run EPP tests against. One tool–the EPP tool– provides a web interface for creating EPP Extensible Markup Language (XML) commands and sending them to a configurable set of target servers. This helps registrars in creating the template XML and testing a variety of test cases against the EPP servers. An Operational Test and Evaluation (OT&E) environment, which runs the same software as the production system so approved registrars can integrate and test their software before moving into a live production environment, is also available.

2 TECHNICAL PLAN SCOPE/SCALE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

Verisign, Web.com's selected backend registry services provider, is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign's scaling models are proven predictors of needed capacity and related cost. As

such, they provide the means to link the projected infrastructure needs of the .web gTLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain the .web gTLD. Verisign's pricing for the backend registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

3 TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

Verisign, Web.com's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support the provisioning of EPP services:

- Application Engineers: 19
- Database Engineers: 3
- Quality Assurance Engineers: 11

To implement and manage the .web gTLD as described in this application, Verisign, Web.com's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only the .web gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and the .web gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

4 ABILITY TO COMPLY WITH RELEVANT RFCS

Verisign, Web.com's selected backend registry services provider, incorporates design reviews, code reviews, and peer reviews into its software development lifecycle (SDLC) to ensure compliance with the relevant RFCs. Verisign's dedicated QA team creates extensive test plans and issues internal certifications when it has confirmed the accuracy of the code in relation to the RFC requirements. Verisign's QA organization is independent from the development team within engineering. This separation helps Verisign ensure adopted

processes and procedures are followed, further ensuring that all software releases fully consider the security and stability of the .web gTLD.

For the .web gTLD, the Shared Registration System (SRS) complies with the following IETF EPP specifications, where the XML templates and XML schemas are defined in the following specifications:

- EPP RGP 3915 (http://www.apps.ietf.org/rfc/rfc3915.html): EPP Redemption Grace Period (RGP) Mapping specification for support of RGP statuses and support of Restore Request and Restore Report (authored by Verisign's Scott Hollenbeck)
- EPP 5730 (http://tools.ietf.org/html/rfc5730): Base EPP specification (authored by Verisign's Scott Hollenbeck)
- EPP Domain 5731 (http://tools.ietf.org/html/rfc5731): EPP Domain Name Mapping specification (authored by Verisign's Scott Hollenbeck)
- EPP Host 5732 (http://tools.ietf.org/html/rfc5732): EPP Host Mapping specification (authored by Verisign's Scott Hollenbeck)
- EPP Contact 5733 (http://tools.ietf.org/html/rfc5733): EPP Contact Mapping specification (authored by Verisign's Scott Hollenbeck)
- EPP TCP 5734 (http://tools.ietf.org/html/rfc5734): EPP Transport over Transmission Control Protocol (TCP) specification (authored by Verisign's Scott Hollenbeck)
- EPP DNSSEC 5910 (http://tools.ietf.org/html/rfc5910): EPP Domain Name System Security Extensions (DNSSEC) Mapping specification (authored by Verisign's James Gould and Scott Hollenbeck)

5 PROPRIETARY EPP EXTENSIONS

Verisign, Web.com's selected backend registry services provider, uses its SRS to provide registry services. The SRS supports the following EPP specifications, which Verisign developed following the guidelines in RFC 3735, where the XML templates and XML schemas are defined in the specifications:

- IDN Language Tag (http://www.verisigninc.com/assets/idn-language-tag.pdf): EPP internationalized domain names (IDN) language tag extension used for IDN domain name registrations
- RGP Poll Mapping (http://www.verisigninc.com/assets/whois-info-extension.pdf): EPP mapping for an EPP poll message in support of Restore Request and Restore Report
- Whois Info Extension (http://www.verisigninc.com/assets/whois-info-extension.pdf): EPP extension for returning additional information needed for transfers
- EPP ConsoliDate Mapping (http://www.verisigninc.com/assets/consolidate-mapping.txt): EPP mapping to support a Domain Sync operation for synchronizing domain name expiration dates
- NameStore Extension (http://www.verisigninc.com/assets/namestore-extension.pdf): EPP extension for routing with an EPP intelligent gateway to a pluggable set of backend products and services
- Low Balance Mapping (http://www.verisigninc.com/assets/low-balance-mapping.pdf): EPP mapping to support low balance poll messages that proactively notify registrars of a low balance (available credit) condition

As part of the 2006 implementation report to bring the EPP RFC documents from Proposed Standard status to Draft Standard status, an implementation test matrix was completed. Two independently developed EPP client implementations based on the RFCs were tested against the Verisign EPP server for the domain, host, and contact transactions. No compliance related issues were identified during this test, providing evidence that these extensions comply with RFC 3735 guidelines and further demonstrating Verisign's ability to design, test, and deploy an RFC-compliant EPP implementation.

5.1 EPP Templates and Schemas

The EPP XML schemas are formal descriptions of the EPP XML templates. They are used to express the set of rules to which the EPP templates must conform in order to be considered valid by the schema. The EPP schemas define the building blocks of the EPP templates, describing the format of the data and the different EPP commands' request and response formats. The current EPP implementations managed by Verisign, Web.com's selected backend registry services provider, use these EPP templates and schemas, as will the .web gTLD. For each proprietary XML template/schema Verisign provides a reference to the applicable template and includes the schema. These schema can be found in the attachment titled "dot web Q25 EPP Schemas."

6 PROPRIETARY EPP EXTENSION CONSISTENCY WITH REGISTRATION LIFECYCLE

Web.com's selected backend registry services provider's (Verisign's) proprietary EPP

extensions, defined in Section 5 above, are consistent with the registration lifecycle documented in the response to Question 27, Registration Lifecycle. Details of the registration lifecycle are presented in that response. As new registry features are required, Verisign develops proprietary EPP extensions to address new operational requirements. Consistent with ICANN procedures Verisign adheres to all applicable Registry Services Evaluation Process (RSEP) procedures.

26. Whois

1 COMPLETE KNOWLEDGE AND UNDERSTANDING OF THIS ASPECT OF REGISTRY TECHNICAL REQUIREMENTS

Please note; all figures, tables and diagrams referenced in the following response can be found in the attachment titled “Attachment dot web Q26.”

Verisign, Web.com Group, Inc.’s (”Web.com”) selected backend registry services provider, has operated the Whois lookup service for the gTLDs and ccTLDs it manages since 1991, and will provide these proven services for the .web gTLD registry. In addition, it continues to work with the Internet community to improve the utility of Whois data, while thwarting its application for abusive uses.

1.1 High-Level Whois System Description
Like all other components of Web.com’s selected backend registry services provider’s (Verisign’s) registry service, Verisign’s Whois system is designed and built for both reliability and performance in full compliance with applicable RFCs. Verisign’s current Whois implementation has answered more than five billion Whois queries per month for the TLDs it manages, and has experienced more than 250,000 queries per minute in peak conditions. The .web gTLD will use a Whois system design and approach that is comparable to the current implementation. Independent quality control testing ensures Verisign’s Whois service is RFC-compliant through all phases of its lifecycle.

Verisign’s redundant Whois databases further contribute to overall system availability and reliability. The hardware and software for its Whois service is architected to scale both horizontally (by adding more servers) and vertically (by adding more CPUs and memory to existing servers) to meet future need.

Verisign can fine-tune access to its Whois database on an individual Internet Protocol (IP) address basis, and it works with registrars to help ensure their services are not limited by any restriction placed on Whois. Verisign provides near real-time updates for Whois services for the TLDs under its management. As information is updated in the registration database, it is propagated to the Whois servers for quick publication. These updates align with the near real-time publication of Domain Name System (DNS) information as it is updated in the registration database. This capability is important for the .web gTLD registry as it is Verisign’s experience that when DNS data is updated in near real time, so should Whois data be updated to reflect the registration specifics of those domain names.

Verisign’s Whois response time has been less than 500 milliseconds for 95 percent of all Whois queries in .com, .net, .tv, and .cc. The response time in these TLDs, combined with Verisign’s capacity, enables the Whois system to respond to up to 30,000 searches (or queries) per second for a total capacity of 2.6 billion queries per day.

The Whois software written by Verisign complies with RFC 3912. Verisign uses an advanced in-memory database technology to provide exceptional overall system performance and security. In accordance with RFC 3912, Verisign provides a website at whois.nic.〈TLD〉 that provides free public query-based access to the registration data.

Verisign currently operates both thin and thick Whois systems.

Verisign commits to implementing a RESTful Whois service upon finalization of agreements with the IETF (Internet Engineering Task Force).

Provided Functionalities for User Interface

To use the Whois service via port 43, the user enters the applicable parameter on the command line as illustrated here:

- For domain name: whois EXAMPLE.TLD
- For registrar: whois ”registrar Example Registrar, Inc.”
- For name server: whois ”NS1.EXAMPLE.TLD” or whois ”name server (IP address)”

To use the Whois service via the web-based directory service search interface:

- Go to http://whois.nic.〈TLD〉
- Click on the appropriate button (Domain, Registrar, or Name Server)
- Enter the applicable parameter:
  - Domain name, including the TLD (e.g., EXAMPLE.TLD)
  - Full name of the registrar, including punctuation (e.g., Example Registrar, Inc.)
  - Full host name or the IP address (e.g., NS1.EXAMPLE.TLD or 198.41.3.39)
- Click on the Submit button.

Provisions to Ensure That Access Is Limited to Legitimate Authorized Users and Is in Compliance with Applicable Privacy Laws or Policies

To further promote reliable and secure Whois operations, Verisign, Web.com’s selected backend registry services provider, has implemented rate-limiting characteristics within the Whois service software. For example, to prevent data mining or other abusive behavior, the service can throttle a specific requestor if the query rate exceeds a configurable threshold. In addition, QoS technology enables rate limiting of queries before they reach the servers, which helps protect against denial of service (DoS) and distributed denial of service (DDoS) attacks.

Verisign’s software also permits restrictions on search capabilities. For example, wild card searches can be disabled. If needed, it is possible to temporarily restrict and/or block requests coming from specific IP addresses for a configurable amount of time. Additional features that are configurable in the Whois software include help files, headers and footers for Whois query responses, statistics, and methods to memory map the database. Furthermore, Verisign is European Union (EU) Safe Harbor certified and has worked with European data protection authorities to address applicable privacy laws by developing a tiered Whois access structure that requires users who require access to more extensive data to (i) identify themselves, (ii) confirm that their use is for a specified purpose and (iii) enter into an agreement governing their use of the more extensive Whois data.

1.2 Relevant Network Diagrams

Figure 26-1 provides a summary network diagram of the Whois service provided by Verisign, Web.com’s selected backend registry services provider. The figure details the configuration with one resolution/Whois site. For the .web gTLD Verisign provides Whois service from 6 of its 17 primary sites based on the proposed gTLD’s traffic volume and patterns. A functionally equivalent resolution architecture configuration exists at each Whois site.

1.3 IT and Infrastructure Resources

Figure 26-2 summarizes the IT and infrastructure resources that Verisign, Web.com’s selected backend registry services provider, uses to provision Whois services from Verisign primary resolution sites. As needed, virtual machines are created based on actual and projected demand.

1.4 Description of Interconnectivity with Other Registry Systems

Figure 26-3 provides a technical overview of the registry system provided by Verisign, Web.com’s selected backend registry services provider, and shows how the Whois service component fits into this larger system and interconnects with other system components.

1.5 Frequency of Synchronization Between Servers

Synchronization between the SRS and the geographically distributed Whois resolution sites occurs approximately every three minutes. Verisign, Web.com’s selected backend registry services provider, uses a two-part Whois update process to ensure Whois data is accurate and available. Every 12 hours an initial file is distributed to each resolution site. This file is a complete copy of all Whois data fields associated with each domain name under management. As interactions with the SRS cause the Whois data to be changed, these incremental changes are distributed to the resolution sites as an incremental file update.

This incremental update occurs approximately every three minutes. When the new 12-hour full update is distributed, this file includes all past incremental updates. Verisign's approach to frequency of synchronization between servers meets the Performance Specifications defined in Specification 10 of the Registry Agreement for new gTLDs.

2 TECHNICAL PLAN SCOPE/SCALE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

Verisign, Web.com's selected backend registry services provider, is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign's scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the .web gTLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain this gTLD. Verisign's pricing for the backend registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

3 TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

Verisign, Web.com's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support Whois services:

- Application Engineers: 19
- Database Engineers: 3
- Quality Assurance Engineers: 11

To implement and manage the .web gTLD as described in this application, Verisign, Web.com's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only the .web gTLD, Verisign

realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and the .web gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

4 COMPLIANCE WITH RELEVANT RFC

Web.com's selected backend registry services provider's (Verisign's) Whois service complies with the data formats defined in Specification 4 of the Registry Agreement. Verisign will provision Whois services for registered domain names and associated data in the top-level domain (TLD). Verisign's Whois services are accessible over Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6), via both Transmission Control Protocol (TCP) port 43 and a web-based directory service at whois.nic.〈TLD〉, which in accordance with RFC 3912, provides free public query-based access to domain name, registrar, and name server lookups. Verisign's proposed Whois system meets all requirements as defined by ICANN for each registry under Verisign management. Evidence of this successful implementation, and thus compliance with the applicable RFCs, can be verified by a review of the .com and .net Registry Operator's Monthly Reports that Verisign files with ICANN. These reports provide evidence of Verisign's ability to meet registry operation service level agreements (SLAs) comparable to those detailed in Specification 10. The reports are accessible at the following URL: http://www.icann.org/en/tlds/monthly-reports/.

5 COMPLIANCE WITH SPECIFICATIONS 4 AND 10 OF REGISTRY AGREEMENT

In accordance with Specification 4, Verisign, Web.com's selected backend registry services provider, provides a Whois service that is available via both port 43 in accordance with RFC 3912, and a web-based directory service at whois.nic.web also in accordance with RFC 3912, thereby providing free public query-based access. Verisign acknowledges that ICANN reserves the right to specify alternative formats and protocols, and upon such specification, Verisign will implement such alternative specification as soon as reasonably practicable.

The format of the following data fields conforms to the mappings specified in Extensible Provisioning Protocol (EPP) RFCs 5730 – 5734 so the display of this information (or values returned in Whois responses) can be uniformly processed and understood: domain name status, individual and organizational names, address, street, city, state/province, postal code, country, telephone and fax numbers, email addresses, date, and times.

Specifications for data objects, bulk access, and lookups comply with Specification 4 and are detailed in the following subsections, provided in both bulk access and lookup modes.

Bulk Access Mode. This data is provided on a daily schedule to a party designated from time to time in writing by ICANN. The specification of the content and format of this data, and the procedures for providing access, shall be as stated below, until revised in the ICANN Registry Agreement.

The data is provided in three files:

- Domain Name File: For each domain name, the file provides the domain name, server name for each name server, registrar ID, and updated date.
- Name Server File: For each registered name server, the file provides the server name, each IP address, registrar ID, and updated date.
- Registrar File: For each registrar, the following data elements are provided: registrar ID, registrar address, registrar telephone number, registrar email address, Whois server, referral URL, updated date, and the name, telephone number, and email address of all the registrar's administrative, billing, and technical contacts.

Lookup Mode. Figures 26-4 through Figure 26-6 provide the query and response format for domain name, registrar, and name server data objects.

5.1 Specification 10, RDDS Registry Performance Specifications

The Whois service meets all registration data directory services (RDDS) registry performance specifications detailed in Specification 10, Section 2. Evidence of this

performance can be verified by a review of the .com and .net Registry Operator's Monthly Reports that Verisign files monthly with ICANN. These reports are accessible from the ICANN website at the following URL: http://www.icann.org/en/tlds/monthly-reports/.

In accordance with RDDS registry performance specifications detailed in Specification 10, Verisign's Whois service meets the following proven performance attributes:

- RDDS availability: 〈=864 min of downtime (~98%)
- RDDS query RTT: 〈=2000 ms, for at least 95% of the queries
- RDDS update time: 〈=60 min, for at least 95% of the probes

6 SEARCHABLE WHOIS

Verisign, Web.com's selected backend registry services provider, provides a searchable Whois service for the .web gTLD. Verisign has experience in providing tiered access to Whois for the .name registry, and uses these methods and control structures to help reduce potential malicious use of the function. The searchable Whois system currently uses Apache's Lucene full text search engine to index relevant Whois content with near-real time incremental updates from the provisioning system.

Features of the Verisign searchable Whois function include:

- Provision of a web-based searchable directory service
- Ability to perform partial match, at least, for the following data fields: domain name, contacts and registrant's name, and contact and registrant's postal address, including all the sub-fields described in EPP (e.g., street, city, state, or province)
- Ability to perform exact match, at least, on the following fields: registrar ID, name server name, and name server's IP address (only applies to IP addresses stored by the registry, i.e., glue records)
- Ability to perform Boolean search supporting, at least, the following logical operators to join a set of search criteria: AND, OR, NOT
- Search results that include domain names that match the selected search criteria

Verisign's implementation of searchable Whois is EU Safe Harbor certified and includes appropriate access control measures that help ensure that only legitimate authorized users can use the service. Furthermore, Verisign's compliance office monitors current ICANN policy and applicable privacy laws or policies to help ensure the solution is maintained within compliance of applicable regulations. Features of these access control measures include:

- All unauthenticated searches are returned as thin results.
- Registry system authentication is used to grant access to appropriate users for thick Whois data search results.
- Account access is granted by the Web.com defined .web gTLD admin user.

Potential Forms of Abuse and Related Risk Mitigation. Leveraging its experience providing tiered access to Whois for the .name registry and interacting with ICANN, data protection authorities, and applicable industry groups, Verisign, Web.com's selected backend registry services provider, is knowledgeable of the likely data mining forms of abuse associated with a searchable Whois service. Figure 26-7 summarizes these potential forms of abuse and Verisign's approach to mitigate the identified risk.

27. Registration Life Cycle

1 COMPLETE KNOWLEDGE AND UNDERSTANDING OF REGISTRATION LIFECYCLES AND STATES

Please note; all figures, tables and diagrams referenced in the following response can be found in the attachment titled "Attachment dot web Q27."

Starting with domain name registration and continuing through domain name delete operations, Web.com Group, Inc.'s ("Web.com") selected backend registry services provider's (Verisign's) registry implements the full registration lifecycle for domain names

supporting the operations in the Extensible Provisioning Protocol (EPP) specification. The registration lifecycle of the domain name starts with registration and traverses various states as specified in the following sections. The registry system provides options to update domain names with different server and client status codes that block operations based on the EPP specification. The system also provides different grace periods for different billable operations, where the price of the billable operation is credited back to the registrar if the billable operation is removed within the grace period. Together Figure 27-1 and Figure 27-2 define the registration states comprising the registration lifecycle and explain the trigger points that cause state-to-state transitions. States are represented as green rectangles within Figure 27-1.

1.1 Registration Lifecycle of Create/Update/Delete

The following section details the create/update/delete processes and the related renewal process that Verisign, Web.com's selected backend registry services provider, follows. For each process, this response defines the process function and its characterization, and as appropriate provides a process flow chart.

Create Process. The domain name lifecycle begins with a registration or what is referred to as a Domain Name Create operation in EPP. The system fully supports the EPP Domain Name Mapping as defined by RFC 5731, where the associated objects (e.g., hosts and contacts) are created independent of the domain name.

Process Characterization. The Domain Name Create command is received, validated, run through a set of business rules, persisted to the database, and committed in the database if all business rules pass. The domain name is included with the data flow to the DNS and Whois resolution services. If no name servers are supplied, the domain name is not included with the data flow to the DNS. A successfully created domain name has the created date and expiration date set in the database. Creates are subject to grace periods as described in Section 1.3 of this response, Add Grace Period, Redemption Grace Period, and Notice Periods for Renewals or Transfers.

The Domain Name Create operation is detailed in Figure 27-3 and requires the following attributes:

- A domain name that meets the string restrictions.
- A domain name that does not already exist.
- The registrar is authorized to create a domain name in .web.
- The registrar has available credit.
- A valid Authorization Information (Auth-Info) value.
- Required contacts (e.g., registrant, administrative contact, technical contact, and billing contact) are specified and exist.
- The specified name servers (hosts) exist, and there is a maximum of 13 name servers.
- A period in units of years with a maximum value of 10 (default period is one year).

Renewal Process. The domain name can be renewed unless it has any form of Pending Delete, Pending Transfer, or Renew Prohibited.

A request for renewal that sets the expiry date to more than ten years in the future is denied. The registrar must pass the current expiration date (without the timestamp) to support the idempotent features of EPP, where sending the same command a second time does not cause unexpected side effects.

Automatic renewal occurs when a domain name expires. On the expiration date, the registry extends the registration period one year and debits the registrar account balance. In the case of an auto-renewal of the domain name, a separate Auto-Renew grace period applies. Renewals are subject to grace periods as described in Section 1.3 of this response, Add Grace Period, Redemption Grace Period, and Notice Periods for Renewals or Transfers.

Process Characterization. The Domain Name Renew command is received, validated, authorized, and run through a set of business rules. The data is updated and committed in the database if it passes all business rules. The updated domain name's expiration date is included in the flow to the Whois resolution service.

The Domain Name Renew operation is detailed in Figure 27-4 and requires the following

attributes:

- A domain name that exists and is sponsored by the requesting registrar.
- The registrar is authorized to renew a domain name in .web.
- The registrar has available credit.
- The passed current expiration date matches the domain name's expiration date.
- A period in units of years with a maximum value of 10 (default period is one year).

A domain name expiry past ten years is not allowed.

Registrar Transfer Procedures. A registrant may transfer his/her domain name from his/her current registrar to another registrar. The database system allows a transfer as long as the transfer is not within the initial 60 days, per industry standard, of the original registration date.

The registrar transfer process goes through many process states, which are described in detail below, unless it has any form of Pending Delete, Pending Transfer, or Transfer Prohibited.

A transfer can only be initiated when the appropriate Auth-Info is supplied. The Auth-Info for transfer is only available to the current registrar. Any other registrar requesting to initiate a transfer on behalf of a registrant must obtain the Auth-Info from the registrant.

The Auth-Info is made available to the registrant upon request. The registrant is the only party other than the current registrar that has access to the Auth-Info. Registrar transfer entails a specified extension of the expiry date for the object. The registrar transfer is a billable operation and is charged identically to a renewal for the same extension of the period. This period can be from one to ten years, in one-year increments.

Because registrar transfer involves an extension of the registration period, the rules and policies applying to how the resulting expiry date is set after transfer are based on the renewal policies on extension.

Per industry standard, a domain name cannot be transferred to another registrar within the first 60 days after registration. This restriction continues to apply if the domain name is renewed during the first 60 days. Transfer of the domain name changes the sponsoring registrar of the domain name, and also changes the child hosts (ns1.sample.xyz) of the domain name (sample .xyz).

The domain name transfer consists of five separate operations:

- Transfer Request (Figure 27-5): Executed by a non-sponsoring registrar with the valid Auth-Info provided by the registrant. The Transfer Request holds funds of the requesting registrar but does not bill the registrar until the transfer is completed. The sponsoring registrar receives a Transfer Request poll message.
- Transfer Cancel (Figure 27-6): Executed by the requesting registrar to cancel the pending transfer. The held funds of the requesting registrar are reversed. The sponsoring registrar receives a Transfer Cancel poll message.
- Transfer Approve (Figure 27-7): Executed by the sponsoring registrar to approve the Transfer Request. The requesting registrar is billed for the Transfer Request and the sponsoring registrar is credited for an applicable Auto-Renew grace period. The requesting registrar receives a Transfer Approve poll message.
- Transfer Reject (Figure 27-8): Executed by the sponsoring registrar to reject the pending transfer. The held funds of the requesting registrar are reversed. The requesting registrar receives a Transfer Reject poll message.
- Transfer Query (Figure 27-9): Executed by either the requesting registrar or the sponsoring registrar of the last transfer.

The registry auto-approves a transfer if the sponsoring registrar takes no action. The requesting registrar is billed for the Transfer Request and the sponsoring registrar is credited for an applicable Auto-Renew grace period. The requesting registrar and the sponsoring registrar receive a Transfer Auto-Approve poll message.

Delete Process. A registrar may choose to delete the domain name at any time.

Process Characterization. The domain name can be deleted, unless it has any form of Pending Delete, Pending Transfer, or Delete Prohibited.

A domain name is also prohibited from deletion if it has any in-zone child hosts that are name servers for domain names. For example, the domain name “sample.xyz” cannot be deleted if an in-zone host “ns.sample.xyz” exists and is a name server for “sample2.xyz.”

If the Domain Name Delete occurs within the Add grace period, the domain name is immediately deleted and the sponsoring registrar is credited for the Domain Name Create. If the Domain Name Delete occurs outside the Add grace period, it follows the Redemption grace period (RGP) lifecycle.

Update Process. The sponsoring registrar can update the following attributes of a domain name:

- Auth-Info
- Name servers
- Contacts (i.e., registrant, administrative contact, technical contact, and billing contact)
- Statuses (e.g., Client Delete Prohibited, Client Hold, Client Renew Prohibited, Client Transfer Prohibited, Client Update Prohibited)

Process Characterization. Updates are allowed provided that the update includes the removal of any Update Prohibited status. The Domain Name Update operation is detailed in Figure 27-10. A domain name can be updated unless it has any form of Pending Delete, Pending Transfer, or Update Prohibited.

1.2 Pending, Locked, Expired, and Transferred

Verisign, Web.com’s selected backend registry services provider, handles pending, locked, expired, and transferred domain names as described here. When the domain name is deleted after the five-day Add grace period, it enters into the Pending Delete state. The registrant can return its domain name to active any time within the five-day Pending Delete grace period. After the five-day Pending Delete grace period expires, the domain name enters the Redemption Pending state and then is deleted by the system. The registrant can restore the domain name at any time during the Redemption Pending state.

When a non-sponsoring registrar initiates the domain name transfer request, the domain name enters Pending Transfer state and a notification is mailed to the sponsoring registrar for approvals. If the sponsoring registrar doesn’t respond within five days, the Pending Transfer expires and the transfer request is automatically approved.

EPP specifies both client (registrar) and server (registry) status codes that can be used to prevent registry changes that are not intended by the registrant. Currently, many registrars use the client status codes to protect against inadvertent modifications that would affect their customers’ high-profile or valuable domain names.

Verisign’s registry service supports the following client (registrar) and server (registry) status codes:

- clientHold
- clientRenewProhibited
- clientTransferProhibited
- clientUpdateProhibited
- clientDeleteProhibited
- serverHold
- serverRenewProhibited
- serverTransferProhibited
- serverUpdateProhibited
- serverDeleteProhibited

1.3 Add Grace Period, Redemption Grace Period, and Notice Periods for Renewals or Transfers

Verisign, Web.com’s selected backend registry services provider, handles Add grace periods, Redemption grace periods, and notice periods for renewals or transfers as described here.

• Add Grace Period: The Add grace period is a specified number of days following the initial registration of the domain name. The current value of the Add grace period for all registrars is five days.
• Redemption Grace Period: If the domain name is deleted after the five-day grace period expires, it enters the Redemption grace period and then is deleted by the system. The registrant has an option to use the Restore Request command to restore the domain name within the Redemption grace period. In this scenario, the domain name goes to Pending Restore state if there is a Restore Request command within 30 days of the Redemption grace period. From the Pending Restore state, it goes either to the OK state, if there is a Restore Report Submission command within seven days of the Restore Request grace period, or a Redemption Period state if there is no Restore Report Submission command within seven days of the Restore Request grace period.
• Renew Grace Period: The Renew/Extend grace period is a specified number of days following the renewal/extension of the domain name's registration period. The current value of the Renew/Extend grace period is five days.
• Auto-Renew Grace Period: All auto-renewed domain names have a grace period of 45 days.
• Transfer Grace Period: Domain names have a five-day Transfer grace period.

1.4 Aspects of the Registration Lifecycle Not Covered by Standard EPP RFCs
Web.com's selected backend registry services provider's (Verisign's) registration lifecycle processes and code implementations adhere to the standard EPP RFCs related to the registration lifecycle. By adhering to the RFCs, Verisign's registration lifecycle is complete and addresses each registration-related task comprising the lifecycle. No aspect of Verisign's registration lifecycle is not covered by one of the standard EPP RFCs and thus no additional definitions are provided in this response.

2 CONSISTENCY WITH ANY SPECIFIC COMMITMENTS MADE TO REGISTRANTS AS ADAPTED TO THE OVERALL BUSINESS APPROACH FOR THE PROPOSED gTLD
The registration lifecycle described above applies to the .web gTLD as well as other TLDs managed by Verisign, Web.com's selected backend registry services provider; thus Verisign remains consistent with commitments made to its registrants. No unique or specific registration lifecycle modifications or adaptations are required to support the overall business approach for the .web gTLD.

To accommodate a range of registries, Verisign's registry implementation is capable of offering both a thin and thick Whois implementation, which is also built upon Verisign's award-winning ATLAS infrastructure.

3 COMPLIANCE WITH RELEVANT RFCs
Web.com's selected backend registry services provider's (Verisign's) registration lifecycle complies with applicable RFCs, specifically RFCs 5730 – 5734 and 3915. The system fully supports the EPP Domain Name Mapping as defined by RFC 5731, where the associated objects (e.g., hosts and contacts) are created independent of the domain name.

In addition, in accordance with RFCs 5732 and 5733, the Verisign registration system enforces the following domain name registration constraints:

• Uniqueness/Multiplicity: A second-level domain name is unique in the .web database. Two identical second-level domain names cannot simultaneously exist in .web. Further, a second-level domain name cannot be created if it conflicts with a reserved domain name.
• Point of Contact Associations: The domain name is associated with the following points of contact. Contacts are created and managed independently according to RFC 5733.
• Registrant
• Administrative contact
• Technical contact
• Billing contact
• Domain Name Associations: Each domain name is associated with:
• A maximum of 13 hosts, which are created and managed independently according to RFC 5732
• An Auth-Info, which is used to authorize certain operations on the object
• Status(es), which are used to describe the domain name's status in the registry
• A created date, updated date, and expiry date

4 DEMONSTRATES THAT TECHNICAL RESOURCES REQUIRED TO CARRY THROUGH THE PLANS FOR THIS

ELEMENT ARE ALREADY ON HAND OR READILY AVAILABLE

Verisign, Web.com's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for the .web gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support the registration lifecycle:

- Application Engineers: 19
- Customer Support Personnel: 36
- Database Administrators: 8
- Database Engineers: 3
- Quality Assurance Engineers: 11
- SRS System Administrators: 13

To implement and manage the .web gTLD as described in this application, Verisign, Web.com's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only the .web gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and the .web gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

28. Abuse Prevention and Mitigation

1. COMPREHENSIVE ABUSE POLICIES, WHICH INCLUDE CLEAR DEFINITIONS OF WHAT CONSTITUTES ABUSE IN THE TLD, AND PROCEDURES THAT WILL EFFECTIVELY MINIMIZE POTENTIAL FOR ABUSE IN THE TLD

Please note; all figures, tables and diagrams referenced in the following response can be found in the attachment titled "Attachment dot web Q28."

Web.com Group, Inc ("Web.com") has been in the business of helping our near 3 million

customers establish their online presences for over 15 years. As such, we have a rich history of understanding the importance of abuse prevention and mitigation as a core objective. We are active participants in a variety of industry and government efforts to prevent domain name abuse and are constantly updating our operating procedures to ensure our customers are as protected from this type of activity as they can be.

The .web gTLD will help customers launch and leverage their presence on the World Wide Web. As a leading global provider of online marketing services to small businesses, Web.com recognizes that finding a relevant and memorable domain name can be challenging. Since many keywords and descriptive phrases associated with existing gTLDs have already been registered, it is difficult to pinpoint a domain name which contains a limited number of characters. Consequently, prospective registrants are often unable to secure a unique name. Regularly, in the .com space amongst others, this is because of exploitative or abusive registrations. In the forthcoming .web namespace, we will endeavor to the utmost of our ability to prevent this pattern from repeating.

One of the most important reasons our customers choose Web.com is because of our reputation for great products and exceptional customer service. The .web gTLD is a natural extension of our business. It is a place where we can help customers be successful on the web. At Web.com, we believe that a website is only as good as the services and support behind it. With the .web gTLD, we have the chance to bring this same commitment to service and support to a gTLD. For companies and consumers who stake their reputation on a .web domain name, having a gTLD that is trusted and secure is critical.

Unfortunately, some of the current gTLDs are not operated in a manner that instills this level of confidence. Web.com hopes to make the .web gTLD different. In launching the .web gTLD we have put together a tapestry of efforts that seek to prevent and successfully mitigate domain name abuse, making the web a more accessible and friendly place for small and medium sized businesses as well as consumers. These efforts include:

- An acceptable use policy that clearly defines what is considered abuse and what registrants may and may not do with their domain names
- A seasoned abuse mitigation team that has years of experience in dealing with these issues
- Technological Measures for Removal of Orphan Glue Records
- Efforts and measures to promote accurate and complete Whois
- Requirements for .web accredited registrars to enact measures in support of these efforts

The fight against abusive behavior is not static and Web.com is committed to ensuring that our efforts are constantly evolving to meet the ever changing landscape of threats.

1.1 .web Abuse Prevention and Mitigation Implementation Plan

Preventing domain name abuse in the .web gTLD is of critical importance to registrants, consumers and Web.com. To demonstrate our commitment to make the .web gTLD more resistant to abusive behavior than just about any other gTLD that currently exists, Web.com has explored various mechanisms to help prevent abusive registrations. We were particularly impressed with the set of 31 Proposed Security, Stability and Resiliency Requirements for Financial TLDs that were developed by the Security Standards Working Group (SSWG) under the guidance of the financial services industry. Following their recommendation that all potential applicants look at these standards for their own TLDs, Web.com has completed a thorough review to determine which might enhance the .web gTLD experience. While not all of the proposed standards are applicable to the .web gTLD, we will endeavor to implement several of them to aid in our efforts to prevent and mitigate abusive registrations.

Web.com has developed and will look to deploy a customized approach that seeks to minimize the potential for abusive registrations and mitigate them as soon as possible should they occur. Registrants, Registrars and the Registry will all play a role in this endeavor. Having all three levels of the .web gTLD ecosystem participate in these measures will help ensure a comprehensive approach to these critical objectives. Web.com has designed the following procedure to prevent and mitigate abusive registrations:

Acceptable Use Policy - Web.com has developed a draft Acceptable Use Policy (AUP) which can be found in ”Attachment dot web Q28.” This AUP clearly defines what is considered abuse and

what type of behavior is expressly prohibited in conjunction with the use of a .web domain name. Web.com will require, through the Registry Registrar Agreement (RRA), that this AUP be included in the registration agreement used by all .web gTLD accredited registrars. This registration agreement must be accepted by a registrant prior to them being able to register a name in the .web gTLD.

Annual Certification of Registrar compliance with Registry-Registrar Agreement. The self-certification program consists, in part, of evaluations applied equally to all operational .web gTLD accredited registrars and conducted from time to time throughout the year. Process steps are as follows:

- Web.com sends an email notification to the ICANN primary registrar contact, requesting that the contact go to a designated URL, log in with his/her Web ID and password, and complete and submit the online form. The contact must submit the form within 15 business days of receipt of the notification.
- When the form is submitted, Web.com sends the registrar an automated email confirming that the form was successfully submitted.
- Web.com reviews the submitted form to ensure the certifications are compliant.
- Web.com sends the registrar an email notification if the registrar is found to be compliant in all areas.
- If a review of the response indicates that the registrar is out of compliance or if Web.com has follow-up questions, the registrar has 10 days to respond to the inquiry.
- If the registrar does not respond within 15 business days of receiving the original notification, or if it does not respond to the request for additional information, Web.com sends the registrar a Breach Notice and gives the registrar 30 days to cure the breach.
- If the registrar does not cure the breach, Web.com terminates the Registry-Registrar Agreement (RRA).

The .web gTLD registry will provide and maintain a primary point of contact for abuse complaints. We will display the contact information for the Abuse Mitigation Team, which serves as the primary point of contact for reporting abuse within the .web gTLD, on the .web gTLD website.

Each .web gTLD accredited registrar will provide and maintain a primary point of contact for abuse complaints. The registrar must provide and maintain valid primary contact information for reporting abuse in the .web gTLD on their website. This will be required as part of the .web gTLD RRA.

Web.com will explicitly define for Registrars what constitutes abusive behavior including but not limited to, malicious, negligent, and reckless behavior. The definition of abusive behavior will be contained in the AUP that Registrars will be required to include as part of the Registration Agreement. This will be required as part of the .web gTLD RRA.

Registrar must notify Registry Operator immediately regarding any investigation or compliance action including the nature of the investigation or compliance action by ICANN or any outside party (e.g., law enforcement, etc.), along with the TLD impacted. This will be required as part of the .web gTLD RRA.

Development of an Abuse Prevention and Mitigation Working Group. To give the Web.com team alternate perspectives about handling incidents of abuse and ways to mitigate them, we will form an Abuse Prevention and Mitigation Working Group. This team will not only be comprised of a cross functional group of Web.com professionals but also look to involve representatives from law enforcement, our customer base and outside experts. The group would meet regularly to discuss the latest trends in domain name abuse and the most effective way to prevent and remedy them.

1.2 Policies for Handling Complaints Regarding Abuse

Web.com will staff a Single Point of Contact (SPoC) Abuse team to address abuse and malicious use requests. The role of the abuse team is to monitor registry services and review complaints entered online by end users, customers, and/or Law Enforcement. The complaints will be managed in accordance with the applicable Acceptable Use Policy (AUP) and Terms of Service (TOS) which shall allow the Abuse team discretion to suspend a domain instantly or send the complaint through the appropriate escalation channel for complaint resolution.

Complaints shall be received via email at abuse@registry.web as will be prominently provided on the .web website (http://registry.web). Registrar access to .web's Abuse Team will be provided via a hotline number, email address and additional personnel for filing direct requests. Complaints may be submitted 24x7 and each request path requires the submitter to provide personal contact information. .web will acknowledge the complaint within one (1) business day and will provide the requestor acceptance and/or resolution within three (3) business days depending on severity and complexity of the complaint.

Web.com views domain name abuse as a serious matter that produces direct harm to Internet users and .web customers. As such, .web will handle each abuse complaint as a direct threat and intends to resolve each validated complaint with a sense of urgency. Our Abuse Policies recognize many forms of abuse related to the registrations and use of domain names. Abuses and their respective mitigation strategy listed here is not an exhaustive list, but is meant to highlight general process and procedure by which .web will manage the most common forms of abuse. The .web Abuse Team collaborates and participates with industry experts and forums to understand the latest forms of abuse in an attempt to protect customers of our services and Internet users where possible.

DRAFT ABUSE REMEDY PROCESS

Listed here is the proposed process for dealing with the major forms of domain abuse:

1. Customer or end user submits abuse complaint to abuse@registry.web;
2. Abuse Coordinator receives request and acknowledges receipt of complaint;
3. Abuse Coordinator analyzes request to determine the abuse type to be addressed and references the .web knowledgebase for detailed procedures;
4. Abuse Coordinator assigns a severity rating based on complaint type;
5. Abuse Coordinator resolves the complaint based on the following decision tree:
   a. Is the request a court ordered seizure and transfer?
      i. Yes – See section 28.1.1
      ii. No - next step
   b. Does the request reflect a potential DDOS Attack?
      i. Yes – See section 28.1.2
      ii. No - next step
   c. Is the request a phishing complaint?
      i. Yes – See section 28.1.3
      ii. No - next step
   d. Is the complaint a notice of a trademark infringement?
      i. Yes – See section 28.1.4
      ii. No - next step
   e. Is the request a possible hijacking case or a transfer dispute?
      i. Yes – See section 28.1.5
      ii. No - next step
   f. Is the request an email service abuse?
      i. Yes – See section 28.1.6
      ii. No - next step
   g. Does the complaint refer to abusive or offensive content hosted on a .web domain?
      i. Yes – See section 28.1.7
      ii. No - next step
   h. For all other abuses not defined:
      i. Escalate request to Abuse Manager for guidance and resolution

28.1.1 Court Ordered Seizure and Transfer

Definition: Law enforcement via a court of legal jurisdiction orders that domain be seized due to illegal activity of applicable law.

Service Level: One (1) business day

Procedure:

- Abuse Coordinator contacts the legal jurisdiction to request signed copies of the court order;
- Upon receipt of court order, Abuse Coordinator confirms request with the Abuse

Situation Manager;
- If the request is determined to be valid, Abuse Coordinator will submit a request to the Registry Support team to have the domain pushed to the requested registrar as directed by the applicable judicial entity;
- If the request is determined to be invalid or documents submitted are in question, the Abuse Coordinator will contact the legal jurisdiction requesting the appropriate documentation or to provide reasoning as to why the request cannot be fulfilled.

28.1.2 DOS or DDOS Attack

Definition: A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer or network resource unavailable to its intended users.

Service Level: One (1) business day

Procedure:
- Abuse Coordinator will confirm the DDOS attack with the Abuse Manager;
- If the complaint is confirmed as a DDOS attack:
  - Abuse Coordinator will escalate the request to the respective Registrar Support Team;
  - If not , Abuse Coordinator will respond to the complainant as unable to confirm and request additional information or close the complaint;
- Registrar Support team will suspend the domain registration until further notice.

28.1.3 Phishing

Definition: Phishing is a website fraudulently presenting itself as a trusted site (often a bank) in order to deceive Internet users into divulging sensitive information (e.g. online banking credentials, email passwords).

Service Level: One (1) business day

Procedure:
- Abuse Coordinator will confirm the phishing scam with the Abuse Manager;
- If the complaint is confirmed as a legitimate phishing event;
  - Abuse Coordinator will escalate the request to the Registry Support Team;
  - If not , Abuse Coordinator will respond to the complainant as unable to confirm and request additional information or close the complaint;
- Registry Support Team will immediately suspend the domain;
- Abuse Manager will investigate the Phish event and determine the intent of the domain registrant, the Registry Support team seize and/or delete the domain from the zone.

28.1.4 Cybersquatting / Trademark Infringement

Definition: Cybersquatting is the deliberate and bad-faith registration and use of a name that is a registered brand or mark of an unrelated entity, often for the purpose of profiting (typically, though not exclusively, through pay-per-click advertisements).

Service Level: Three (3) business days

Procedure:
- If request appears to be an initial complaint on a possible infringement, Abuse Coordinator will direct complainant to the UDRP/WIPO process;
- If not , if the request of transfer is from a .web registrar, Abuse Coordinator will work with the Registrar to ensure the domain in question is transferred appropriately.

28.1.5 Transfer Disputes / Hijacking

Definition: Domain hijacking or domain theft is the act of changing the registration of a domain name without the permission of its original registrant.

Service Level: Three (3) business days

Procedure:
• Abuse Coordinator will confirm the OFAC request with the Abuse Manager;
• Abuse Coordinator will escalate request to and Registrar shall internal policies and procedures to investigate the transfer.

28.1.6 Email Service Abuse

Definition: An illegitimate use of email systems to distribute abusive content or in a manner that violates the Acceptable Use Policy. Examples of this abuse are Un-Solicited Commercial Email (UCE/SPAM).

Service Level: Three (3) business days

Procedure:
• Abuse Coordinator will validate the complaint for UCE/SPAM elements and collaborate with the Complainant to acquire the examples of the offensive material;
• If Abuse Coordinator deems the offensive material to violate Acceptable Use Policy and is deemed to be offensive material, Abuse Coordinator will escalate the request to the Registry Support team for suspension;
• Registry Support team will immediately suspend the domain;
• If a .web customer is found to be unknowingly sending UCE, Customer shall be allotted the opportunity to correct the situation and assurances must be received by offender to ensure against future occurrences.

28.1.7 Web Hosting Abuse

Definition: Content or material hosted on a website that that is deemed to be offensive or against the .web Acceptable Use Policy. Material that is deemed offensive by registrar/host shall result in a Warning, then Suspension if material is not removed and possible seizure or termination of services.

Service Level: Three (3) business days

Procedure:
• Abuse Coordinator will validate the information in the complaint to confirm that the hosting package is being used in a way that is not compliant with the .web Acceptable Use Policy. Some examples may include the following:
  o Documents, videos, pictures, music files, software etc. is not associated with the function or serving up of website;
  o Content being stored is not accessible from the Website;
  o An open FTP server;
  o Storage being used as a hard drive/backup; or
  o Space Manager usage exceeds 2GB of storage on the UNIX hosting platform only.
• If one or more of the above is confirmed and validated, the Abuse Coordinator or Technical Services will notify the Customer that they are in violation of the .web AUP and/or Terms of Service;
• An email will be sent immediately to the Registrant, Admin and Technical contact on file to advise of the violation. The email should instruct the Customer to take the appropriate action within 24 hours to remove the offending content or they may be subjected to a suspension of services;
• During Business Hours, the Abuse Coordinator will contact the Customer via phone in addition to sending the email to inform the Registrant, Admin or Technical contacts of the offending violation. The Technical Services agents will follow the same process for After Hours handling;
• If no response is received within 24 hours, a second phone and email attempt will be made to reach the Registrant, Admin and Technical contact;
• If the offending party does not respond by the end of the second business day, action will be taken to remove the offending content that is causing server degradation;
• Technical Support team will suspend the Hosting services;
• The Registry Support team will place the domain on Registrar hold to de-resolve the name;
• If the offending party responds and agrees to remove the offending content within the 24 hour time frame, the Abuse Coordinator or Technical Services agent must confirm the material has been removed, and note the appropriate remediation within the CRM system;
• If the offending party responds and agrees to remove the offending content after

the service suspension, the Registry Support team may remove the suspension and allow customer to remove the content. Support will confirm the offending material has been removed, and note the appropriate CRM systems;

- If the offending party requests that .web remove the offending material, the Abuse Coordinator agent must call the Customer and obtain confirmation to remove the content on behalf of the Customer. The Abuse Coordinator will also obtain written confirmation from the Customer via the Registrant, Administrative or Technical Contacts that are listed. The confirmation should be noted in the appropriate CRM system;
- If there is no response from the offending party after 7 Days, the Abuse Coordinator will submit a request to delete the offending content from the servers to the Abuse Manager for approval to delete the content;
- Prior to deleting the content, an email will be sent to the appropriate internal Legal point of contact to advise of the issue and obtain approval to delete the content.

1.3 Proposed Measures for Removal of Orphan Glue Records

Although orphan glue records often support correct and ordinary operation of the Domain Name System (DNS), registry operators will be required to remove orphan glue records (as defined at http://www.icann.org/en/committees/security/sac048.pdf) when provided with evidence in written form that such records are present in connection with malicious conduct. Web.com's selected backend registry services provider's registration system is specifically designed to not allow orphan glue records. Registrars are required to delete/move all dependent DNS records before they are allowed to delete the parent domain.

To prevent orphan glue records, Verisign, Web.com's chosen backend registry services provider, performs the following checks before removing a domain or name server:

Checks during domain delete:

- Parent domain delete is not allowed if any other domain in the zone refers to the child name server.
- If the parent domain is the only domain using the child name server, then both the domain and the glue record are removed from the zone.

Check during explicit name server delete:

- Verisign confirms that the current name server is not referenced by any domain name (in-zone) before deleting the name server.

Zone-file impact:

- If the parent domain references the child name server AND if other domains in the zone also reference it AND if the parent domain name is assigned a serverHold status, then the parent domain goes out of the zone but the name server glue record does not.
- If no domains reference a name server, then the zone file removes the glue record.

1.4 Resourcing Plans

Details related to resourcing plans for the initial implementation and ongoing maintenance of Web.com's abuse plan are provided in Section 2 of this response.

1.5 Measures to Promote Whois Accuracy

Web.com supports efforts to improve the accuracy and completeness of Whois records. To that end, we will seek to implement a series of measures that require registrars and registrants to help us in this pursuit. This includes a Whois reminder process at the registry level, regular scans of the Whois data to search for blank or incomplete data and economic incentives for registrars who achieve 100% complete and accurate Whois data for those names they have registered.

Regular Monitoring of Registration Data for Accuracy and Completeness

Whois data reminder process. Verisign regularly reminds registrars of their obligation to comply with ICANN's Whois Data Reminder Policy, which was adopted by ICANN as a consensus policy on 27 March 2003 (http://www.icann.org/en/registrars/wdrp.htm). Verisign sends a notice to all registrars once a year reminding them of their obligation to be diligent in validating the Whois information provided during the registration process, to investigate claims of fraudulent Whois information, and to cancel domain name registrations for which

Whois information is determined to be invalid.

Bi-Annual Whois Verification by Registrars. As will be required in the Registry-Registrar Agreement, all .web accredited registrars will be required to verify Whois data for each record they have registered in the TLD twice a year. Verification can take place via email, phone or any other methods as long as there is a proactive action by the registrant to confirm the accuracy of the Whois data associated with the domain name. Web.com will randomly audit Whois records to ensure compliance and accuracy. As part of the .web gTLD Abuse reporting system, users can report missing or incomplete Whois data via the registry website.

Quarterly Scan of the Zone file for incomplete Registrant Data. On a quarterly basis, Web.com will do a scan of all Whois records in the .web gTLD to find any blank fields or missing registration data. Upon completion of the scan, registrars will be sent a report detailing which domain names are missing data. As part of their responsibilities in the RAA to work towards 100% accuracy of Whois data, registrars must then alert registrants that there is data missing in their Whois record and remind them of their responsibility contained in the registration agreement that they must comply with ICANN requirements for complete and accurate Whois data.

Economic incentives for Registrars to achieve 100% Whois Accuracy

Web.com will offer Market Development Funds (MDF) to those registrars who can demonstrate via a third party audit that the .web gTLD names registered with them have 100% complete and accurate Whois data.

1.6 Malicious or Abusive Behavior Definitions, Metrics, and Service Level Requirements for Resolution

Web.com defines Malicious and Abusive behavior based on the following but not limited definitions:

Phishing is a criminal activity employing tactics to defraud and defame Internet users via sensitive information with the intent to steal or expose credentials, money or identities. A phishing attack begins with a spoofed email posing as a trustworthy electronic correspondence that contains hijacked brand names i.e. (financial institutions, credit card companies, e-commerce sites). The language of a phishing email is misleading and persuasive by generating either fear and/or excitement to ultimately lure the recipient to a fraudulent website. It is paramount for both the phishing email and website to appear credible in order for the attack to influence the recipient. As with the spoofed email, phishers aim to make the associated phishing website appear credible. The legitimate target website is mirrored to make the fraudulent site look professionally designed. Fake third-party security endorsements, spoofed address bars, and spoofed padlock icons falsely lend credibility to fraudulent sites as well. The persuasive inflammatory language of the email combined with a legitimate looking website is used to convince recipients to disclose sensitive information such as passwords, usernames, credit card numbers, social security numbers, account numbers, and mother’s maiden name.

Malware is malicious software that was intentionally developed to infiltrate or damage a computer, mobile device, software and/or operating infrastructure or website without the consent of the owner or authorized party. This includes, amongst others, Viruses, Trojan horses, and worms.

Domain Name or Domain Theft is the act of changing the registration of a domain name without the permission of its original registrant.
Section 1.2 outlines the Web.com Policies and Procedures for Handling Complaints Regarding Abuse as defined above.

As pertains to Web.com performance metrics and service level requirements for resolution, we adhere to a 12 hour timeframe to address and potentially rectify the issue as it pertains to all forms of abuse and fraud. Once a notification is received via email, call center or fax, the Web.com Customer Service centers immediately create a support ticket in order to monitor and track the issue through resolution. If notifications are received during normal business hours (8am – 11pm EST. (Monday – Friday) and 8am – 6pm EST (Saturday & Sunday) the majority of issues are resolved in less than a 4 hour period.

1.7 Controls to Ensure Proper Access to Domain Functions

To ensure proper access to domain functions, Web.com incorporates Verisign's Registry-Registrar Two-Factor Authentication Service into its full-service registry operations. The service is designed to improve domain name security and assist registrars in protecting the accounts they manage by providing another level of assurance that only authorized personnel can communicate with the registry. As part of the service, dynamic one-time passwords (OTPs) augment the user names and passwords currently used to process update, transfer, and/or deletion requests. These one-time passwords enable transaction processing to be based on requests that are validated both by "what users know" (i.e., their user name and password) and "what users have" (i.e., a two-factor authentication credential with a one-time-password).

Registrars can use the one-time-password when communicating directly with Verisign's Customer Service department as well as when using the registrar portal to make manual updates, transfers, and/or deletion transactions. The Two-Factor Authentication Service is an optional service offered to registrars that execute the Registry-Registrar Two-Factor Authentication Service Agreement. As shown in Figure 28-1, the registrars' authorized contacts use the OTP to enable strong authentication when they contact the registry. There is no charge for the Registry-Registrar Two-Factor Authentication Service. It is only enabled for registrars that wish to take advantage of the added security provided by the service.

2. TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

Resource Planning

Web.com is a leading provider of Internet services for small to medium-sized businesses (SMBs). Web.com is the parent company of two global domain name registrars and further meets the Internet needs of SMBs throughout their lifecycle with affordable value added services that including domain name registration, website design, search engine optimization, search engine marketing, social media and mobile products, local sales leads, eCommerce solutions and call center services. Headquartered in Jacksonville, FL, USA, Web.com is NASDAQ traded company serving nearly three million customers with more than 1,700 global employees in fourteen locations in North America, South America and the United Kingdom.

Our business is helping people establish, maintain, promote, and optimize their web presence. Web.com intentionally chose Verisign as our registry services provider because of their unsurpassed track record in operating some of the world's most complex and critical top level domains. Verisign's support for the .web gTLD will help ensure its success

The .web gTLD will be fully supported by a cross function team of Web.com professionals. Numbers and types of employees will vary for each function but Web.com projects it will use the following personnel to support the resource planning requirements:

- Quality Assurance Engineer: 0.5 FTE
- System Administrator: 1 FTE
- Database Administrator: 0.5 FTE
- Technical Project Manager: 0.5 FTE
- Marketing Director: 1 FTE
- Sales Manager: 1 FTE
- Legal Counsel: 1 FTE
- Finance/Accounting: 1 FTE
- Customer Service: 2 FTEs

Resource Planning Specific to Backend Registry Activities

Verisign, Web.com's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These

models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of
Proposed Registry, to support abuse prevention and mitigation:

- Application Engineers: 19
- Business Continuity Personnel: 3
- Customer Affairs Organization: 9
- Customer Support Personnel: 36
- Information Security Engineers: 11
- Network Administrators: 11
- Network Architects: 4
- Network Operations Center (NOC) Engineers: 33
- Project Managers: 25
- Quality Assurance Engineers: 11
- Systems Architects: 9

To implement and manage the Web.com .web gTLD as described in this application, Verisign, Web.com's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only this proposed gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

3. POLICIES AND PROCEDURES IDENTIFY AND ADDRESS THE ABUSIVE USE OF REGISTERED NAMES AT STARTUP AND ON AN ONGOING BASIS

3.1 Start-Up Anti-Abuse Policies and Procedures

Verisign, Web.com's selected backend registry services provider, provides the following domain name abuse prevention services, which Web.com incorporates into its full-service registry operations. These services are available at the time of domain name registration.

Registry Lock. The Registry Lock Service allows registrars to offer server-level protection for their registrants' domain names. A registry lock can be applied during the initial standup of the domain name or at any time that the registry is operational.

Specific Extensible Provisioning Protocol (EPP) status codes are set on the domain name to

prevent malicious or inadvertent modifications, deletions, and transfers. Typically, these ‘server’ level status codes can only be updated by the registry. The registrar only has ‘client’ level codes and cannot alter ‘server’ level status codes. The registrant must provide a pass phrase to the registry before any updates are made to the domain name. However, with Registry Lock, provided via Verisign, Web.com’s subcontractor, registrars can also take advantage of server status codes.

The following EPP server status codes are applicable for domain names: (i) serverUpdateProhibited, (ii) serverDeleteProhibited, and (iii) serverTransferProhibited. These statuses may be applied individually or in combination.

The EPP also enables setting host (i.e., name server) status codes to prevent deleting or renaming a host or modifying its IP addresses. Setting host status codes at the registry reduces the risk of inadvertent disruption of DNS resolution for domain names.

The Registry Lock Service is used in conjunction with a registrar’s proprietary security measures to bring a greater level of security to registrants’ domain names and help mitigate potential for unintended deletions, transfers, and/or updates.

Two components comprise the Registry Lock Service:

- Web.com and/or its registrars provides Verisign, the provider of backend registry services, with a list of the domain names to be placed on the server status codes. During the term of the service agreement, the registrar can add domain names to be placed on the server status codes and/or remove domain names currently placed on the server status codes. Verisign then manually authenticates that the registrar submitting the list of domain names is the registrar of record for such domain names.
- If Web.com and/or its registrars requires changes (including updates, deletes, and transfers) to a domain name placed on a server status code, Verisign follows a secure, authenticated process to perform the change. This process includes a request from a Web.com-authorized representative for Verisign to remove the specific registry status code, validation of the authorized individual by Verisign, removal of the specified server status code, registrar completion of the desired change, and a request from the Web.com-authorized individual to reinstate the server status code on the domain name. This process is designed to complement automated transaction processing through the Shared Registration System (SRS) by using independent authentication by trusted registry experts.

Web.com intends to charge registrars based on the market value of the Registry Lock Service. A tiered pricing model is expected, with each tier having an annual fee based on per domain name/host and the number of domain names and hosts to be placed on Registry Lock server status code(s).

3.2 Ongoing Anti-Abuse Policies and Procedures

3.2.1 Policies and Procedures That Identify Malicious or Abusive Behavior

Verisign, Web.com’s selected backend registry services provider, provides the following service to Web.com for incorporation into its full-service registry operations.

Malware scanning service. Registrants are often unknowing victims of malware exploits. Verisign has developed proprietary code to help identify malware in the zones it manages, which in turn helps registrars by identifying malicious code hidden in their domain names.

Verisign’s malware scanning service helps prevent websites from infecting other websites by scanning web pages for embedded malicious content that will infect visitors’ websites. Verisign’s malware scanning technology uses a combination of in-depth malware behavioral analysis, anti-virus results, detailed malware patterns, and network analysis to discover known exploits for the particular scanned zone. If malware is detected, the service sends the registrar a report that contains the number of malicious domains found and details about malicious content within its TLD zones. Reports with remediation instructions are provided to help registrars and registrants eliminate the identified malware from the registrant’s website.

3.2.2 Policies and Procedures That Address the Abusive Use of Registered Names

Suspension processes.

In the case of domain name abuse, Web.com will determine whether to take down the subject domain name. Verisign, Web.com's selected backend registry services provider, will follow the following auditable processes to comply with the suspension request.

Verisign Suspension Notification. Web.com submits the suspension request to Verisign for processing, documented by:

- Threat domain name
- Registry incident number
- Incident narrative, threat analytics, screen shots to depict abuse, and/or other evidence
- Threat classification
- Threat urgency description
- Recommended timeframe for suspension/takedown
- Technical details (e.g., Whois records, IP addresses, hash values, anti-virus detection results/nomenclature, name servers, domain name statuses that are relevant to the suspension)
- Incident response, including surge capacity

Verisign Notification Verification. When Verisign receives a suspension request from Web.com, it performs the following verification procedures:

- Validate that all the required data appears in the notification.
- Validate that the request for suspension is for a registered domain name.
- Return a case number for tracking purposes.

Suspension Rejection. If required data is missing from the suspension request, or the domain name is not registered, the request will be rejected and returned to Web.com with the following information:

- Threat domain name
- Registry incident number
- Verisign case number
- Error reason

Registrar Notification. Once Verisign has performed the domain name suspension, and upon Web.com request, Verisign notifies the registrar of the suspension. Registrar notification includes the following information:

- Threat domain name
- Registry incident number
- Verisign case number
- Classification of type of domain name abuse
- Evidence of abuse
- Anti-abuse contact name and number
- Suspension status
- Date/time of domain name suspension

Registrant Notification. Once Verisign has performed the domain name suspension, and upon Web.com request, Verisign notifies the registrant of the suspension. Registrant notification includes the following information:

- Threat domain name
- Registry incident number
- Verisign case number
- Classification of type of domain name abuse
- Evidence of abuse
- Registrar anti-abuse contact name and number

Upon Web.com request, Verisign can provide a process for registrants to protest the suspension.
Domain Suspension. Verisign places the domain to be suspended on the following statuses:

- serverUpdateProhibited

- serverDeleteProhibited
- serverTransferProhibited
- serverHold

Suspension Acknowledgement. Verisign notifies Web.com that the suspension has been completed. Acknowledgement of the suspension includes the following information:

- Threat domain name
- Registry incident number
- Verisign case number
- Case number
- Domain name
- Web.com abuse contact name and number, or registrar abuse contact name and number
- Suspension status

4. WHEN EXECUTED IN ACCORDANCE WITH THE REGISTRY AGREEMENT, PLANS WILL RESULT IN COMPLIANCE WITH CONTRACTUAL REQUIREMENTS

Web.com is fully committed to improving the completeness and accuracy of Whois data and to preventing and mitigating domain name abuse in the .web gTLD. We strongly believe the efforts that we have outlined will go a long way in this critical area and most certainly meet the requirements as outlined by ICANN.

The fight against domain names abuse is not a static fight. The tactics used by malicious parties are constantly evolving and web.com is committed to evolving our systems to address these ongoing threats not because ICANN says we have to but simply because it is what our customers have come to expect from Web.com.

The .web gTLD is an extension of our current business. At Web.com, we believe that a website is only as good as the services and support behind it. With the .web gTLD, we have the chance to bring this same commitment to service and support to a gTLD. For companies and consumers who stake their reputation on a .web domain name, having a gTLD that is trusted and secure is critical.

5. TECHNICAL PLAN SCOPE/SCALE THAT IS CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

Scope/Scale Consistency

As one of the first domain registrars, Web.com and its subsidiaries have seen the Internet grow exponentially across three decades. Web.com has grown to a point where it now serves approximately 3 million customers, comprising over 8 million domain names under management. As our customer base grew and the number of domains we managed with it, we expanded our operations to meet customer needs. We anticipate doing exactly the same as .web proliferates. Our systems are highly developed and continually tested and audited, and will scale as we scale. The commitments we will seek to make to prevent domain name abuse will expand to meet the anticipated growth of the .web gTLD. We invest tens of millions each year in upgrading infrastructure and developing new business processes to meet the growth and needs of our customer base, and consider doing so of paramount importance.

After 15 years of developing in this way, Web.com is a leading provider of Internet services for small- to medium-sized businesses (SMBs). Web.com is the parent company of two global domain name registrars, and further meets the Internet needs of consumers and businesses throughout their lifecycle with affordable value-added services. Those services include domain name registration; website design; search engine optimization; search engine marketing; social media and mobile products; local sales leads; eCommerce solutions; and call center services.

Headquartered in Jacksonville, FL, USA, Web.com is a publicly traded company (Nasdaq: WWWW), with more than 1,700 global employees in fourteen locations in North America, South America and the United Kingdom. Web.com brings a wealth of experience in providing a seamless process for customers from the first point of registration through the growth of their Internet properties.

Indeed, following our acquisition of Register.com in July 2010 and the subsequent

acquisition of Network Solutions, LLC, in October 2011, we have become one of the largest domain name registrars in the world. Web.com offers a variety of gTLDs and a full suite of domain name services, including registration, management, renewal, expiration protection and privacy services.

It is clear, therefore, that managing the potentially enormous growth of the .web namespace will be a challenge, but a challenge to which we are more than equal.

Scope/Scale Consistency Specific to Backend Registry Activities

Verisign, Web.com's selected backend registry services provider, is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign's scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the .web gTLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain this gTLD. Verisign's pricing for the backend registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Other Operating Cost" (Template 1, Line I.L) within the Question 46 financial projections response.

29. Rights Protection Mechanisms

1 MECHANISMS DESIGNED TO PREVENT ABUSIVE REGISTRATIONS

Web.com Group, Inc ("Web.com") has been in the business of helping our nearly 3 million customers establish their online presence for over 15 years. Through our recent acquisition of Network Solutions, the oldest ICANN accredited registrar, with over 25 years of experience, we have a long history of understanding the importance of rights protection. This is a core objective not only from our own personal perspective as the holder of various trademarks including web.com®, but also on behalf of our customers who have their own trademarks.

Web.com will implement and adhere to any rights protection mechanisms (RPMs) that may be mandated by ICANN, including each mandatory RPM set forth in the Registry Agreement, specifically Specification 7. Web.com acknowledges that, at a minimum, ICANN requires a Sunrise period, a Trademark Claims period, and interaction with the Trademark Clearinghouse with respect to the registration of domain names for the .web gTLD. It should be noted that because ICANN, as of the time of this application submission, has not issued final guidance with respect to the Trademark Clearinghouse, Web.com cannot fully detail the specific implementation of the Trademark Clearinghouse within this application. Web.com will adhere to all processes and procedures to comply with ICANN guidance once this guidance is finalized.

We understand the importance of Trademark holders to manage and protect their brands. In order to demonstrate our commitment to ensure the .web gTLD will accommodate the Intellectual Property community, Web.com has analyzed various additional mechanisms to help prevent abusive registrations. We were particularly impressed with the set of 31 Proposed Security, Stability and Resiliency Requirements for Financial gTLDs that were developed by the Security Standards Working Group (SSWG) under the guidance of the financial services industry. Following their recommendation that all potential applicants look at these standards for their own gTLDs, Web.com completed a thorough review to determine which standards may enhance the .web gTLD experience. While not all of the proposed standards are applicable to the .web gTLD, we will strive to implement several of these standards to ensure trademark owners will be able to take advantage of the

additional protection beyond the minimums set forth by ICANN.

Web.com has developed and will deploy a customized approach that seeks to minimize the potential for abusive registrations and incorporate a proactive mitigation process if a situation were to arise. Registrants, Registrars and the Registry will be contributing participants in this endeavor. Having all three participating entities of the .web gTLD ecosystem take part in these measures will ensure a comprehensive approach to these critical objectives.
Web.com has designed the following procedures to help protect the rights of trademark owners:

- Extended Sunrise Services
- Extended Trademark Claims Service
- Name Selection Policy
- Acceptable Use Policy
- Name Allocation Policy
- URS and UDRP
- PDDRP and RRDRP
- Rapid Takedown or Suspension
- Anti-Abuse Process
- Malware Code Identification
- DNSSEC Signing Service
- Biannual WHOIS Verification
- Participation in Anti-abuse Community Activities

As described in this response, Web.com will implement a Sunrise period and Trademark Claims service with respect to the registration of domain names within the .web gTLD. Certain aspects of the Sunrise period and/or Trademark Claims service may be administered on behalf of Web.com by Web.com approved registrars or by authorized subcontractors of Web.com, such as its selected backend registry services provider, Verisign.

Sunrise Periods. As it pertains to the launch of the .web gTLD, Web.com is currently planning on holding two different sunrise periods. Sunrise A will enable those participants that wish to register trademarks in the .web gTLD. A second sunrise period, Sunrise B, will be held for those who wish to reserve a domain name already registered in another gTLD. A more detailed explanation of each Sunrise Period follows.

Sunrise A

As set forth in the ICANN Applicant Guidebook, the Sunrise service pre-registration procedure for domain names must last for at least 30 days prior to the launch of the general registration of domain names in the gTLD.

To ensure that trademark owners have ample time to participate in the midst of the possible launch of several other gTLDs, Web.com is planning on extending the sunrise to 60 days, 30 days longer than the ICANN mandated minimum.

During the Sunrise period, holders of marks that have been previously validated by the Trademark Clearinghouse receive notice of domain names that are an identical match (as defined in the ICANN Applicant Guidebook) to their mark(s). Such notice is in accordance with ICANN’s requirements and is provided by Web.com either directly or through Web.com-approved registrars.

Web.com requires all registrants, either directly or through Web.com-approved registrars, who are in good-standing with ICANN, to i) affirm that said registrants meet the Sunrise Eligibility Requirements (SER) and ii) submit to the Sunrise Dispute Resolution Policy (SDRP) consistent with Section 6 of the Trademark Clearinghouse model. At a minimum Web.com recognizes and honors all word marks for which a proof of use was submitted and validated by the Trademark Clearinghouse.

During the Sunrise period, Web.com and/or Web.com-approved registrars, as applicable, are responsible for determining whether each domain name is eligible to be registered (including in accordance with the SERs).

Sunrise B

During a potential Sunrise B, registrants of domain names in other gTLDs may be able to file an application through a .web gTLD accredited registrar to register their existing domain name in the .web gTLD. Proof of registration of the domain name will be verified at the time of application. This sunrise period will last 30 days and at the end of the registration period, if there are no identical matches to any other applied for strings, the domain name will be registered to the appropriate applicant. If there are competing applications for the same domain name, qualified applicants will proceed to a closed auction to resolve the conflict.

Trademark Claims Service. As provided by the Trademark Clearinghouse model set forth in the January 11, 2012 version of the ICANN Applicant Guidebook, all new gTLDs will be required to provide a Trademark Claims service for a minimum of 60 days after the launch of the general registration of domain names in the gTLD (Trademark Claims period).

Similar to our voluntarily extending the sunrise period to accommodate the needs of trademark owners, Web.com is planning on extending the trademark claims services to 120 days, double the ICANN mandated minimum. As the processes for how the trademark clearinghouse, including technical and financial specifics of how the program will work, are not finalized as of the filing of this application, Web.com reserves the right to revisit the length of the Trademark Claims Service.

During the Trademark Claims period, in accordance with ICANN’s requirements, Web.com or the Web.com-approved registrar will send a Trademark Claims Notice to any prospective registrant of a domain name that is an identical match (as defined in the ICANN Applicant Guidebook) to any mark that is validated in the Trademark Clearinghouse. The Trademark Claims Notice will include links to the Trademark Claims as listed in the Trademark Clearinghouse and will be provided at no cost.

Prior to registration of said domain name, Web.com or the Web.com-approved registrar will require each prospective registrant to provide the warranties dictated in the Trademark Clearinghouse model set forth in the ICANN Applicant Guidebook. Those warranties will include receipt and understanding of the Trademark Claims Notice and confirmation that registration and use of said domain name will not infringe on the trademark rights of the mark holders listed. Without receipt of said warranties, Web.com or the Web.com-approved registrar will not have the ability to process the domain name registration.

Following the registration of a domain name, the Web.com-approved registrar will provide a notice of domain name registration to the holders of marks that have been previously validated by the Trademark Clearinghouse and are an identical match. This notice will be as dictated by ICANN. At a minimum Web.com will recognize, honor and adhere to all word marks validated by the Trademark Clearinghouse.

Adoption of Certain SSWG Elevated Security Standards

As referenced earlier in this question, Web.com will work to implement the following elevated security standards in the .web gTLD:

Name Selection Policy

The .web gTLD will enforce a name selection policy that ensures that all names registered in the gTLD will be in compliance with ICANN mandated technical standards. These include restrictions on 2 character names, tagged names, and reserved names for Registry Operations. All names must also be in compliance with all applicable RFCs governing the composition of domain names. In addition, registrations of Country, Geographical and Territory Names will only be allowed in compliance with the restrictions as outlined in the answer to Question 22.

Name Allocation Policy

As described above, Web.com plans on implementing an extended Sunrise A period for Trademark Holders and a Sunrise B Period for domain name holders. In addition, our current plans call for incorporating a Landrush Period during which applicants can secure preferred .web domains, followed by a General Availability. With the exception of the Sunrise B Period, all registrations will occur on a first come first served basis. Web.com reserves

the right to adjust this allocation Policy as it works through implementation details.

Acceptable Use Policy

Web.com has developed a draft the Registry Operator Acceptable Use Policy (AUP) which is further described in our response to Question 28. This AUP clearly defines what type of behavior is expressly prohibited in conjunction with the use of a .web domain name. Web.com will require, through the Registry Registrar Agreement (RRA), that this AUP be included in the registration agreement used by all .web gTLD accredited registrars. This registration agreement must be agreed upon by a registrant prior to them being able to register a name in the .web gTLD.

2 MECHANISMS DESIGNED TO IDENTIFY AND ADDRESS THE ABUSIVE USE OF REGISTERED NAMES ON AN ONGOING BASIS

In addition to the Sunrise and Trademark Claims services described in Section 1 of this response, Web.com will implement and adhere to RPMs post-launch as mandated by ICANN, and confirm that registrars accredited for the .web gTLD are in compliance with these mechanisms. Certain aspects of these post-launch RPMs may be administered on behalf of Web.com by Web.com-approved registrars or by approved subcontractors of Web.com, such as its selected backend registry services provider, Verisign.

These post-launch RPMs include the established Uniform Domain Name Dispute Resolution Policy (UDRP), as well as the newer Uniform Rapid Suspension System (URS) and Trademark Post-Delegation Dispute Resolution Procedure (PDDRP). Where applicable, Web.com will implement all determinations and decisions issued under the corresponding RPM.

After a domain name is registered, trademark holders may object to the registration through the UDRP or URS. Objections to the operation of the gTLD can be made through the PDDRP.

The following descriptions provide implementation details of each post-launch RPM for the .web gTLD:

- UDRP: The UDRP provides a mechanism for complainants to object to domain name registrations. The complainant files its objection with a UDRP provider and the domain name registrant has an opportunity to respond. The UDRP provider makes a decision based on the papers filed. If the complainant is successful, ownership of the domain name registration is transferred to the complainant. If the complainant is not successful, ownership of the domain name remains with the domain name registrant. Web.com and entities operating on its behalf adhere to all decisions rendered by UDRP providers.

- URS: As provided in the Applicant Guidebook, all registries are required to implement the URS. Similar to the UDRP, a complainant files its objection with a URS provider. The URS provider conducts an administrative review for compliance with filing requirements. If the complaint passes review, the URS provider notifies the registry operator and locks the domain. A domain lock means that the registry restricts all changes to the registration data, but the name will continue to resolve. After the domain is locked, the complaint is served to the domain name registrant, who has an opportunity to respond accordingly. If the complainant is successful, the registry operator is informed and the domain name is suspended for the balance of the registration period; the domain name will not resolve to the original source, but to an informational approved web page provided by the URS provider. If the complainant is not successful, the URS is terminated and full control of the domain name registration is returned to the domain name registrant. Similar to the existing UDRP, Web.com and entities operating on its behalf adhere to decisions rendered by the URS providers.

- PDDRP: As provided in the Applicant Guidebook, all registries are required to implement the PDDRP. The PDDRP provides a mechanism for a complainant to object to the registry operator’s manner of operation or use of the gTLD. The complainant files its objection with a PDDRP provider, who performs a threshold review. The registry operator has the opportunity to respond and the provider issues its determination based on the papers filed, although there may be opportunity for further discovery and a hearing. Web.com participates in the PDDRP process as specified in the Applicant Guidebook.

Additional Measures Specific to Rights Protection. Web.com provides additional measures

against abusive registrations. These measures will assist with mitigation of, but are not limited to, the following activities: phishing, pharming, and other Internet security threats. The measures exceed the minimum requirements for RPMs defined by Specification 7 of the Registry Agreement and are available at the time of registration.

These measures include:

- Rapid Takedown or Suspension Based on Court Orders: Web.com complies promptly with any order from a court of competent jurisdiction that directs it to take any action on a domain name that is within its technical capabilities as a gTLD registry. These orders may be issued when abusive content, such as but not limited to child pornography, counterfeit goods or illegal pharmaceuticals, is associated with the domain name.
- Anti-Abuse Process: Web.com implements an anti-abuse process that is executed based on the type of domain name takedown requested. The anti-abuse process is for malicious exploitation of the DNS infrastructure, such as phishing, botnets, and malware.
- Authentication Procedures: Verisign, Web.com's selected backend registry services provider, uses two-factor authentication to enhance security protocols for telephone, email, and chat communications.
- Registry Lock: Verisign's Registry Lock service allows registrants to lock a domain name at the authoritative registry level to protect against both unintended and malicious changes, deletions, and transfers. Only Verisign, as Web.com's backend registry services provider, can release the lock; thus all other entities that normally are permitted to update Shared Registration System (SRS) records are prevented from doing so. This lock is released only after the authorized registrar makes the request to unlock.
- Malware Code Identification: This safeguard reduces opportunities for abusive behaviors that use registered domain names in the gTLD. Registrants are often unknowing victims of malware exploits. As Web.com's backend registry services provider, Verisign has developed proprietary code to help identify malware in the zones it manages, which in turn helps registrars by identifying malicious code hidden in their domain names.
- DNSSEC Signing Service: Domain Name System Security Extensions (DNSSEC) helps mitigate pharming and phishing attacks that use cache poisoning to redirect unsuspecting users to fraudulent websites or addresses. It uses public key cryptography to digitally sign DNS data when it comes into the system and then validate it at its destination. The .web gTLD is DNSSEC-enabled as part of Verisign's core backend registry services.
- Biannual Whois Verification As detailed in our response to Question 28, all .web gTLD accredited registrars will be required as part of their RRA with Web.com to perform a Whois confirmation process twice a year. By asking registrants to confirm this information every 6 months, the .web gTLD should have a higher level of accurate Whois information for registered names in the event there is a case of trademark infringement by a non authorized registrant. Having accurate Whois information is critical to solving these issues in a timely manner.
- Participation in Anti-abuse Community Activities. Since our founding in 1997, Web.com has been an active participant and leader in multiple organizations, symposia, forums and other efforts that focus on the prevention of domain name abuse, including trademark infringement. Specifically, we are an active member of the Certificate Authentication Board, ICANN, the Internet standards development community, and we participate in SSAC. We find this participation extremely helpful in staying abreast of the latest changes and challenges in this field. Participation in these efforts also allows us to not only share our best practices with the rest of the anti-abuse community, but to learn from what others have been doing and incorporate it into how we operate our business. As mentioned earlier in this question, Web.com will be incorporating some of the SSWG enhanced security standards which is proof that community led efforts can produce significant results.

3. RESOURCING PLANS

Resource Planning

Web.com is a leading provider of Internet services for small to medium-sized businesses (SMBs). Web.com is the parent company of two global domain name registrars and further meets the Internet needs of consumers and businesses throughout their lifecycle with affordable value added services that including domain name registration, website design, search engine optimization, search engine marketing, social media and mobile products, local sales leads, eCommerce solutions and call center services. Headquartered in Jacksonville, FL, USA, Web.com is NASDAQ traded company serving nearly three million

customers with more than 1,700 global employees in fourteen locations in North America, South America and the United Kingdom.

Our business is helping people establish, maintain, promote, and optimize their web presence. Web.com intentionally chose Verisign as our registry services provider because of their unsurpassed track record in operating some of the world's most complex and critical top level domains. Verisign's support for the .web gTLD will help ensure its success

The .web gTLD will be fully supported by a cross function team of Web.com professionals. Numbers and types of employees will vary for each function but Web.com projects it will use the following personnel to support the resource planning requirements;

- Quality Assurance Engineer: 0.5 FTE
- System Administrator: 1 FTE
- Database Administrator: 0.5 FTE
- Technical Project Manager: 0.5 FTE
- Marketing Director: 1 FTE
- Sales Manager: 1 FTE
- Legal Counsel: 1 FTE
- Finance/Accounting: 1 FTE
- Customer Service: 2 FTEs

Resource Planning Specific to Backend Registry Activities

Verisign, Web.com's selected backend registry services provider, is the most experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely modifies these staffing models to account for new tools, standards and policy implementations and process innovations. These models enable Verisign to continually allocate the appropriate staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it will extend to Web.com fully accounts for cost related to this infrastructure, which is provided as Line IIb.G, Total Critical Registry Function Cash Outflows, within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability at 100 percent of the time for more than 13 years for .com, which exceeds the current several level agreements, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's gTLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support the implementation of RPMs:

- Customer Affairs Organization: 9
- Customer Support Personnel: 36
- Information Security Engineers: 11

To implement and manage the .web gTLD as described in this application, Verisign, Web.com's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of gTLDs. Consistent with its resource modeling, Verisign frequently reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified and skilled candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its gTLDs instead of creating a new entity to manage only this

proposed gTLD, Verisign realizes significant economies of scale and ensures its gTLD best practices are followed consistently. This consistent demonstration of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest gTLDs (i.e., .com). Moreover, by augmenting existing teams, Verisign ensures new employees are provided the opportunity to be trained and mentored by existing senior staff. This coaching and mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

30(a). Security Policy: Summary of the security policy for the proposed registry

1 DETAILED DESCRIPTION OF PROCESSES AND SOLUTIONS DEPLOYED TO MANAGE LOGICAL SECURITY ACROSS INFRASTRUCTURE AND SYSTEMS, MONITORING AND DETECTING THREATS AND SECURITY VULNERABILITIES AND TAKING APPROPRIATE STEPS TO RESOLVE THEM

Please note; all figures, tables and diagrams referenced in the following response can be found in attachment titled "Attachment dot web Q30A."

Web.com Group, Inc. ("Web.com") selected backend registry services provider's (Verisign's) comprehensive security policy has evolved over the years as part of managing some of the world's most critical TLDs. Verisign's Information Security Policy is the primary guideline that sets the baseline for all other policies, procedures, and standards that Verisign follows. This security policy addresses all of the critical components for the management of backend registry services, including architecture, engineering, and operations.

Verisign's general security policies and standards with respect to these areas are provided as follows:

- Architecture
  - Information Security Architecture Standard: This standard establishes the Verisign standard for application and network architecture. The document explains the methods for segmenting application tiers, using authentication mechanisms, and implementing application functions.
  - Information Security Secure Linux Standard: This standard establishes the information security requirements for all systems that run Linux throughout the Verisign organization.
  - Information Security Secure Oracle Standard: This standard establishes the information security requirements for all systems that run Oracle throughout the Verisign organization.
  - Information Security Remote Access Standard: This standard establishes the information security requirements for remote access to terminal services throughout the Verisign organization.
  - Information Security SSH Standard: This standard establishes the information security requirements for the application of Secure Shell (SSH) on all systems throughout the Verisign organization.

- Engineering
  - Secure SSL/TLS Configuration Standard: This standard establishes the information security requirements for the configuration of Secure Sockets Layer/Transport Layer Security (SSL/TLS) for all systems throughout the Verisign organization.
  - Information Security C++ Standards: These standards explain how to use and implement the functions and application programming interfaces (APIs) within C++. The document also describes how to perform logging, authentication, and database connectivity.
  - Information Security Java Standards: These standards explain how to use and implement the functions and APIs within Java. The document also describes how to perform logging, authentication, and database connectivity.

- Operations
  - Information Security DNS Standard: This standard establishes the information security requirements for all systems that run DNS systems throughout the Verisign

organization.

- Information Security Cryptographic Key Management Standard: This standard provides detailed information on both technology and processes for the use of encryption on Verisign information security systems.
- Secure Apache Standard: Verisign has a multitude of Apache web servers, which are used in both production and development environments on the Verisign intranet and on the Internet. They provide a centralized, dynamic, and extensible interface to various other systems that deliver information to the end user. Because of their exposure and the confidential nature of the data that these systems host, adequate security measures must be in place. The Secure Apache Standard establishes the information security requirements for all systems that run Apache web servers throughout the Verisign organization.
- Secure Sendmail Standard: Verisign uses sendmail servers in both the production and development environments on the Verisign intranet and on the Internet. Sendmail allows users to communicate with one another via email. The Secure Sendmail Standard establishes the information security requirements for all systems that run sendmail servers throughout the Verisign organization.
- Secure Logging Standard: This standard establishes the information security logging requirements for all systems and applications throughout the Verisign organization. Where specific standards documents have been created for operating systems or applications, the logging standards have been detailed. This document covers all technologies.
- Patch Management Standard: This standard establishes the information security patch and upgrade management requirements for all systems and applications throughout Verisign.

- General
- Secure Password Standard: Because passwords are the most popular and, in many cases, the sole mechanism for authenticating a user to a system, great care must be taken to help ensure that passwords are “strong” and secure. The Secure Password Standard details requirements for the use and implementation of passwords.
- Secure Anti-Virus Standard: Verisign must be protected continuously from computer viruses and other forms of malicious code. These threats can cause significant damage to the overall operation and security of the Verisign network. The Secure Anti-Virus Standard describes the requirements for minimizing the occurrence and impact of these incidents.

Security processes and solutions for the .web gTLD are based on the standards defined above, each of which is derived from Verisign’s experience and industry best practice. These standards comprise the framework for the overall security solution and applicable processes implemented across all products under Verisign’s management. The security solution and applicable processes include, but are not limited to:

- System and network access control (e.g., monitoring, logging, and backup)
- Independent assessment and periodic independent assessment reports
- Denial of service (DoS) and distributed denial of service (DDoS) attack mitigation
- Computer and network incident response policies, plans, and processes
- Minimization of risk of unauthorized access to systems or tampering with registry data
- Intrusion detection mechanisms, threat analysis, defenses, and updates
- Auditing of network access
- Physical security

Further details of these processes and solutions are provided in Part B of this response.

1.1 Security Policy and Procedures for the Proposed Registry

Specific security policy related details, requested as the bulleted items of Question 30 – Part A, are provided here.

Independent Assessment and Periodic Independent Assessment Reports. To help ensure effective security controls are in place, Web.com, through its selected backend registry services provider, Verisign, conducts a yearly American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) SAS 70 audit on all of its data centers, hosted systems, and applications. During these SAS 70 audits, security controls at the operational, technical, and human level are rigorously tested. These audits are conducted by a certified and accredited third party and help ensure that Verisign in-place environments meet the security criteria specified in Verisign’s customer contractual agreements and are in accordance with commercially accepted security controls and practices. Verisign also performs numerous audits throughout the year to verify its security processes and activities. These audits cover many different environments and

technologies and validate Verisign's capability to protect its registry and DNS resolution environments. Figure 30A-1 lists a subset of the audits that Verisign conducts. For each audit program or certification listed in Figure 30A-1, Verisign has included, as attachments to the Part B component of this response, copies of the assessment reports conducted by the listed third-party auditor. From Verisign's experience operating registries, it has determined that together these audit programs and certifications provide a reliable means to ensure effective security controls are in place and that these controls are sufficient to meet ICANN security requirements and therefore are commensurate with the guidelines defined by ISO 27001.

Augmented Security Levels or Capabilities. See Section 5 of this response.

Commitments Made to Registrants Concerning Security Levels. See Section 4 of this response.

2 SECURITY CAPABILITIES ARE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

Verisign, Web.com's selected backend registry services provider, is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign's scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the .web gTLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain this gTLD. Verisign's pricing for the backend registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

3 TECHNICAL PLAN ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

Resource Planning
Web.com is a leading provider of Internet services for small to medium-sized businesses (SMBs). Web.com is the parent company of two global domain name registrars and further meets the Internet needs of consumers and businesses throughout their lifecycle with affordable value added services that including domain name registration, website design, search engine optimization, search engine marketing, social media and mobile products, local sales leads, eCommerce solutions and call center services. Headquartered in Jacksonville, FL, USA, Web.com is NASDAQ traded company serving nearly three million customers with more than 1,700 global employees in fourteen locations in North America, South America and the United Kingdom.

Our business is helping people establish, maintain, promote, and optimize their web presence. Web.com intentionally chose Verisign as our registry services provider because of their unsurpassed track record in operating some of the world's most complex and critical top level domains. Verisign's support for the .web gTLD will help ensure its success.

The .web gTLD will be fully supported by a cross function team of Web.com professionals. Numbers and types of employees will vary for each function but Web.com projects it will use the following personnel to support the resource planning requirements:

- Quality Assurance Engineer: 0.5 FTE
- System Administrator: 1 FTE
- Database Administrator: 0.5 FTE
- Technical Project Manager: 0.5 FTE
- Marketing Director: 1 FTE
- Sales Manager: 1 FTE
- Legal Counsel: 1 FTE

- Finance/Accounting: 1 FTE
- Customer Service: 2 FTEs

Resource Planning Specific to Backend Registry Activities
Verisign, Web.com's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 – Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to Web.com fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel role, which is described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support its security policy:

- Information Security Engineers: 11

To implement and manage the .web gTLD as described in this application, Verisign, Web.com's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only the .web gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this the .web gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

4 SECURITY MEASURES ARE CONSISTENT WITH ANY COMMITMENTS MADE TO REGISTRANTS REGARDING SECURITY LEVELS

Verisign is Web.com's selected backend registry services provider. For the .web gTLD, no unique security measures or commitments must be made by Verisign or Web.com to any registrant.

5 SECURITY MEASURES ARE APPROPRIATE FOR THE APPLIED-FOR gTLD STRING (FOR EXAMPLE, APPLICATIONS FOR STRINGS WITH UNIQUE TRUST IMPLICATIONS, SUCH AS FINANCIAL SERVICES-ORIENTED STRINGS, WOULD BE EXPECTED TO PROVIDE A COMMENSURATE LEVEL OF SECURITY)

No unique security measures are necessary to implement the .web gTLD. As defined in Section 1 of this response, Verisign, Web.com's selected backend registry services provider, commits to providing backend registry services in accordance with the following international and relevant security standards:

- American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) SAS 70
- WebTrust/SysTrust for Certification Authorities (CA)

© Internet Corporation For Assigned Names and Numbers.

EXHIBIT JMR-17

JMR-17

New gTLD Application Submitted to ICANN by: DotWeb Inc.

String: web

Originally Posted: 13 June 2012

Application ID: 1-956-26846

Applicant Information

1. Full legal name

DotWeb Inc.

2. Address of the principal place of business

Contact Information Redacted

3. Phone number

Contact nformation Redacted

4. Fax number

Contact nformation Redacted

5. If applicable, website or URL

http://www.radixregistry.com

Primary Contact

6(a). Name

Mr. Brijesh Harish Joshi

6(b). Title

Director & GM

6(c). Address

6(d). Phone Number

Contact nformation Redacted

6(e). Fax Number

6(f). Email Address

Contact Information Redacted

Secondary Contact

7(a). Name

Mr. Namit Sunil Merchant

7(b). Title

General Manager

7(c). Address

7(d). Phone Number

Contact nformation Redacted

7(e). Fax Number

7(f). Email Address

Contact Information Redacted

Proof of Legal Establishment

8(a). Legal form of the Applicant

International Business Company (Limited Liability Company)

8(b). State the specific national or other jursidiction that defines the type of entity identified in 8(a).

Republic of Seychelles, International Business Companies Act, 1994 (Act 24 of 1994)

8(c). Attach evidence of the applicant's establishment.

Attachments are not displayed on this form.

9(a). If applying company is publicly traded, provide the exchange and symbol.

9(b). If the applying entity is a subsidiary, provide the parent company.

9(c). If the applying entity is a joint venture, list all joint venture partners.

Applicant Background

11(a). Name(s) and position(s) of all directors

Brijesh Joshi	Director & General Manager

11(b). Name(s) and position(s) of all officers and partners

Brijesh Joshi	Director & General Manager
Namit Merchant	General Manager
Vishal Manjalani	Vice President

11(c). Name(s) and position(s) of all shareholders holding at least 15% of shares

Directi FZC dba Radix	Not Applicable

11(d). For an applying entity that does not have directors, officers, partners, or shareholders: Name(s) and position(s) of all individuals having legal or executive responsibility

Applied-for gTLD string

13. Provide the applied-for gTLD string. If an IDN, provide the U-label.

web

14(a). If an IDN, provide the A-label (beginning with "xn--").

14(b). If an IDN, provide the meaning or restatement of the string in English, that is, a description of the literal meaning of the string in the opinion of the applicant.

14(c). If an IDN, provide the language of the label (in English).

14(c). If an IDN, provide the language of the label (as referenced by ISO-639-1).

14(d). If an IDN, provide the script of the label (in English).

14(d). If an IDN, provide the script of the label (as referenced by ISO 15924).

14(e). If an IDN, list all code points contained in the U-label according to Unicode form.

15(a). If an IDN, Attach IDN Tables for the proposed registry.

Attachments are not displayed on this form.

15(b). Describe the process used for development of the IDN tables submitted, including consultations and sources used.

15(c). List any variant strings to the applied-for gTLD string according to the relevant IDN tables.

16. Describe the applicant's efforts to ensure that there are no known operational or rendering problems concerning the applied-for gTLD string. If such issues are

known, describe steps that will be taken to mitigate these issues in software and other applications.

We have engaged ARI Registry Services (ARI) to deliver backend technology services for this TLD.

ARI is experienced with:
– The operational issues of operating TLDs, including ccTLDs.
– TLDs that offer registrations at the third level (e.g. .com.au, .net.au) and which have their own set of unique issues.
– The rendering and operational issues surrounding the introduction of IDNs.

The following is the result of ARI's analysis.

1. INTRODUCTION

ARI has not found any issues unique to this TLD with respect to operational and rendering issues.

This has been established by:
– Testing of the TLD string itself.
– Researching issues experienced by others.
– Our understanding of published material.
– Our own experience.

2. LOCAL TESTING OF THE TLD STRING

ARI has executed a suite of tests to evaluate any issues arising from the use of the TLD string. ARI configured a test environment that consisted of DNS software that served authoritative responses for this TLD, web server software that hosted a simple website, and an email server that provided mailboxes for sample domains in this TLD. Testing included:

– Navigation of websites using the address bar and hyperlinks.
– Composition and delivery of mail.
– Mail filters such as spam detection.
– Display of domain names in address bars, hyperlinks, and free text.

Where possible, ARI attempted to test many equivalent applications, however the number of and different versions of applications means that testing was limited to the more common environments. Tested platforms and applications included:
– Microsoft Windows, Apple OS X and Red Hat Linux.
– Internet Explorer, Safari, Opera, Firefox and Chrome.
– Exchange, Sendmail and Postfix.

ARI did not find any operational or rendering issues with this TLD that are unique to this TLD.

This completes our response to Q16.

17. (OPTIONAL) Provide a representation of the label according to the International Phonetic Alphabet (http://www.langsci.ucl.ac.uk/ipa/).

Mission/Purpose

18(a). Describe the mission/purpose of your proposed gTLD.

The mission/purpose of .web is first choice. Domain name first choice, once again - globally. Some registrants got their first choice of a .com name. Many did not. When the .com registry gained its momentum selling names early on, the North American market and particularly the United States were the first and primary purchasers of .com names. They got their first choice. And many global registrants who came after did not. Other generic top level domains have been introduced: .info, .biz, .net, .org – but none of those names have the true global generic appeal of the .com brand. Each of those four strings brings some characteristic that taints the string with some preconception.

* .info is short for information – but my site does much more than information

* .biz is short for business – but my site is not business related

* .net is short for network – but the term “the net” died several years ago

* .org is short for organization – but my site is not a non-profit

* .com is short for commercial or company, and is not truly a generic extension

Country code top-level domains (ccTLD) are an option, however a ccTLD such as Germany (.DE) or Japan (.JP) brings the impression that the website is tied to the country or region, but not truly global. Hence the need for .web – a truly generic top level domain that means the same in Shanghai, Munich, Sao Paolo, Mumbai, Johannesburg, Tokyo and your city. The mission of .web is to give international registrants the same opportunity the North American market had - to get their unique name in a truly global name space – with nothing added – just trusted and secure access to the web. The mission of .web is first choice.

The goal of .web is to provide first choice name registration to individuals, entrepreneurs, communities, small and medium sized businesses, multi-national corporations, non-profits and anyone else seeking a truly global domain name. Based on our experience, when a potential registrant goes to a registrar’s site to register a new gTLD domain name, the domain name is unavailable over 70% of the time (Source: Internal Research on com availability checks) and the registrant is presented with a long list of permutation options that are not their first choice – either for the name or the TLD.

The goal of .web is to register your first choice name. The Mission and purpose of our TLD is also to contribute to the Internet Namespace in the following ways:

1.1 ENHANCE REGISTRANT CHOICE

To create a namespace that provides registrants greater choice to represent themselves online in the manner they please. Due to the saturated nature of the existing gTLD space, many Internet users have to opt for a name that does not suit their needs best. Our Registry will provide Registrants a higher probability of obtaining their desired name.

1.2 CREATE A CLEANER INTERNET SPACE

To create a cleaner internet experience for end users by implementing pioneering registration policies, content and usage policies, and abuse mitigation processes.

1.3 CREATE A STABLE AND RESILIENT INTERNET SPACE

To deliver a stable and resilient internet experience to registrants and end-users by going above and beyond the ICANN mandated SLAs and delivering 100% resolution uptime

This completes our response to Q18(a).

18(b). How do you expect that your proposed gTLD will benefit registrants, Internet users, and others?

1. GOAL OF .WEB

1.1 SPECIALTY

* Our goal for .web in terms of area of specialty is to be the first choice generic TLD among new registrants. We will support the rapidly developing domain name markets, not just in traditional markets such as Western Europe and North America, but equally in the growing regions of South America, Asia, Eastern Europe, the entire Pacific Rim. The .web registry will provide registrants the opportunity for first choice of their preferred domain name on a generic global TLD.

1.2 SERVICE LEVELS

Our goal for .Web in terms of service levels is to go above and beyond the ICANN SLAs. ICANN provides for its expected SLA in Specification 10 in the Registry Agreement in the Applicant guidebook.

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provides registry services for a number of TLDs including the .au ccTLD.

Our contract with ARI is attached to our response to Q46. This contract details the SLA we intend on achieving with this TLD. As can be seen in the contract we have exceeded the ICANN required SLA on every parameter.

Our response to Q34 and Q35 provides details on ARI's distributed anycast DNS network. ARI's DNS network provides for 16 geo distributed sites resulting in a very low resolution latency for end-users, amongst the lowest in the industry.

It is our objective to provide 100% uptime, a resilient global DNS infrastructure, and very low latency in terms of DNS resolution for this TLD

1.3 REPUTATION

Reputation of our TLD is of paramount importance to us. The reputation of our TLD directly relates to how end-users on the internet perceive our Registrants. We will ensure the highest reputation of .Web by ensuring the following –

* Maintaining a high quality bar with respect to Registrants in the TLD
* Well defined Acceptable usage and content policies
* Well defined dispute resolution mechanisms
* Ensuring Whois accuracy to support abuse mitigation
* Well defined and implemented abuse mitigation processes
* Well defined and implemented rights protection mechanisms
* Exceptional service levels

To this effect we have created unprecedented Abuse mitigation policies and Rights protection mechanisms that go significantly above and beyond mandatory requirements and common practice described in considerable detail in our response to Q28 and Q29. We also commit to extremely high service levels that go beyond the stipulated service levels in the applicant guidebook.

2. CONTRIBUTION OF .WEB TO THE NAMESPACE

2.1 CONTRIBUTION IN TERMS OF COMPETITION, DIFFERENTIATION, OR INNOVATION

Per ICANN's Bylaws as amended June 24, 2011, ICANN's core value number six is "Introducing and promoting competition in the registration of domain names where practicable and beneficial in the public interest."

The .web registry will be a new direct and formidable competitor to the current group of global generic TLDs. This will be especially true in the key growing international markets.

Since Directi has been a registrar for over 10 years, managing over 4 million domain names across the globe, we understand the nuances of domain name buying behaviour. The .Web registry will leverage this unique market knowledge to design competitive offerings against other global gTLDs.

Directi will be offering the language and culture agnostic .web to international markets, with the goal of a truly global distribution of registrants. Most gTLDs have largely focused on developed markets with 70+% internet penetration, namely North America and European marketplaces. Domain Name and website growth is yet to occur in other developing markets like India, Brazil, Russia, China, Indonesia etc. However as the market for websites and domain names grows in these economies the existing gTLD space in TLDs like .com, .net, .org etc will already be saturated with all tier 1 names no longer available to markets like asia, africa. 70% of .com check availability checks return unavailable (data obtained from Internal Reserach). New companies have to resort to 2nd tier long multi-word names for their businesses in these markets. .Web will broaden the namespace by providing an alternative for Registrants in developing markets to register the domain name of their choice, creating competition.

Lastly .Web will provide registrants the option to register more desirable and shorter names as opposed to names they would have otherwise registered in existing gTLDs due to the high saturation of the existing namespaces.

Our intent is to operate .Web with a focus on integrity and quality for the .Web brand. This entails running robust abuse mitigation programs and pioneering Rights Protection Mechanisms from initiation, which in our case not only meets ICANN’s requirements, but extends significantly beyond it as described in our response to Q28 and Q29.

3. USER EXPERIENCE GOALS

.Web considers both its Registrants and the end-users that access .Web websites as its users. Our goal is to create a highly reliable namespace and provide an outstanding user experience to both Registrants and end-users of .Web.

Registrants of .Web have an assurance of a scalable, resilient registry with 100% uptime, low latency, and exemplary security standards. Registrants will have the option to register the domain name of their choice, without much saturation of the namespace. Our registration policies and abuse mitigation policies ensure that Registrants will get advantages like higher recognition, better branding and more desirable, shorter names.

Our content and acceptable use policies and abuse mitigation processes ensure that end-users are benefited from a clean namespace. These are described in further detail in our response to Q28 and Q29.

4. REGISTRATION POLICIES IN SUPPORT OF GOALS

4.1 GENERAL NAMES

The purpose of .web is to allow registrants to register their first choice name. As such, the TLD will offer registrations at the second level, and will have an open registration policy so that registrants have the choice and the freedom to find the name that they like best. The TLD will be open to registrants in all areas of the world, without nexus or pre-qualification requirements. Registrations in .web can be used for any purpose, including for use by businesses, individuals, and not-for-profit entities. We anticipate that registrants will introduce many unique, new, dedicated Web sites to the Internet using their .web domain names.

The goals of .Web are outlined in the sections above. These goals are supported by the following artifacts –
* Registration policies and processes
* Acceptable usage policies and content guidelines
* Abuse mitigation processes
* Rights protection mechanisms
* Dispute resolution polices

To this effect we have created unprecedented Abuse mitigation policies and Rights protection mechanisms that go significantly above and beyond mandatory requirements and common practice. The salient aspects of all of the above are described below -

* DotWeb Inc. is a wholly owned subsidiary within the Directi Group. The Directi Group runs various businesses including several ICANN Accredited Domain Registrars (ResellerClub.com and BigRock.com) and Web Hosting companies. With over four million active domain names registered through its registrars, Directi has significant experience (over 10 years) of managing domain name abuse mitigation and rights protection. Directi has been heralded as a white hat registrar and the undisputed leader with respect to abuse mitigation.
* Our Abuse and compliance processes will be run by the Directi Group
* We have an elaborate and detailed Accepted usage and content policy that covers over 11 macro forms of violations
* .Web will create a zero-tolerance reputation when it comes to abuse
* We have a defined SLA for responding to abuse complaints ensuring guaranteed turn-around time on any abuse complaint depending on its severity
* We will work closely with LEA and other security groups to mitigate abuse within the TLD by providing them with special interfaces (eg searcheable whois) and interacting with them regularly in terms of knowledge sharing.
* Other abuse mitigation steps we undertake include profiling, blacklisting, proactive quality reviews, industry collaboration and information sharing, regular sampling, contractual enforcements and sanctions
* The protection of trademark rights is a core goal of .Web. .Web will have a professional plan for rights protection. It will incorporate best practices of existing TLDs, going above and beyond the ICANN mandated RPMs to prevent abusive registrations and rapidly take-down abuse when it does occur.
* Standard RPMs such as Sunrise, Trademarks claims service, URS, UDRP, SDRP, PDDRP, SPOC etc are all provided for. Additional RPMs such as Optional Trademark declaration, profiling and blacklisting, proactive quality reviews, APWG Review and others will also be provided.

The above salient points barely scratch the surface in detailing the steps that .Web will take in order to build a reputation of operating a clean, secure and trusted namespace. Significant details of all of the above and more are provided in our responses to Q26, Q27, Q28 and Q29

4.2. OTHER NAMES

* We will reserve the following classes of domain names, which will not be available to registrants via the Sunrise or subsequent periods:
** The reserved names required in Specification 5 of the new gTLD Registry Agreement.
** The geographic names required in Specification 5 of the new gTLD Registry Agreement. See our response to Question 22 (“Protection of Geographic Names”) for details.
** The registry operator will reserve its own name and variations thereof, and registry operations names (such as nic.Web, registry.Web, and www.Web), so that we can point them to our Web site. Reservation of the registry operator’s names was standard in ICANN’s past gTLD contracts.
** We will also reserve names related to ICANN and Internet standards bodies (iana.Web, ietf.Web, w3c.Web, etc.), for delegation of those names to the relevant organizations upon their request. Reservation of this type of names was standard in ICANN’s past gTLD contracts. The list of reserved names will be published publicly before the Sunrise period begins, so that registrars and potential registrants will know which names have been set aside.

* We will reserve generic names which will be set aside for distribution via special mechanisms.

5. PROTECTING PRIVACY OF REGISTRANTS’ OR USERS’ INFORMATION

.Web is committed to providing a secure and trusted namespace to its Registrants and end-users. To that extent we will have several measures for protecting the privacy or confidential information of registrants or users -

* Our Whois service (web-based whois, port 43 whois and searchable whois) all have built in abuse prevention mechanisms to prevent unauthorized access, data mining, data scraping and any other abusive behavior. Details of this are provided in our response to Q26

* .Web will allow Registrants to use privacy protection services provided by their Registrars in the form of a Proxy whois service as long as they follow the guidelines stipulated within our response to Q28 to prevent any abuse of the same

* As per the requirements of the new gTLD Registry Agreement (Article 2.17), we shall notify each of our registrars regarding the purposes for which data about any identified or identifiable natural person (“Personal Data”) submitted to the Registry Operator by such registrar is collected and used, and the intended recipients (or categories of recipients) of such Personal Data. (This data is basically the registrant and contact data required to be published in the WHOIS.)

* We will also require each registrar to obtain the consent of each registrant in the TLD for such collection and use of Personal Data. As the registry operator, we shall not use or authorize the use of Personal Data in a way that is incompatible with the notice provided to registrars.

* As the registry operator we shall take significant steps to protect Personal Data collected from registrars from loss, misuse, unauthorized disclosure, alteration, or destruction. In our responses to Q24, Q30 and Q38 we detail the security policies and procedures we will use to protect the registry system and the data contained there from unauthorized access and loss.

* As registry operator we impose certain operational standards for our registrars. In order to gain and maintain accreditation for our TLD, we require them to adhere to certain information technology policies designed to help protect registrant data. These include standards for access to the registry system. Please see our response to Q24, Q25 and Q30 for details.

* We offer a “registry lock” service, designed to help protect participating registrants’ contact data from unauthorized modification, and against unauthorized domain transfers and deletions. Please see our response to Q27 for details.

* .Web implements DNSSEC at the zone which guarantees origin authentication of DNS data, authenticated denial of existence, and data integrity. This protects end-users from a man-in-the-middle attack protecting the privacy of data of end-users.

6. OUTREACH AND COMMUNICATIONS

* Our goal for .web is for it to be the first-choice generic TLD among new registrants. To achieve this, we will emphasize distribution channels internationally.

* We will also engage in relevant PR and outreach programs as well as ensure appropriate publication of information on our website.

* For many Internet users, the World Wide Web is the first thing they think of when they think of the Internet. For first-time registrants, a .web TLD will be easy to understand and easy to communicate about.

* Our outreach efforts will be directed towards our target market in coordination with Registrar partners, to ensure greater adoption of the .Web TLD. One important method of outreach will involve co-marketing programs with registrars. We will also leverage Directi’s existing channel of 65,000 Resellers, and its strategic relationships with other ICANN Accredited Registrars.

The communication and outreach will focus on -

* Educating audiences regarding this new namespace which has a high availability of names, and the immense possibilities and internet innovations that it could result in.

* Generating awareness of our Registration policies, Acceptable usage and content policies, Abuse mitigation processes and Rights protection mechanisms

This completes our response to Q18(b).

18(c). What operating rules will you adopt to eliminate or minimize social costs?

.Web considers both its Registrants and the end-users that access .Web websites as its users. Our goal is to create a highly reliable namespace and provide an outstanding user experience to both Registrants and end-users of .Web. To that extent it is our goal to –

* Reduce ⁄ minimize any incremental costs ⁄ negative consequences imposed upon our users
* Increase ⁄ maximize the value added to our Registrants and end-users
* Ensure that the net effect of .Web on its users is that of positive value creation

In this response we explore how .Web achieves a net benefit for Registrants and End-users.

1. MINIMIZING COSTS

1.1 REGISTRANTS

It is our goal to provide Registrants of .Web incremental value and minimize any negative consequences and costs associated with .Web. We address this in the following manner

1.1.1 SUNRISE, TMCH, RPMs

Rights protection is a core goal of .Web. Our Rights Protection mechanisms go significantly above and beyond the mandatory RPMs ensuring protection of trademark and IP rights of domain registrants and reducing the costs associated with rights protection for Registrants. Our elaborate RPMs are described in significant detail in our response to Q29. Some salient aspects of these are as follows -

* We offer a sunrise period to provide an opportunity for legitimate Registrants to block domain names in .Web before general availability begins, preventing unnecessary post-facto litigation

* We will integrate with the Trademark Clearing House in the manner prescribed to provide the Trademarks claims service, so as to alert potential Registrants of any trademark violations prior to registration, as well as notify mark holders of potential mark violations

* We will provide SDRP, URS, UDRP and PDDRP reducing litigation costs by providing legitimate Registrants the opportunity to resolve disputes through standardized arbitration proceedings.

* Additionally we have pioneering RPMs like Optional Trademark Declaration, Profiling and Blacklisting, Proactive Quality assurance, APWG review etc – all intended to reduce rights violations and hence reduce costs for Registrants

The above salient points barely scratch the surface in detailing the steps that .Web will take in order to reduce costs of Registrants with respect to rights violations. Significant details of all of the above and more are provided in our responses to Q26, Q27, Q28 and Q29.

1.1.2 MULTIPLE APPLICATIONS FOR A DOMAIN

All of the RPMs described in section 1.1.1 above ensure that applicants for domain names in .Web are legitimate right holders for the applied string.

During general availability domain names will be allocated on a first come first serve basis amongst applicants. During the initial registry launch periods of Sunrise and Landrush if multiple applications for the same domain name are received from applicants then the same will be distributed in the following manner –

* Incase of multiple sunrise applications for the same domain name, all applications will be validated against the TMCH for a valid trademark. Applications that do not qualify will be dropped.

* All remaining applications will be distributed through a fair auction.

1.1.3 COST BENEFITS FOR REGISTRANTS

The ICANN new gTLD program marks a historical event in the timeline of the Internet. It is an unprecedented event and one that will yield tremendous benefits for consumers. At this preliminary stage it is impossible to determine the true value consumers will derive from increase in competition and choice. However there is historical data to go by. Upon the launch of Domain Registrars and creation of competition amongst registrars, the Registrants benefited from reduced pricing.

With .Web our goal is to provide fair pricing for domains within .Web that reflect the value proposition derived by the Registrants of .Web. While we do not have any committed pricing plans as yet and the same will be determined during the launch process, we do anticipate providing promotional offers through the life of .Web for the purpose of customer acquisition. This is not too dissimilar from other gTLD registries currently in existence who offer ongoing promotional offers to their customer base.

1.1.4 PRICE ESCALATIONS

The ICANN new gTLD program is an unprecedented event and the actual nature of pricing pressures will only be determinable once several TLDs have successfully launched. At this preliminary stage it is impossible to commit to any pricing strategy on our part. We strongly believe that ultimately, the open market will determine the viability of pricing models and dictate pricing strategy for everyone. We intend to maintain the freedom to set pricing to accommodate for the existence of 100s of TLDs and business models and create a sustainable long term business model. Our goal is to provide fair pricing for domains within .Web that reflect the value proposition derived by the Registrants of .Web.

1.2 END USERS

It is our goal to provide end users of .Web incremental value and minimize any negative consequences and costs associated with .Web. We address this in the following manner

End-users bear a considerable amount of cost as a result of various forms of Internet abuse such as spam, malware, phishing, pharming, hacking, identity theft etc. Any TLD that implements policies and processes to create a clean namespace will result in a considerable reduction of these forms of abuse and hence a significant saving in terms of cost to consumers

.Web intends to set an example when it comes to abuse mitigation and preventing abuse within .Web. To this effect we have created unprecedented Abuse mitigation policies and Rights protection mechanisms that go significantly above and beyond mandatory requirements and common practice. These are detailed in our response to Q28. We strongly believe these practices will result in a significant reduction in online abuse and considerable savings for end users of .Web. We similarly hope to set an example for other TLDs and cooperate with the industry in creating a clean internet experience for internet users.

2. COST BENEFIT ANALYSIS

There has been considerable debate within the community concerning the cost benefit analysis of launching new gTLDs. We strongly believe that the launch of new gTLDs and our implementation of .Web will add considerable value and result in a net positive effect on Registrants and end-users worldwide.

We recognize that there will be a post launch review of the New gTLD Program, from the perspective of assessing therelative costs and benefits achieved in the expanded gTLD space.

To this extent we would like to offer the following pointers concerning .Web as well as the general expansion of the new gTLD space in determining the net positive value generated for Registrants and end users –

* .Web will reduce overall cost for end-users in combating fraud and other forms of online abuse by implementing pioneering processes and anti-abuse policies as described in our

response to Q28. Billions of dollars are spent worldwide combating various forms of fraud such as malware, phishing, spamming etc. Our abuse policies will result in overall reduction of these forms of abuses within .Web resulting in a considerable reduction in global costs spent towards combating these abuses. We also strongly believe that introduction of new gTLDs will result in increased competition which will drive significant innovation as well as competitive pressures for everyone in the industry to improve their abuse mitigation processes resulting in overall cost reduction for end-users

* The value of a Registrant getting the name they want is immeasurably larger than any costs resulting from expansion of the namespace. DotWeb Inc. is a subsidiary within the Directi Group which owns and operates several ICANN Accredited Registrars. Our stats show that 70% of the users who check for a .com domain name do not get their desired name. Until this launch of the new gTLD program there were very limited alternatives and none very viable/desirable for Registrants to choose from. .Web will expand the namespace thus providing a higher probability for new Registrants to obtain names they desire

* In general increased competition always results in pricing benefits for Registrants. .Web will provide additional options to new Registrants resulting in overall benefits to Registrants

This completes our response to Q18(c).

Community-based Designation

19. Is the application for a community-based TLD?

No

20(a). Provide the name and full description of the community that the applicant is committing to serve.

20(b). Explain the applicant's relationship to the community identified in 20(a).

20(c). Provide a description of the community-based purpose of the applied-for gTLD.

20(d). Explain the relationship between the applied-for gTLD string and the community identified in 20(a).

20(e). Provide a description of the applicant's intended registration policies in support of the community-based purpose of the applied-for gTLD.

20(f). Attach any written endorsements from institutions/groups representative of the community identified in 20(a).

Attachments are not displayed on this form.

Geographic Names

21(a). Is the application for a geographic name?

No

Protection of Geographic Names

22. Describe proposed measures for protection of geographic names at the second and other levels in the applied-for gTLD.

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. This response describes protection of geographic names as implemented by ARI.

1. PROTECTION OF GEOGRAPHIC NAMES

In accordance with Specification 5 of the New gTLD Registry Agreement, we will initially reserve all geographic names at the second level, and at all other levels within the TLD at which the registry operator provides for registrations.
ARI supports this requirement by using the following internationally recognised lists to develop a comprehensive master list of all geographic names that are initially reserved:

- The 2-letter alpha-2 code of all country and territory names contained on the ISO 3166-1 list, including all reserved and unassigned codes [http://www.iso.org/iso/support/country_codes/iso_3166_code_lists/iso-3166-1_decoding_table.htm].

- The short form (in English) of all country and territory names contained on the ISO 3166-1 list, including the European Union, which is exceptionally reserved on the ISO 3166-1 List, and its scope extended in August 1999 to any application needing to represent the name European Union [http://www.iso.org/iso/support/country_codes/iso_3166_code_lists/iso-3166-1_decoding_table.htm#EU].

- The United Nations Group of Experts on Geographical Names, Technical Reference Manual for the Standardisation of Geographical Names, Part III Names of Countries of the World. This lists the names of 193 independent States generally recognised by the international community

in the language or languages used in an official capacity within each country and is current as of August 2006[http://unstats.un.org/unsd/geoinfo/ungegn/docs/pubs/UNGEGN%20tech%20ref%20manual_m87_combined.pdf].

– The list of UN member states in sixofficial UN languages prepared by the Working Group on Country Names of the United Nations Conference on the standardisation of Geographical Names [http://unstats.un.org/unsd/geoinfo/UNGEGN/docs/9th-uncsgn-docs/econf/9th_UNCSGN_e-conf-98-89-add1.pdf].

Names on this reserved list in ARI's registry system are prevented from registration.
A corresponding list of geographic names will also be available to the public via our website, to inform Registrars and potential registrants of reserved names. The lists noted above, are regularly monitored for revisions, therefore the reserved list (both within the registry and publicly facing) will be continually updated to reflect any changes.

In addition to these requirements, ARI are able to support the wishes of the Governmental Advisory Council (GAC) or any individual Government in regard to the blocking of individual terms on a case by case basis. ARI's registry system allows such additions to be made by appropriately authorised staff, with no further system development changes required.

The following applies to all Domain Names contained within the registry's reserved list:

– Attempts to register listed Domain Names will be rejected.
– WhoIs queries for listed Domain Names will receive responses indicating their reserved status.
– Reserved geographic names will not appear in the TLD zone file.
– DNS queries for reserved domain names will result in an NXDOMAIN response.

2. PROCEDURES FOR RELEASE

We understand that if we wish to release the reserved names at a later date, this will require agreement from the relevant government(s) or review by the GAC, and subsequent approval from ICANN.

This completes our response to Q22.

Registry Services

23. Provide name and full description of all the Registry Services to be provided.

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. This response describes the Registry Services for our TLD, as provided by ARI.

1. INTRODUCTION

ARI's Managed TLD Registry Service is a complete offering, providing all of the required Registry services. What follows is a description of each of those services.

2. REGISTRY SERVICES

The following sections describe the registry services provided. Each of these services has, where required, been designed to take into account the requirements of consensus policies as documented here:
[http://www.icann.org/en/resources/Registrars/consensus-policies]

2.1 RECEIPT OF DATA FROM REGISTRARS

The day-to-day functions of the Registry, as perceived by Internet users, involves the receipt of data from Registrars and making the necessary changes to the SRS database. Functionality such as the creation, renewal and deletion of domains by Registrars, on behalf of Registrants, is provided by two separate systems:

* An open protocol -based provisioning system commonly used by Registrars with automated domain management functionality within their own systems.

* A dedicated website providing the same functionality for user interaction.

Registrants (or prospective Registrants) who wish to manage their existing domains or credentials, register new domains or delete their domains will have their requests carried out by Registrars using one of the two systems described below.
ARI operates Extensible Provisioning Protocol (EPP) server software and distributes applicable toolkits to facilitate the receipt of data from Registrars in a common format. EPP offers a common protocol for Registrars to interact with SRS data and is favoured for automating such interaction in the Registrar's systems. In addition to the EPP server, Registrars have the ability to use a web -based management interface (SRS Web Interface), which provides functions equivalent to the EPP server functionality.

2.1.1 EPP

The EPP software allows Registrars to communicate with the SRS using a standard protocol. The EPP server software is compliant with all appropriate RFCs and will be updated to comply with any relevant new RFCs or other new standards, as and when they are finalised. All standard EPP operations on SRS objects are supported.

Specifically, the EPP service complies with the following standards:

* RFC 5730 Extensible Provisioning Protocol (EPP).
* RFC 5731 Extensible Provisioning Protocol (EPP) Domain Name Mapping.
* RFC 5732 Extensible Provisioning Protocol (EPP) Host Mapping.
* RFC 5733 Extensible Provisioning Protocol (EPP) Contact Mapping.
* RFC 5734 Extensible Provisioning Protocol (EPP) Transport over TCP.
* RFC 5910 Domain Name System (DNS) Security Extensions for the Extensible Provisioning Protocol (EPP).
* RFC 3915 Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol (EPP).
* Extensions to ARI's EPP service comply with RFC 3735 Guidelines for Extending the Extensible Provisioning Protocol (EPP).

2.1.1.1 SECURITY FOR EPP SERVICE

To avoid abuse and to mitigate potential fraudulent operations, the EPP server software uses a number of security mechanisms that restrict the source of incoming connections and prescribe the authentication and authorisation of the client. Connections are further managed by command rate limiting and are restricted to only a certain number for each Registrar, to help reduce unwanted fraudulent and other activities. Additionally, secure communication to the EPP interface is required, lowering the likelihood of the authentication mechanisms being compromised.

The EPP server has restrictions on the operations it is permitted to make to the data within the Registry database. Except as allowed by the EPP protocol, the EPP server cannot update the credentials used by Registrars for access to the SRS. These credentials include those used by Registrars to login to ARI's SRS Web Interface and the EPP service.

Secure communication to the EPP server is achieved via the encryption of EPP sessions. The Registry system and associated toolkits support AES 128 and 256 via TLS.

All communication between the Registrar or the Registrars systems and the SRS is encrypted using at least 128 bit encryption which been designated as 'Acceptable' till '2031 and beyond' by NIST Special Publication 800-57.

The Production and Operational Testing and Evaluation (OTE) EPP service is protected behind a secure firewall that only accepts connections from registered IP addresses. Registrars are required to supply host IP addresses that they intend to use to access the EPP service.

Certificates are used for encrypted communications with the Registry. Registrars require a valid public/private key pair signed by the ARI CA to verify authenticity. These certificates are used to establish a TLS secure session between client and server.

EPP contains credential elements in its specification which are used as an additional layer of authentication. In accordance with the EPP specification, the server does not allow client sessions to carry out any operations until credentials are verified.

The EPP server software combines the authentication and authorisation elements described above to ensure the various credentials supplied are associated with the same identity. This verification requires that:
* The username must match the common name in the digital certificate.
* The certificate must be presented from a source IP listed against the Registrar whose common name appears in the certificate.
* The username and password must match the user name and password listed against the Registrar's account with that source IP address.

To manage normal operations and prevent an accidental or intentional Denial of Service, the EPP server can be configured to rate limit activities by individual Registrars. Further details are provided for in Q24 and Q25.

2.1.1.2 STABILITY CONSIDERATIONS

The measures that restrict Registrars to a limit of connections and operations for security purposes also serve to keep the SRS and the EPP server within an acceptable performance and resource utilisation band. Therefore, scaling the service is an almost linear calculation based on well-defined parameters.

The EPP server offers consistent information between Registrars and the SRS Web Interface. The relevant pieces of this information are replicated to the DNS within seconds of alteration, thus ensuring that a strong consistency between the SRS and DNS is maintained at all times.

2.1.2 SRS WEB INTERFACE

The Registry SRS Web Interface offers Registrars an alternative SRS interaction mechanism to the EPP server. Available over HTTPS, this interface can be used to carry out all operations which would otherwise occur via EPP, as well as many others. Registrars can use the SRS Web Interface, the EPP server interface or both – with no loss of consistency within the SRS.

2.1.2.1 SECURITY AND CONSISTENCY CONSIDERATIONS FOR SRS WEB INTERFACE

The SRS Web Interface contains measures to prevent abuse and to mitigate fraudulent operations. By restricting access, providing user level authentication and authorisation, and protecting the communications channel, the application limits both the opportunity and scope of security compromise.

Registrars are able to create individual users that are associated with their Registrar account. By allocating the specific operations each user can access, Registrars have full control over how their individual staff members interact with the SRS. Users can be audited to identify which operations were conducted and to which objects those operations were applied.

A secure connection is required before credentials are exchanged and once authenticated. On login, any existing user sessions are invalidated and a new session is generated, thereby mitigating session-fixation attacks and reducing possibilities that sessions could be compromised.

All communication between the Registrar or the Registrars systems and the SRS is encrypted using at least 128 bit encryption which been designated as 'Acceptable' till '2031 and beyond' by NIST Special Publication 800-57.

2.1.3 SECURING AND MAINTAINING CONSISTENCY OF REGISTRY-REGISTRAR INTERACTION SYSTEMS

ARI ensures all systems through which Registrars interact with the SRS remain consistent with each other and apply the same security rules. Additionally, ARI also ensures that operations on SRS objects are restricted to the appropriate entity. For example:

* In order to initiate a transfer a Registrar must provide the associated domain password (authinfo) which will only be known by the Registrant and the current sponsoring Registrar.
* Only sponsoring Registrars are permitted to update Registry objects.

All operations conducted by Registrars on SRS objects are auditable and are identifiable to the specific Registrar's user account, IP address and the time of the operation.

2.2 DISSEMINATE STATUS INFORMATION OF TLD ZONE SERVERS TO REGISTRARS

The status of TLD zone servers and their ability to reflect changes in the SRS is of great importance to Registrars and internet users alike. ARI will ensure that any change from normal operations is communicated to the relevant stakeholders as soon as is appropriate. Such communication might be prior to the status change, during the status change and/or after the status change (and subsequent reversion to normal) – as appropriate to the party being informed and the circumstance of the status change.

Normal operations are those when:
* DNS servers respond within SLAs for DNS resolution.
* Changes in the SRS are reflected in the zone file according to the DNS update time SLA.

The SLAs are those from Specification 10 of the Registry Agreement.
A deviation from normal operations, whether it is registry wide or restricted to a single DNS node, will result in the appropriate status communication being sent.

2.2.1 COMMUNICATION POLICY

ARI maintains close communication with Registrars regarding the performance and consistency of the TLD zone servers.

A contact database containing relevant contact information for each Registrar is maintained. In many cases, this includes multiple forms of contact, including email, phone and physical mailing address. Additionally, up -to -date status information of the TLD zone servers is provided within the SRS Web Interface.

Communication using the Registrar contact information discussed above will occur prior to any maintenance that has the potential to effect the access to, consistency of, or reliability of the TLD zone servers. If such maintenance is required within a short time frame, immediate communication occurs using the above contact information. In either case, the nature of the maintenance and how it affects the consistency or accessibility of the TLD zone servers, and the estimated time for full restoration, are included within the communication.

That being said, the TLD zone server infrastructure has been designed in such a way that we expect no down time. Only individual sites will potentially require downtime for maintenance; however the DNS service itself will continue to operate with 100% availability.

2.2.2 SECURITY AND STABILITY CONSIDERATIONS

ARI restricts zone server status communication to Registrars, thereby limiting the scope for malicious abuse of any maintenance window. Additionally, ARI ensures Registrars have effective operational procedures to deal with any status change of the TLD nameservers and will seek to align its communication policy to those procedures.

2.3 ZONE FILE ACCESS PROVIDER INTEGRATION

Individuals or organisations that wish to have a copy of the full zone file can do so using the Zone Data Access service. This process is still evolving; however the basic requirements are unlikely to change. All registries will publish the zone file in a common format

accessible via secure FTP at an agreed URL.

ARI will fully comply with the processes and procedures dictated by the Centralised Zone Data Access Provider (CZDA Provider or what it evolves into) for adding and removing Zone File access consumers from its authentication systems. This includes:

* Zone file format and location.
* Availability of the zone file access host via FTP.
* Logging of requests to the service (including the IP address, time, user and activity log).
* Access frequency.

2.4 ZONE FILE UPDATE

To ensure changes within the SRS are reflected in the zone file rapidly and securely, ARI updates the zone file on the TLD zone servers using software compliant with RFC 2136 (Dynamic Updates in the Domain Name System (DNS UPDATE)) and RFC 2845 (Secret Key Transaction Authentication for DNS (TSIG)).

This updating process follows a staged but rapid propagation of zone update information from the SRS, outwards to the TLD zone servers – which are visible to the Internet. As changes to the SRS data occur, those changes are updated to isolated systems which act as the authoritative Primary server for the zone, but remain inaccessible to systems outside ARI’s network. The primary servers notify the designated Secondary servers, which service queries for the TLD zone from the public. Upon notification, the secondary servers transfer the incremental changes to the zone and publicly present those changes.

The protocols for dynamic update are robust and mature, as is their implementation in DNS software. The protocols’ mechanisms for ensuring consistency within and between updates are fully implemented in ARI’s TLD zone update procedures. These mechanisms ensure updates are quickly propagated while the data remains consistent within each incremental update, regardless of the speed or order of individual update transactions. ARI has used this method for updating zone files in all its TLDs including the .au ccTLD, pioneering this method during its inception in 2002.
Mechanisms separate to RFC 2136-compliant transfer processes exist; to check and ensure domain information is consistent with the SRS on each TLD zone server within 10 minutes of a change.

2.5 OPERATION OF ZONE SERVERS

ARI maintains TLD zone servers which act as the authoritative servers to which the TLD is delegated.

2.5.1 SECURITY AND OPERATIONAL CONSIDERATIONS OF ZONE SERVER OPERATIONS

The potential risks associated with operating TLD zone servers are recognised by ARI such that we will perform the steps required to protect the integrity and consistency of the information they provide, as well as to protect the availability and accessibility of those servers to hosts on the Internet. The TLD zone servers comply with all relevant RFCs for DNS and DNSSEC, as well as BCPs for the operation and hosting of DNS servers. The TLD zone servers will be updated to support any relevant new enhancements or improvements adopted by the IETF.

The DNS servers are geographically dispersed across multiple secure data centres in strategic locations around the world. By combining multi-homed servers and geographic diversity, ARI’s zone servers remain impervious to site level, supplier level or geographic level operational disruption.

The TLD zone servers are protected from accessibility loss by malicious intent or misadventure, via the provision of significant over-capacity of resources and access paths. Multiple independent network paths are provided to each TLD zone server and the query servicing capacity of the network exceeds the extremely conservatively anticipated peak load requirements by at least 10 times, to prevent loss of service should query loads significantly increase.

As well as the authentication, authorisation and consistency checks carried out by the

Registrar access systems and DNS update mechanisms, ARI reduces the scope for alteration of DNS data by following strict DNS operational practices:
* TLD zone servers are not shared with other services.
* The Primary authoritative TLD zone server is inaccessible outside ARI's network.
* TLD zone servers only serve authoritative information.
* The TLD zone is signed with DNSSEC and a DNSSEC Practice⁄Policy Statement published.

2.6 DISSEMINATION OF CONTACT OR OTHER INFORMATION

Registries are required to provide a mechanism to identify the relevant contact information for a domain. The traditional method of delivering this is via the Whois service, a plain text protocol commonly accessible on TCP port 43. ARI also provides the same functionality to users via a web -based Whois service. Functionality remains the same with the web -based service, which only requires a user to have an Internet browser.

Using the Whois service, in either of its forms, allows a user to query for domain -related information. Users can query for domain details, contact details, nameserver details or Registrar details.

A Whois service, which complies with RFC 3912, is provided to disseminate contact and other information related to a domain within the TLD zone.

2.6.1 SECURITY AND STABILITY CONSIDERATIONS

ARI ensures the service is available and accurate for Internet users, while limiting the opportunity for its malicious use. Many reputation and anti-abuse services rely on the availability and accuracy of the Whois service, However the potential for abuse of the Whois service exists.

Therefore, certain restrictions are made to the access of Whois services, the nature of which depend on the delivery method – either web -based or the traditional text -based port 43 service. In all cases, there has been careful consideration given to the benefits of Whois to the Internet community, as well as the potential harm to Registrants - as individuals and a group - with regard to Whois access restrictions.

The Whois service presents data from the Registry Database in real time. However this access is restricted to reading the appropriate data only. The Whois service does not have the ability to alter data or to access data not related to the Whois service. The access limitations placed on the Whois services prevent any deliberate or incidental denial of service that might impact other Registry Services.

Restrictions placed on accessing Whois services do not affect legitimate use. All restrictions are designed to target abusive volume users and to provide legitimate users with a fast and available service. ARI has the ability to 'whitelist' legitimate bulk users of Whois, to ensure they are not impacted by standard volume restrictions.

The data presentation format is consistent with the canonical representation of equivalent fields, as defined in the EPP specifications and ICANN agreement.

2.6.1.1 PORT 43 WHOIS

A port 43 -based Whois service complying with RFC 3912 is provided and will be updated to meet any other relevant standards or best practice guidelines related to the operation of a Whois service.
While the text -based service can support thousands of simultaneous queries, it has dynamic limits on queries per IP address to restrict data mining efforts. In the event of identified malicious use of the service, access from a single IP address or address ranges can be limited or blocked.

2.6.1.2 WEB -BASED WHOIS

ARI's web -based Whois service provides information consistent with that contained within the SRS.

The web -based Whois service contains an Image Verification Check (IVC) and query limits per IP address. These restrictions strike a balance between acceptable public usage and abusive use or data mining. The web -based Whois service can blacklist IP addresses or ranges to prevent abusive use of the service.

2.6.1.3 SEARCHABLE WHOIS

ARI will provide a Web-based Searchable Whois Service for the identification of domain names having similar registration data. This service, deployed as a web-interface alongside the SRS Web Interface, is restricted to pre-authorised clients.

The service is made available to authorized third parties. ARI will perform relevant background checks on a user before providing them with access to the searchable whois. The user will be required to change their password on first successful login, and every 6 months thereafter. Clients that have not used the service in a 3-month period will have their access revoked. ARI will periodically review the information submitted by the client to ensure that contact and usage information is up to date.

Access is logged and monitored to protect against abuse of this service. All searches are logged with the client and timestamp of the request. IP address, port, and browser information is collected in the event that this information is required to assist in identifying the user. The use of HTTPS is enforced for the entire service to prevent exposure of the information from client-side or middle-box caches.

ARI will conduct periodic audits of query logs to identify usage patterns and identify potential occurrences of data mining. Usage patterns will be matched back to the client’s specified reason for use. The client may be suspended from use of the service if ARI believes that abuse is occurring.

Further details on this service are described in the answer to Question 262.7 IDNs—Internationalised Domain Names

An Internationalised Domain Name (IDN) allows registrants to register domains in their native language and have it display correctly in IDN aware software. This includes allowing a language to be read in the manner that would be common for its readers. For example, an Arabic domain would be presented right to left for an Arabic IDN aware browser.
The inclusion of IDNs into the TLD zones is supported by ARI. All the Registry services, such as the EPP service, SRS Web Interface and RDPS (web and port 43), support IDNs. However there are some stability and security considerations related to IDNs which fall outside the general considerations applicable individually to those services.

2.7.1 STABILITY CONSIDERATIONS SPECIFIC TO IDN

To avoid the intentional or accidental registration of visually similar chars, and to avoid identity confusion between domains, there are several restrictions on the registration of IDNs.

2.7.1.1 PREVENT CROSS LANGUAGE REGISTRATIONS

Domains registered within a particular language are restricted to only the chars of that language. This avoids the use of visually similar chars within one language which mimic the appearance of a label within another language, regardless of whether that label is already within the DNS or not.

2.7.1.2 INTER-LANGUAGE AND INTRA-LANGUAGE VARIANTS TO PREVENT SIMILAR REGISTRATIONS

ARI restricts child domains to a specific language and prevents registrations in one language being confused with a registration in another language, for example Cyrillic a (U+0430) and Latin a (U+0061).

2.8 DNSSEC

DNSSEC provides a set of extensions to the DNS that allow an internet user (normally the

resolver acting on a user's behalf) to validate that the DNS responses they receive were not manipulated en-route.
This type of fraud, commonly called 'man in the middle', allows a malicious party to misdirect internet users. DNSSEC allows a domain owner to sign their domain and to publish the signature, so that all DNS consumers who visit that domain can validate that the responses they receive are as the domain owner intended.

Registries, as the operators of the parent domain for registrants, must publish the DNSSEC material received from registrants, so that Internet users can trust the material they receive from the domain owner. This is commonly referred to as a 'chain of trust'. Internet users trust the root (operated by IANA), which publishes the registries' DNSSEC material, therefore registries inherit this trust. Domain owners within the TLD subsequently inherit trust from the parent domain when the registry publishes their DNSSEC material.

In accordance with new gTLD requirements, the TLD zone will be DNSSEC signed and the receipt of DNSSEC material from Registrars for child domains is supported in all provisioning systems. Recommendation 26 calls for DNSSEC deployment at each zone and subsequent sub-zones at Registry, Registrar and Registrant level. Our compliance wrt the same is detailed in Q43.

2.8.1 STABILITY AND OPERATIONAL CONSIDERATIONS FOR DNSSEC

2.8.1.1 DNSSEC PRACTICE STATEMENT

ARI's DNSSEC Practice Statement is included in our response to Question 43. The DPS following the guidelines set out in the draft IETF DNSOP DNSSEC DPS Framework document.

2.8.1.2 RECEIPT OF PUBLIC KEYS FROM REGISTRARS

The public key for a child domain is received by ARI from the Registrar via either the EPP or SRS Web Interface. ARI uses an SHA-256 digest to generate the DS Resource Record (RR) for inclusion into the zone file.

2.8.1.3 RESOLUTION STABILITY

DNSSEC is considered to have made the DNS more trustworthy; however some transitional considerations need to be taken into account. DNSSEC increases the size and complexity of DNS responses. ARI ensures the TLD zone servers are accessible and offer consistent responses over UDP and TCP.

The increased UDP and TCP traffic which results from DNSSEC is accounted for in both network path access and TLD zone server capacity. ARI will ensure that capacity planning appropriately accommodates the expected increase in traffic over time.

ARI complies with all relevant RFCs and best practice guides in operating a DNSSEC -signed TLD. This includes conforming to algorithm updates as appropriate. To ensure Key Signing Key Rollover procedures for child domains are predictable, DS records will be published as soon as they are received via either the EPP server or SRS Web Interface. This allows child domain operators to rollover their keys with the assurance that their timeframes for both old and new keys are reliable.

3. APPROACH TO SECURITY AND STABILITY

Stability and security of the Internet is an important consideration for the Registry system. To ensure that the Registry services are reliably secured and remain stable under all conditions, ARI takes a conservative approach with the operation and architecture of the Registry system.

By architecting all Registry Services to use the least privileged access to systems and data, risk is significantly reduced for other systems and the Registry services as a whole should any one service become compromised. By continuing that principal through to our procedures and processes, we ensure that only access that is necessary to perform tasks is given. ARI has a comprehensive approach to security modeled of the ISO27001 series of standards and explored further in the relevant questions of this response.

By ensuring all our services adhering to all relevant standards, ARI ensures that entities which interact with the Registry Services do so in a predictable and consistent manner. When variations or enhancements to services are made, they are also aligned with the appropriate interoperability standards.

This completes our response to Q23.

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q24 – ARI Background & Roles.pdf'. This response describes the SRS as implemented by ARI.

1. INTRODUCTION

ARI has demonstrated delivery of an SRS with exceptional availability, performance and reliability. ARI's SRS has successfully supported a large group of Registrars for ASCII and IDN based TLDs. ARI's SRS meets the following requirements:

* Resilient to wide range of security & availability threats
* Consistently exceeds performance & availability SLAs
* Allows capacity increase with minimal impact to service
* Provides fair & equitable provisioning for all Registrars

2. CAPACITY

ARI's SRS infrastructure was built to sustain 20M domain names at less than 50% utilization. Based on ARI's experience and industry analysis, ARI were able to calculate the conservative characteristics of a registry of this size.

Through conservative statistical analysis of the .au registry and data presented in the May 2011 ICANN reports for the .com & .net, .org, .mobi, .info, .biz and .asia [http://www.icann.org/en/resources/registries/reports] we know there is:

 * An average of 70 SRS TPS per domain, per month; and
 * A ratio of 3 query to 2 transform txs

For a Registry with 20M domains this indicates an expected monthly transaction volume of 1,400M txs (840M query and 560M transforms).

Through conservative comparison of .au registry numbers and the .net RFP response - specifically http://archive.icann.org/en/tlds/net-rfp/applications/sentan.htm we also know:

 * The peak daily txs is 6% of the monthly total (.au:6%, .net: 5%)
 * The peak 5 min txs is 5% of the peak daily (.au and .net: 5%)

Hence for 20M domains we expect a peak EPP tx rate of 14,000 TPS (5,600 transform TPS and 8,400 query TPS)
Through conservative statistical analysis of the .au registry we additionally know:

 * The avg no. of contacts/domain is 3.76 (overall not assigned)
 * The avg no. of hosts/domain is 2.28 (overall not assigned)

This translates into a requirement to store 75.2M contacts and 45.6M hosts.
Finally through real world observations of the .au registry, which has a comprehensive web interface when compared to those offered by current gTLD registries, we know that there is an avg of 0.5 HTTP requests/sec to the SRS web interface per registrar. We also know that this behaviour is reasonably flat. To support an estimated 1000 Registrars, would require into a HTTP request load of 500 requests/second.

For perspective on the conservativeness of this, the following was taken from data in the May 2011 ICANN reports referenced above:

* .info: ~7.8M. domain names peaks at ~1,400 TPS (projected peak TPS of ~3,600 with 20M)

* .com: ~98M domain names peaks at ~41,000 TPS (projected peak TPS of ~8,300 TPS with 20M)

* .org: ~9.3M domain names, peaks at ~1,400 TPS (projected peak TPS of ~3,100 with 20M)

After performing this analysis the projected TPS for .com was still the largest value seen. ARI's estimated value of 14,000 TPS for a registry with 20M Domains is roughly twice that of the .com projected peak of ~8300 TPS.

ARI benchmarked their SRS infrastructure and used the results to calculate the required computing resources for each of the tiers within the SRS architecture; allowing ARI to accurately estimate the required CPU, IOPS, storage and memory requirements for each server in the architecture, and the network bandwidth & and packet throughput requirements for the anticipated traffic. These capacity numbers were then doubled to account for unanticipated traffic spikes, errors in predictions, and headroom. Despite doubling numbers, effective estimated capacity is still reported as 20M. The technical resource allocations are explored in Q32.

ARI understand the limitations of these calculations but they serve as a best estimate of probable transaction load. Over and above this ARI has built significant overcapacity of resources and as the numbers themselves are more conservative than real world observations, we are confident these capacity numbers are sufficient.

.Web is projected to reach 471,482 domains at its peak volume and will generate 330 EPP TPS. This will consume 2.36% of the resources of the SRS infrastructure. As is evident ARI's SRS can easily accommodate this TLD's growth plans. See attachment 'Q24 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI expects to provide Registry services to 100 TLDs and a total of 12M domains by end of 2014. With all the TLDs and domains combined, ARI's SRS infrastructure will be only 60% utilized in 2014. The SRS infrastructure capacity can also be easily scaled as described in Q32

3. SRS ARCHITECTURE

ARI's SRS has the following major components:
* Network Infrastructure
* EPP Application Servers
* SRS Web Interface Application Servers
* SRS Database

Attachment 'Q24 – SRS.pdf' shows the SRS systems architecture and data flows. Detail on this architecture is in our response to Q32. ARI provides two distinct interfaces to the SRS: EPP and SRS Web. Registrar SRS traffic enters the ARI network via the redundant Internet link and passes (via the firewall) to the relevant application server for the requested service (EPP or SRS Web). ARI's EPP interface sustains high volume and throughput domain provisioning transactions for a large number of concurrent Registrar connections. ARI's SRS Web interface provides an alternative to EPP and provides features additional to those provided by the EPP interface.

3.1 EPP

ARI's EPP application server is based on EPP as defined in RFCs 5730 – 5734. Registrars send XML based transactions to a load balanced EPP interface which forwards to one of the EPP application servers. The EPP application server then processes the XML and converts the request into database calls that retrieve or modify registry objects in the SRS database. The EPP application server tier comprises of 3 independent servers with dedicated connections to the Registry database. Failure of any one of these servers will cause Registrar connections to automatically re-establish with one of the remaining servers. All EPP servers accept EPP both IPv4 & IPv6.

3.2 SRS WEB

The SRS Web application server is a Java web application. Registrars connect via the load balancer to a secure HTTPS listener running on the web servers. The SRS web application converts HTTPS requests into database calls which query or update objects in the SRS database. The SRS Web application server tier consists of 2 independent servers that connect to the database via JDBC. If one of these servers is unavailable the load balancer re-routes requests to the surviving server. These servers accept both IPv4 & IPv6.

3.3 SRS DATABASE

The SRS database provides persistent storage for domains and supporting objects. It offers a secure way of storing and retrieving objects provisioned within the SRS and is built on the Oracle 11g Enterprise Edition RDBMS. The SRS Database tier consists of four servers clustered using Oracle Real Application Clusters (RAC). In the event of failure of a database server, RAC will transparently transition its client connections to a surviving database host.

The SRS database is stored on a storage area network concurrently accessed by all of the database servers which supports N+N redundancy. The SAN consists of 2 switches, 2o control enclosures (each with dual controllers), and 2 expansion enclosures per control enclosure. Each database server host is configured with two 4-port Fibre Channel Host Bus Adaptors (HBAs). Each HBA has 2 SAN fabric connections, one to each SAN switch — providing a total of 4 fabric connections per database server.

Each SAN switch has dual redundant connections to each controller in each Control Enclosure. All disks under the control of a Control Enclosure are configured in a highly resilient RAID 10 array. The Storwize V7000 uses SAN mirroring technology to duplicate data across Control Enclosures. This SAN design provides protection against failure of any component within the Storage Area Network including complete loss of a Control Enclosure and associated expansion enclosures.

3.4 NUMBER OF SERVERS

EPP Servers – The EPP cluster consists of 3 EPP servers that can more than handle the anticipated 20M. .Web will utilize 2.36% of this at its peak volume. As the utilization increases ARI will add additional EPP servers ensuring the total utilization doesn't exceed 50% of total capacity. Adding a new server to the cluster can be done live without downtime and does not impact the infrastructure.

SRS Web Servers – The SRS Web cluster consists of 2 SRS Web servers that can more than handle the anticipated 20M. .Web will utilize 2.36% of this at its peak volume. As the utilization increases ARI will add additional SRS Web servers ensuring total utilization doesn't exceed 50% of total capacity. Adding a new server to the cluster can be done live without downtime and does not impact the infrastructure.

SRS DB Servers – The SRS DB cluster consists of 4 SRS DB servers that can more than handle the anticipated 20M. .Web will utilize 2.36% of this at its peak volume. As the utilization increases ARI will add additional SRS DB servers ensuring total utilization doesn't exceed 50% of total capacity. Adding a new server to the cluster can be done live without downtime and does not impact the infrastructure.

3.5 SRS SECURITY

ARI adopts a multi-layered security solution to protect the SRS. An industry leading firewall is deployed behind the edge router and is configured to only allow traffic on the minimum required ports and protocols. Access to the ARI EPP service is restricted to a list of known Registrar IPs.

An Intrusion Detection device is in-line with the firewall to monitor and detect suspicious activity.

All servers are configured with restrictive host based firewalls, intrusion detection, and SELinux. Direct root access to these servers is disabled and all access is audited and logged centrally.

The SRS database is secured by removal of non-essential features and accounts, and ensuring all remaining accounts have strong passwords. All database accounts are assigned the minimum privileges required to execute their business function.

All operating system, database, and network device accounts are subject to strict password management controls such as validity & complexity requirements.

Registrar access to the SRS via EPP or the Web interface is authenticated and secured with multi-factor authentication (NIST Level 3) and digital assertion as follows:

* Registrar’s source IP address must be allowed by the front-end firewalls. This source IP address is received from the Registrar via a secure communication channel from within the SRS Web interface;
* Registrar must use a digital certificate provided by ARI;
* Registrar must use authentication credentials that are provided by to the Registrar via encrypted email.

All communication between the Registrar or the Registrars systems and the SRS is encrypted using at least 128 bit encryption which been designated as ‘Acceptable’ till ‘2031 and beyond’ by NIST Special Publication 800-57.

3.6 SRS HIGH AVAILABILITY

SRS availability is of paramount importance. Downtime is eliminated or minimised where possible. The infrastructure contains no single points of failure. N+1 redundancy is used as a minimum, which not only protects against unplanned downtime but also allows ARI to execute maintenance without impacting service.

Redundancy is provided in the network with hot standby devices & multiple links between devices. Failure of any networking component is transparent to Registrar connections.

N+N redundancy is provided in the EPP and SRS Web application server tiers by the deployment of multiple independent servers grouped together as part of a load -balancing scheme. If a server fails the load balancer routes requests to the remaining servers.

N+N redundancy is provided in the database tier by the use of Oracle Real Application Cluster technology. This delivers active⁄active clustering via shared storage. This insulates Registrars from database server failure.

Complete SRS site failure is mitigated by the maintenance of a remote standby site – a duplicate of the primary site ready to be the primary if required.

The standby site database is replicated using real time transaction replication from the main database using Oracle Data Guard physical standby. If required the Data Guard database can be activated quickly and service resumes at the standby site.

3.7 SRS SCALABILITY

ARI’s SRS scales efficiently. At the application server level, additional computing resource can be brought on-line rapidly by deploying a new server online. During benchmarking this has shown near linear.

The database can be scaled horizontally by adding a new cluster node into the RAC cluster online. This can be achieved without disruption to connections. The SRS has demonstrated over 80% scaling at the database level, but due to the distributed locking nature of Oracle RAC, returns are expected to diminish as the number of servers approaches double digits. To combat this ARI ensures that when the cluster is 'scaled' more powerful server equipment is added rather than that equal to the current members. Capacity can be added to the SAN at any time without downtime increasing storage and IOPs.

Additional capacity can be added to the SAN at anytime without downtime. This would result in increasing storage and IOPs.

3.8 SRS INTER-OPERABILITY AND DATA SYNCHRONISATION

The SRS interfaces with a number of related Registry systems as part of normal operations.

3.8.1 DNS UPDATE

Changes made in the SRS are propagated to the DNS via an ARI proprietary DNS Update process. This process runs on the 'hidden' primary master nameserver and waits on a queue. It is notified when the business logic inserts changes into the queue for processing. The DNS Update process reads these queue entries and converts them into DNS update (RFC2136) commands that are sent to the nameserver. The process of synchronizing changes to SRS data to the DNS occurs in real-time.

3.8.2 WHOIS

The provisioned data supporting the SRS satisfies Whois queries. Thus the Whois and SRS share data sets and the Whois is instantaneously updated. Under normal operating conditions the Whois service is provided by the infrastructure at the secondary site in order to segregate the load and protect SRS from Whois demand (and vice versa). Whois queries that hit the standby site will query data stored in the standby database – maintained in near real-time using Oracle Active Data Guard. If complete site failure occurs Whois and SRS can temporarily share the same operations centre at the same site (capacity numbers are calculated for this).

3.8.3 ESCROW

A daily Escrow extract process executes on the database server via a dedicated database account with restricted read-only access. The results are then transferred to the local Escrow Communications server by SSH.

4. OPERATIONAL PLAN

ARI follow defined policies/procedures that have developed over time by running critical Registry systems. Some principals captured by these are:

* Conduct all changes & upgrades under strict and well-practised change control procedures
* test, test and test again
* Maintain Staging environments as close as possible to production infrastructure/configuration
* Eliminate all single points of failure
* Conduct regular security reviews & audits
* Maintain team knowledge & experience via skills transfer/training
* Replace hardware when no longer supported by vendor
* Maintain spare hardware for all critical components
* Execute regular restore tests of all backups
* Conduct regular capacity planning exercises
* Monitor everything from multiple places but ensure monitoring is not 'chatty'
* Employ best of breed hardware & software products & frameworks (such as ITIL, ISO27001 and Prince2)
* Maintain two distinct OT&E environments to support pre*production testing for Registrars

5. DESCRIPTION OF SLA, RELIABILITY & COMPLIANCE

ARI's SRS adheres to and goes beyond the scope of Specification 6 and Specification 10 of the Registry Agreement

ARI's EPP service is XML compliant and XML Namespace aware. It complies with the EPP protocol defined in RFC5730, and the object mappings for domain, hosts & contacts are compliant with RFC 5731, 5732 & 5733 respectively. The transport over TCP is compliant with RFC5734. The service also complies with official extensions to support DNSSEC, RFC5910, & Redemption Grace Period, RFC 3915.
ARI's SRS is sized to sustain a peak transaction rate of 14,000 TPS while meeting strict internal Service Level Agreements (SLAs). The monthly -based SLAs below are more stringent than those in Specification 10 (Section 2).
EPP Service Availability: 100%
EPP Session Command Round Trip Time (RTT): 〈=1000ms for 95% of commands
EPP Query Command Round Trip Time (RTT): 〈=500ms for 95% of commands
EPP Transform Command Round Trip Time (RTT): 〈=1000ms for 95% of commands
SRS Web Interface Service Availability: 99.9%
ARI measures the elapsed time of every query, transform and session EPP transaction, and calculate the percentage of commands that fall within SLA on a periodic basis. If percentage value falls below configured thresholds on-call personnel are alerted.
SRS availability is measured by ARI's monitoring system which polls both the EPP and SRS Web services status. These checks are implemented as full end to end monitoring scripts that mimic user interaction, providing a true representation of availability. These 'scripts' are executed from external locations on the Internet.

6. RESOURCES

This function will be performed by ARI. ARI staff are industry leading experts in domain name registries with the experience and knowledge to deliver outstanding SRS performance.

The SRS is designed, built, operated and supported by the following ARI departments:

* Products and Consulting team (7 staff)
* Production Support Group (27 staff)
* Development Team (11 staff)

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q24 – ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.

ARI provides registry backend services to 5 TLDs and has a vast wealth of experience in estimating the number of resources required to support a Registry System.

Based on past experience ARI estimates that the existing staff is adequate to support a Registry System that is supporting at least 50M domains. Since .Web projects 471,482 domains, 0.94% of these resources are allocated to this TLD. See attachment 'Q24 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required. Additional trained resources can be added to any of the above teams with a 2 month lead time.

7. FINANCIAL COSTS

The usage of the ARI's staff and Registry Systems is included in our contract with ARI attached to Q46. This cost is shown in the financial answers.

This completes our response to Q24.

25. Extensible Provisioning Protocol (EPP)

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q25 – ARI Background & Roles.pdf'. This response describes the Extensible Provisioning Protocol (EPP) interface as implemented by ARI.

1. INTRODUCTION

ARI's EPP service is XML compliant and XML Namespace aware. The service complies with the EPP protocol defined in RFC5730, and the object mappings for domain, hosts and contacts are compliant with RFC5731-3 respectively. The transport over TCP is implemented in compliance with RFC5734. The service also complies with the official extensions to support DNSSEC, RFC5910 and Redemption Grace Period, RFC3915. ARI implemented EPP draft version 0.6 in 2002, then migrated to EPP RFC 1.0 on its publishing in 2004. The system has operated live since 2002 in the .au ccTLD.
Descriptions in this response follow the terminology used in the EPP RFCs. when referring to the software involved in the process, ARI's EPP interface is called the server, and the software used by Registrars is called the client.

2. TRANSPORT LAYER

The ARI EPP service implements the RFC5734 – EPP Transport over TCP. Connections are allowed using TLSv1 encryption, optionally supporting SSLv2 Hello for compatibility with legacy clients. AES cipher suites for TLS as described in RFC3268 are the only ones allowed.

2.1 AUTHENTICATION

Registrar access to the EPP interface is authenticated and secured with multi-factor authentication (NIST Level 3) and digital assertion as follows. Registrars must:

* Present a certificate, during TLS negotiation, signed by the ARI Certificate Authority (CA). The server returns a certificate also signed by the ARI CA. Not presenting a valid certificate results in session termination. ARI requires that the Common Name in the subject field of the certificate identifies the Registrar.

* Originate connections from an IP address that is known to be assigned to the Registrar with that Common Name.
** Registrar must use authentication credentials provided to the Registrar via encrypted email

* Registrars aren't able to exceed a fixed number of concurrent connections. The connection limit is prearranged and designed to prevent abuse of Registrars' systems from affecting the Registry. The limit is set to reasonable levels for each Registrar, but can be increased to ensure legitimate traffic is unaffected. If any of the above conditions aren't met the connection is terminated.

All communication between the Registrars and the EPP service is encrypted using at least 128 bit encryption which been designated as 'Acceptable' till '2031 and beyond' by NIST Special Publication 800-57.

2.2 CONNECTION CLOSE

The server may close the connection as a result of a logout, an error where the state of the connection is indeterminate, or after a timeout. Timeout occurs where no complete EPP message is received on the connection for 10 minutes.

3. EPP PROTOCOL

This section describes the interface relating to the EPP protocol described in RFC5730. This includes session management, poll message functionality and Object mappings for domains, hosts and contacts.

3.1 SESSION MANAGEMENT

Session management refers to login and logout commands, used to authenticate and end a session with the SRS. The Login command is used to establish a session between the client and the server. This command succeeds when:
– The username supplied matches the Common Name in the digital certificate used in establishing the TLS session.
– The provided password is valid for the user.
– The user’s access to the system isn’t suspended.
The Logout command is used to end an active session. On processing a logout the server closes the underlying connection. The Hello command can be used as a session keep-alive mechanism.

3.2 SERVICE MESSAGES

Offline notifications pertaining to certain events are stored in a queue. The client is responsible for polling this queue for new messages and to acknowledge read messages. Messages include notification about server modification of sponsored objects, transfer operations, and balance thresholds.

4. EPP OBJECT MAPPINGS

This section covers the interface for the 3 core EPP objects; domain, host and contact objects, as per RFC5731, 5732, & 5733 respectively.

The EPP domain, contact and host object mapping describes an interface for the check, info, create, delete, renew (domain only), transfer (domain & contact only) and update commands. For domain objects The server doesn’t support the use of host attributes as described by RFC5731, but rather uses host objects as described by RFC5731 and RFC5732. Details of each command are:.

* Check command: checks availability of 1 or more domain, contact or host objects in the SRS. Domain names will be shown as unavailable if in use, invalid or reserved, other objects will be unavailable if in use or invalid.

* info command: retrieves the information of an object provisioned in the SRS. Full information is returned to the sponsoring client or any client that provides authorisation information for the object. Non-sponsoring clients are returned partial information (no more than is available in the WhoIs).

* Create command: provisions objects in the SRS. To ascertain whether an object is available for provisioning, the same rules for the check command apply.

* Delete command: begins the process of removing an object from the SRS. Domain names transition into the redemption period and any applicable grace periods are applied. domain names within the Add Grace Period are purged immediately. All other objects are purged immediately if they are not linked.

* Renew command (domain only): extends the registration period of a domain name. The renewal period must be between 1 to 10 years inclusive and the current remaining registration period, plus the amount requested in the renewal mustn’t exceed 10 years.

* Transfer command (domain and contact only): provides several operations for the management of the transfer of object sponsorship between clients. clients that provide correct authorisation information for the object can request transfers. Domain names may be rejected from transfer within 60 days of creation or last transfer. The requesting client may cancel the transfer, or the sponsoring client may reject or approve the transfer. Both the gaining and losing clients may query the status of the current pending or last completed transfer.

* Update command: updates authorisation information, delegation information (domains), and registration data pertaining to an object.

5. NON-PROPRIETARY EPP MAPPINGS

ARI's EPP service implements 2 non-proprietary EPP mappings, to support the required domain name lifecycle and to provide & manage DNSSEC information. The relevant schema documents aren't provided as they are published as RFCs in the RFC repository.

5.1 GRACE PERIOD MAPPING

The Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol (as per RFC 3915) is used to support the domain name lifecycle as per existing TLDs.The update command is extended by the restore command to facilitate the restoration of previously deleted domains in the redemption period. This command defines 2 operations, request & report, described here:

* Request operation: requests the restoration of a domain.

* Report operation: completes the restoration by specifying the information supporting the restoration of the domain. The restore report must include a copy of the Whois information at both the time the domain was deleted & restored, including the restore reason.

5.2 DNSSEC MAPPING

The Domain Name System (DNS) Security Extensions Mapping for EPP, as per RFC5910, is used to support the provisioning of DNS Security Extensions. ARI requires clients use the Key Data Interface. Clients may associate a maximum of 4 keys per domain. The Registry system generates the corresponding DS data using the SHA-256 digest algorithm for the domain and any active variant domains.

ARI is aware of issues DNSSEC causes when transferring DNS providers – a transfer of Registrar usually means a change in DNS provider. DNSSEC key data won't be removed from the SRS or the DNS if a transfer occurs. It is the responsibility of and requires the cooperation of the Registrant, Registrars, and DNS providers, to provide a seamless transition. ARI observes progress with this issue and implements industry agreed solutions as available. DNSSEC information is included in info responses when the secDNS namespace in login.

6. PROPRIETARY MAPPING

The Registry system supports 3 additional EPP extensions where no published standard for the required functionality exists. Developed to conform to the requirements specified in RFC3735, these extensions include the provisioning of Internationalised Domain Names and domain name variants, and the association of arbitrary data with a domain name. These 3 extensions are introduced below, and further described in the attached schema documentation.

6.1 INTERNATIONALISED DOMAIN NAMES

ARI has developed an extension to facilitate the registration and management of Internationalised Domain Names as per RFCs 5890-5893 (collectively known as the IDNA 2008 protocol). This extension extends the domain create command and the info response.
The create command is extended to capture the language table identifier that identifies the corresponding IDN language table for the domain name. Additionally the extension requires the Unicode form to avoid an inconsistency with DNS-form, as per RFC 5891.

The domain info command is extended to identify the language tag and Unicode form provided in the initial create command. This information is disclosed to all querying clients that provided the extension namespace at login. This extension is documented in the attachment 'Q25 – idnadomain-1.0.pdf'.

6.2 VARIANT

ARI has developed an extension to facilitate the management of Domain Name variants. This extension extends the domain update command and the domain create and info responses. The domain update command is extended to allow the addition (activation) and removal (de-activation) of domain name variants subject to registry operator policy.

The domain create and info responses are extended to return the list of activated domain name variants. This information is disclosed to all querying clients that provided the extension

namespace at login. The extension is documented in the attachment ‘Q25 – variant-1.1.pdf’.

6.3 KEY-VALUE

ARI has developed an extension to facilitate the transport of arbitrary data between clients and the SRS without the need for developing EPP Extensions for each specific use-case. This extension extends the domain create and domain update transform commands and the domain info query command. This extension is documented in the attachment ‘Q25 – kv-1.0.pdf’.

7. ADDITIONAL SECURITY

The Registry system provides additional mechanisms to support a robust interface. The use of command rate limiting enables the Registry to respond to and withstand erroneous volumes of commands, while a user permission model provides fine-grained access to the EPP interface. These 2 mechanisms are described below.

7.1 RATE LIMITING

The Registry system supports command and global rate limits using a token-bucket algorithm. Limits apply to each connection to ensure fair and equitable use by all. Clients that exceed limits receive a command failed response message indicating breach of the limit.

7.2 USER PERMISSION MODEL

The Registry system supports a fine-grained permission model controlling access to each specific command. By default, clients receive access to all functionality; however it is possible to remove access to a specific command in response to abuse or threat to stability of the system. Clients that attempt a command they have lost permission to execute, receive an EPP command failed response indicating loss of authorisation.

8. COMPLIANCE

Compliance with EPP RFCs is achieved through design and quality assurance (QA).The EPP interface was designed to validate all incoming messages against the respective XML Schema syntax. The XML Schema is copied directly from the relevant RFCs to avoid any ambiguity on version used. Inbound messages that are either malformed XML or invalid are rejected with a 2400 response. Outbound messages are validated against the XML Schema, and if an invalid response is generated, it is replaced with a known valid pre-composed 2400 response, and logged for later debugging.

A QA process provides confidence that changes don’t result in regressions in the interface. Automated build processes execute test suites that ensure every facet of the EPP service (including malformed input, commands sequencing and synchronisation, and boundary values) is covered and compliant with RFCs and the EPP service specification. These tests are executed prior to committing code and automatically nightly. The final deliverable is packaged and tested again to ensure no defects were introduced in the packaging process.

New versions of the EPP Service follow a deployment schedule. The new version is deployed into an OT&E environment for Registrar integration testing. Registrars are encouraged during this stage to test their systems operate correctly. After a fixed time in OT&E without issue, new versions are scheduled for production deployment. This ensures incompatibilities with RFCs that made it through QA processes are detected in test environments prior reaching production.

ARI surveys Registrars for information about the EPP client toolkit. These surveys indicated that while many Registrars use ARI toolkits, several Registrars use either their own or that from another registry. The ability for Registrars to integrate with the ARI EPP service without using the supplied toolkit indicates the service is compliant with RFCs.

ARI is committed to providing an EPP service that integrates with third party toolkits and as such tests are conducted using said toolkits. Any issues identified during testing fall into the following categories:

* Third-party toolkit not compliant with EPP

* EPP service not compliant with EPP
* Both third-party toolkit and EPP service are compliant, however another operational issue causes an issue

Defects are raised and change management processes are followed. Change requests may also be raised to promote integration of third-party toolkits and to meet common practice.

9. CAPACITY

.Web is projected to reach 471,482 domains at its peak volume and will generate 330 EPP TPS. This will consume 2.36% of the EPP resources of the SRS infrastructure. ARI's SRS can easily accommodate this. These numbers were described in considerable detail in the capacity section of Q24.

10. RESOURCES

This function will be performed by ARI. ARI provides a technical support team to support Registrars and also provides Registrars with a tool kit (in Java and C++) implementing the EPP protocol. Normal operations for all Registry Services are managed by ARI's Production Support Group (PSG), who ensure the EPP server is available and performing appropriately.

Faults relating to connections with or functionality of the EPP server are managed by PSG. ARI monitors EPP availability and functionality as part of its monitoring practices, and ensures PSG staff are available to receive fault reports from Registrars any time. PSG has the appropriate network, Unix and application (EPP and load balancing) knowledge to ensure the EPP service remains accessible and performs as required. these ARI departments support EPP:

* Products and Consulting Team (7 staff)
* Production Support Group (27 staff)
* Development Team (11 staff)

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q25 – ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.

ARI provides registry backend services to 5 TLDs and has a vast wealth of experience in estimating the number of resources required to support a Registry System.

Based on past experience ARI estimates that the existing staff is adequate to support a Registry System that is supporting at least 50M domains. Since .Web projects 471,482 domains, 0.94% of these resources are allocated to this TLD. See attachment 'Q25 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required. Additional trained resources can be added to any of the above teams with a 2 month lead time.

11. FINANCIAL COSTS

The usage of the ARI's staff and Registry Systems is included in our contract with ARI attached to Q46. This cost is shown in the financial answers.

This completes our response to Q25.

26. Whois

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. For more background information on ARI please see the attachment 'Q26 – ARI Background & Roles.pdf'. This response describes the Whois interface as implemented by ARI.

1. INTRODUCTION

ARI's Whois service is for all domain names, contacts, nameservers and Registrars provisioned in the Registry database. This response describes the port 43, web and searchable whois interfaces, security controls to mitigate abuse, compliance with bulk access requirements for registration data, and the architecture delivering the service.

2. PORT 43 WHOIS SERVICE

Whois is available on TCP port 43 in accordance with RFC3912. Requests are made in semi-free text format and terminated by an ASCII CR & LF. The server responds with a semi-free text format, terminating the response by closing the connection.
To support Internationalised Domain Names and Localised Registration Data we assume the query is encoded in UTF-8 and sends responses encoded in UTF-8. UTF-8 is backwards compatible with the ASCII charset and its use is consistent with the IETF policy on charsets as defined in BCP 18 [http://tools.ietf.org/html/bcp18].

2.1 Query Format

By default Whois searches for domains. To facilitate the queries of other objects a keyword must be included before the search string. Supported keywords are:
* Domain
* Host/Nameserver
* Contact
* Registrar
Keywords are case-insensitive. The remainder of the input is the search string. Wildcard chars may be used in search strings to match zero or more chars (%), or match exactly one char. Wildcard chars must not appear in the first 5 chars.

2.2. RESPONSE FORMAT

The response consists -
* An object-specific response represented by multiple key/value pairs. Where no object could be found the response is 'No Data Found'
* query-related meta-information to identify data freshness
* legal disclaimer
This format is consistent with that prescribed in the Registry agreement.

2.3, DOMAIN DATA

Domain data is returned in response to a query with the keyword omitted, or with the 'domain' keyword. Domain queries return information on domains that are provisioned in the Registry database.
The IDN domains may be specified in either the ASCII-compatible encoded form or the Unicode form. Clients are expected to perform any mappings, in conformance with relevant guidelines such as those specified in RFC5894 and UTS46.
Variant domains may be specified in the search string and Whois will match (using case-insensitive comparison) and return information for the primary registered domain.
For queries containing wildcard chars, If only one domain name is matched its details are returned, If more than one domain name is matched then the first 50 matched domain names are listed.

2.3.1. INTERNATIONALISED DOMAIN NAMES

The Whois response format, prescribed in Specification 4, does not provide a mechanism to identify active variant domain names. ARI will include active variant domain names in Whois responses until a common approach for handling and display of variant names is determined.

2.3.2. RESERVED DOMAIN NAMES

Domain names reserved from allocation will have a specific response that indicates the domain is not registered but also not available.

2.4. NAMESERVER DATA

Nameserver data is returned in response to a query where the ‘nameserver’ or ‘host’ keywords have been used. Nameserver queries return information on hosts that are provisioned in the Registry.
The search string for a nameserver query can be either a hostname or IP. Queries using the hostname produce one result unless wildcards are used. Queries using the IP produce one or more results depending on the number of hostnames that match that address. Queries for the hostname are matched case-insensitively.
The quad-dotted notation is expected for IPv4 and the RFC3513 – IPv6 Addressing Architecture format for IPv6. Wildcards cannot be used for IP queries.

2.5. CONTACT DATA

Contact data is returned in response to a query where the ‘contact’ keyword was used. Contact queries return information on contacts that are provisioned in the Registry.
The search string for a contact query is the contact identifier. Contact identifiers are matched using a case-insensitive comparison. Wildcards cannot be used.

2.6. REGISTRAR DATA

Registrar data is returned in response to a query where the ‘Registrar’ keyword was used. Registrar queries return information on Registrar objects that are provisioned in the Registry.
The search string for a Registrar query can be name or IANA id. Queries using the name or the IANA id produce only one result. Queries for the name are matched using a case-insensitive comparison. Wildcards cannot be used.

2.7. NON-STANDARD DATA

The SRS supports domain-related data beyond that above. It may include information used to claim eligibility to participate in the sunrise process, or other arbitrary data collected using the Key-Value Mapping to the EPP. This information will be included in the Whois response after the last object-specific data field and before the meta-information.

3. WEB-BASED WHOIS SERVICE

Whois is also available via port 80 using HTTP, known as Web-based Whois. This interface provides identical query capabilities to the port 43 interface via an HTML form.

4. SECURITY CONTROLS

Whois has an in-built mechanism to blacklist malicious users for a specified duration. Blacklisted users are blocked by source IP address and receive a specific blacklisted notification instead of the normal Whois response.
Users may be blacklisted if ARI’s monitoring system determines excessive use. A whitelist is used to facilitate legitimate use by law enforcement agencies and other reputable entities.

5. BULK ACCESS

The Registry system complies with the requirements for the Periodic Access to Thin Registration Data and Exceptional Access to Thick Registration Data as described in Specification 4.

5.1. PERIODIC ACCESS TO THIN REGISTRATION DATA

ARI shall provide ICANN with Periodic Access to Thin Registration Data. The data will contain the elements as specified by ICANN. The format of the data will be consistent with the format specified for Data Escrow. The Escrow Format prescribes an XML document encoded in UTF-8. The generated data will be verified to ensure that it is well formed and valid.
The data will be generated every Monday for transactions committed up to and on Sunday unless otherwise directed by ICANN. The generated file will be made available to ICANN using SFTP.

Credentials, encryption material, and other parameters will be negotiated between ARI and ICANN using an out-of-band mechanism.

5.2 Exceptional Access to Thick Registration Data

If requested by ICANN, ARI shall provide exceptional access to thick registration data for a specified Registrar. The date will contain full information for the following objects:

* Domain names sponsored by the Registrar
* Hosts sponsored by the Registrar
* Contacts sponsored by the Registrar
* Contacts linked from domain names sponsored by the Registrar

As above The format of the data will be consistent with the format specified for Data Escrow. And will be made available to ICANN using SFTP.

6. CAPACITY

ARI's Whois infrastructure is built to sustain 20M domain names at less than 50% utilization. Based on ARI's experience running a high volume ccTLD registry (.au) and industry analysis, ARI were able to calculate the conservative characteristics of a registry of this size.

Through conservative statistical analysis of the .au registry and data presented in the May 2011 ICANN reports for the .com & .net, .org, .mobi, .info, .biz and .asia [http://www.icann.org/en/resources/registries/reports we know there is:

* An average of 30 Whois txs per domain, per month.

Which indicates an expected monthly transaction volume of 600M txs For a registry with 20M DUMs

Through conservative comparison of .au registry numbers and the .net RFP response - specifically http://archive.icann.org/en/tlds/net-rfp/applications/sentan.htm we also know:

* The peak daily transactions is 6% of the monthly total (.au:6%, .net: 5%)
* The peak 5 min is 5% of the peak day (.au:5%, .net: 0.6%)

Thus we expect a peak WhoIs tx rate of 6,000 TPS.

For perspective on the conservativeness of this, the following numbers were taken from data in the May 2011 ICANN reports referenced above:

* .info ~7.8M domain names, peaks at ~1,300 TPS (projected peak TPS of ~3,400 with 20M names).
* .mobi ~1M domain names, peaks at ~150 TPS (projected peak TPS of ~3,000 TPS with 20M names).
* .org ~9.3M domain names, peaks at ~1,300 TPS (projected peak TPS of ~2,800 with 20M names).

After performing this analysis the projected TPS for .info was still the largest value seen. ARI's estimated value of 6,000 TPS for a registry with 20M Domains is roughly twice that of the .info projected peak of ~3400 TPS.

ARI benchmarked their WhoIs infrastructure and used the results to calculate the required computing resources for each of the tiers within the WhoIs architecture – allowing ARI to accurately estimate the required CPU, IOPS, storage and memory requirements for each server within the architecture, as well as the network bandwidth and packet throughput requirements for the anticipated traffic. These capacity numbers were then doubled to account for unanticipated traffic spikes, errors in predictions and head room for growth. Despite doubling numbers, effective estimated capacity is still reported as 20 million domain names. The technical resource allocations are explored in question 32.

ARI understand the limitations of these calculations but they serve as a best estimate of probable transaction load. Over and above this ARI has built significant overcapacity of resources and as the numbers themselves are more conservative than real world observations, we are confident these capacity numbers are sufficient.
.Web is projected to reach 471,482 domains at its peak volume and will generate 141 WhoIs

transactions per second. This will consume 2.36% of the resources of the WhoIs infrastructure. As is evident ARI's WhoIs can easily accommodate this TLD's growth plans. See attachment 'Q26 – Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI expects to provide Registry services to 100 TLDs and a total of 12M domains by end of 2014. With all the TLDs and domains combined, ARI's WhoIs infrastructure will be only 60% utilized. The WhoIs infrastructure capacity can also be easily scaled as described in question 32

7. ARCHITECTURE

Whois uses a separate replica database independent of the SRS database. Oracle Data Guard ensures the two databases are synchronised in real-time. The Whois service is operated live from the SRS 'failover' site, with the SRS 'primary' site serving as the 'failover' site for the Whois service. Both sites have enough capacity to run both services simultaneously. The architecture and data flow diagrams are described below and shown in the attachment 'Q26 – WhoIs.pdf'

Traffic enters the network from the Internet through border routers and then firewalls. All traffic destined for this service except for TCP ports 43, 80 & 443 is blocked. Load balancers forward the request to one of the application servers running ARI built Whois software. Each server is connected to the database cluster through another firewall further restricting access to the. Each server uses a restricted Oracle user that has read only access to the Registry data and can only access the data that is relevant to the Whois queries. This ensures that in the unlikely event of an application server compromise the effects are limited.

All components are configured and provisioned to provide N+1 redundancy. Multiple Internet providers with separate upstream bandwidth suppliers are used. At least one additional component of all hardware exists, enabling maintenance without downtime. This configuration provides a service exceeding the availability requirements in Specification 10.

The use of load balancing allows addition of application servers with no downtime. From a database perspective, the ability to scale is enabled by utilising Oracle RAC database clustering.
The entire service, including routers, firewalls and application layer is IPv6 compatible and Whois is offered on both IPv4 and IPv6 interfaces. Detail about this architecture is available in our response to Question 32.

7.1. SYNCHRONIZATION

The Whois database is synchronised with the SRS database using Oracle Data Guard. Committed transactions in the SRS database are reflected in the Whois database in real-time. Should synchronisation break, Whois continues to operate with the latest available data until the issue is reconciled. The channel between the two sites consists of two independent dedicated point to point links as well as the Internet. Replication traffic flows via the dedicated links or if both links fail replication traffic flows over Internet tunnels.

7.2. INTERCONNECTIVITY WITH OTHER SERVICES

The WhoIs service is not directly interconnected with other registry services or systems. The software has been developed to provide the WhoIs service exclusively and retrieve response information from a database physically separate to the SRS transactional database. This database is updated as described in 'Synchronisation' above. The WhoIs servers log every request to a shared central repository that is logically separate from the WhoIs database. This repository is used for query counts, detection of data mining and statistical analysis on query trends.

7.3. IT AND INFRASTRUCTURE RESOURCES

The WhoIs service is provided utilizing Cisco networking equipment, IBM application servers &, IBM database servers and SAN. They are described in the attachment 'Q26 - WhoIs.pdf'. For more information on the IT infrastructure including server specifications and database capabilities please see Q32 & Q33.

8. COMPLIANCE

Compliance with WhoIs RFCs is achieved through design and QA.
QA processes provide confidence that any changes to the service don’t result in regression issues. Automated build processes execute test suites, prior to the committing of code and nightly, that ensure every facet of the WhoIs service is covered and compliant with RFCs. The final deliverable is packaged and tested again.
New versions follow a deployment schedule. The new version is deployed into an OT&E environment for registrar integration testing. After a fixed time in OT&E without issue, they are scheduled for production deployment. This ensures incompatibilities with RFCs that made it through QA processes are detected in test environments.
ARI is committed to providing a WhoIs service that integrates with third party tools without issue and as such tests are conducted using third party tools such as jWhoIs, a popular UNIX command line WhoIs client.
Defects are raised and follow the change management process for all issues where the WhoIs service has been determined to not comply with the RFCs.

9. SEARCHABLE WHOIS

ARI will provide a Web-based Searchable Whois Service restricted to pre-authorised clients.

9.1. DESCRIPTION OF SERVICE

The service provides search capabilities defined in Specification 4 and allows for:

* Exact-match on the registrar id, name server name, and name server’s IP address;
* Partial-match on domain name, contacts, address (street, city, state or province, postcode, country); and
* Boolean search capabilities.

Matches for contact name and all postal address fields are case-insensitive. The client is restricted to one concurrent search to prevent unnecessary load on the system. The results include a list of domain names that match the criteria. The service allows for addition or removal of search criterion to meet local laws.

9.2. AUTHORISATION OF CLIENTS

Potential clients will request access to this service by providing the following on fax:
* Name
* Organisation
* Position
* Contact information
* Reason
* Query volume
* IP address

Access will be approved after background checks. Access is logged and monitored to protect against abuse. The use of HTTPS is enforced for the entire service.

Periodic audits of query logs will be used to identify any occurrences of data mining to suspend abusive clients.

10. RESOURCES

This function will be performed by the following ARI departments:
* Products and Consulting team (7 staff)
* Production Support Group (27 staff)
* Development Team (11 staff)
* Legal, Abuse and Compliance Team (6 staff)
and the following departments outsourced to the Directi Group:
* Abuse and Compliance Team (20 staff)

The products and consulting team is responsible for product management of the Whois solution including working with clients and the industry to identify new features or changes required to the system.

ARI employ a development team responsible for the maintenance and continual improvement of the Whois software

ARI's Production Support Team ensures the successful operation of the Whois system. The team comprises Database Administrators, Systems Administrators and Network Administrators. This team routinely checks and monitors bandwidth, disk and CPU usages to plan and respond to expected increases in the volume of queries, and perform maintenance of the system including security patches and failover and recovery testing.

The Directi Group and ARI Abuse and compliance teams provide abuse monitoring detection mechanisms to block data mining. Additionally the support team in conjunction with both the Compliance teams administer requests for listing on the Whitelist, as well as requests for access to the searchable whois

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q26 – ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within. A detailed list of the Abuse and Compliance desk of Directi is provided in Q28.

ARI provides registry backend services to 5 TLDs and has a vast wealth of experience in estimating the number of resources required to support a Registry System.

Based on past experience ARI estimates that the existing staff is adequate to support a Registry System that is supporting at least 50M domains. Since .Web projects 471,482 domains, 0.94% of these resources are allocated to this TLD. See attachment 'Q26 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required. Additional trained resources can be added to any of the above teams with a 2 month lead time.

The Directi Group is protected against loss of staff due to its scale of operations. This is described in further detail in Q39

11. FINANCIAL COSTS

The usage of the ARI's staff and Registry Systems is included in our contract with ARI attached to Q46. This cost is shown in the financial answers.

The usage of Directi Group's staff is included in our contract with Directi attached to Q46. This cost is shown in the financial answers.

This completes our response to Q26.

27. Registration Life Cycle

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. For more background please see attachment 'Q27 – ARI Background & Roles.pdf'. This response describes the Registration Lifecycle as implemented by ARI.

1. INTRODUCTION

The lifecycle described matches current gTLD registries. All states, grace periods and transitions are supported by the EPP protocol as described in RFC5730 - 5734 & the Grace Period Mapping published in RFC3915. An overview is in attachment 'Q27 – Registration

Lifecycle.pdf'.

2. REGISTRATION PERIODS

The Registry supports registration up to 10 years and renewals for 1 to 10 years. Transfers extend registration by 1 year. The total validity period can't exceed 10 years.

3. STATES

The states that a domain can exist in are: Registered, Pending Transfer, Redemption, Pending Restore & Pending Delete.

All domain name statuses (RFC 3915, 5730-5734 and 5910) are covered below

3.1 REGISTERED

EPP Status: ok
In DNS: Yes
Allowed Operations: Update, Renew, Transfer (request) & Delete
The default state of a domain - No pending operations. The Sponsoring Registrar may update the domain.

3.2 PENDING TRANSFER

EPP Status: pendingTransfer
In DNS: Yes
Allowed Operations: Transfer (cancel, reject, approve)
another Registrar has requested transfer of the domain and it is not yet completed all transform operations, other than those to cancel, reject, or approve the transfer are rejected.

3.3 REDEMPTION

EPP Status:pendingDelete
RGP Status:redemptionPeriod
In DNS:No
Allowed Operations:Restore (request)

Domain has been deleted. The sponsor may request restoration of the domain. The domain continues to be withheld from the DNS unless restored. No transform operations other than restore allowed.

3.4 PENDING RESTORE

EPP Status:pendingDelete
RGP Status:pendingRestore
In DNS:No
Allowed Operations:Restore (report)
a restore request is pending. Sponsor must submit a restore report. The domain remains withheld from the DNS. No transform operations other than restore report allowed.

3.5 PENDING DELETE

EPP Status:pendingDelete
RGP Status:pendingDelete
In DNS:No
Allowed Operations:None
the Redemption Grace Period has lapsed and the domain is pending purge from the Registry. This state prohibits the sponsor from updating, restoring or modifying the domain for 5 days. At the end of this period the domain is purged and made available for registration.

4. GRACE PERIODS

The Registry system supports 4 grace periods: add, renew, auto-renew, and transfer, described below with consideration for overlap of grace periods. States described here are additional to those above.

4.1 ADD GRACE PERIOD

Length:5 days
RGP Status:addPeriod
Allows for the no-cost cancellation of a domain to rectify errors within 5 days from registration. The following rules apply for operations during this period:

* Delete: Sponsoring Registrar may delete the domain with immediate effect and receive a refund subject to the Add Grace Period Limits consensus policy.
* Renew: sponsor may renew the domain and is charged for the operation. The total period is extended by the renewal term, limited to 10 yr maximum.
* Transfer: The Registry system rejects transfers in the first 60 days after the initial registration as per ICANN Policy.
* Bulk Transfers: A bulk transfer is permitted during the Add Grace Period as per ICANN policy, and causes the Add Grace Period to not apply.

4.2 RENEW GRACE PERIOD

Length:5 days
RGP Status:renewPeriod
Allows the Sponsoring Registrar to undo a renewal within 5 days of the renewal command. The following rules apply for operations during this period:

* Delete: Sponsoring Registrar may delete the domain and receive a refund. The extension caused by the preceding renew is reversed and unless the domain is also in the Add Grace Period, the domain enters the Redemption state. If in the Add Grace Period it is deleted with immediate effect and available for registration.
* Renew: sponsor can renew a domain again and is charged for the operation, causing a second independent Renewal Grace Period to start. The total period is extended by the renewal term, limited to 10 yr maximum.
* Transfer: an approved transfer command ends the current Renew Grace Period without a refund and begins a Transfer Grace Period.
* Bulk Transfers: cause the Renew Grace Period to end without a refund, consequently registration periods are not changed.

4.3 AUTO-RENEW GRACE PERIOD

Length:45 days
RGP Status:autoRenewPeriod
Allows for domains to remain in the DNS past expiration giving time for the Registrar to obtain renewal confirmation from the Registrant.
This period lasts for 45 days after expiration. The following rules apply for operations during this period:

* Delete: the Registrar, may delete the domain and receive a refund. The domain enters the Redemption state.
* Renew: the Registrar can renew a domain again and is charged for the operation, causing a second independent Renewal Grace Period to start. The total period is extended by the renewal term, limited to 10 yr maximum.
* Transfer: an approved transfer command ends the current Auto-Renew Grace Period with a refund to the losing Registrar and begins a Transfer Grace Period. The registration period auto-renew extension is reversed and the registration is extended by the period specified in the transfer.
* Bulk Transfers: bulk transfers cause the Auto-Renew Grace Period to end without a refund consequently registration periods are not changed.

4.4 TRANSFER GRACE PERIOD

Length: 5 days

RGP Status:transferPeriod
Transfer Grace Period allows the Sponsoring Registrar to undo the registration period extension (due to a transfer command), via the deletion of a domain within 5 calendar days. The following rules apply for operations during this period:

* Delete: the Registrar may delete the domain and receive a transfer fee refund. The extension to the registration period of the preceding transfer is reversed and the Redemption state is entered.
* Renew: the Registrar can renew the domain causing a Renewal Grace Period to begin. The Registrar is charged and the total period is extended by the renewal term, limited to 10 yr maximum
* Transfer: The Registry system rejects transfers in the first 60 days after the initial registration as per ICANN Policy. Special situations requiring a transfer back to the losing Registrar are dealt with case by case manually.
* Bulk Transfers: bulk transfers cause the Transfer Grace Period to end without a refund; consequently registration periods are not changed.
The Transfer Grace Period does not have any impact on other commands.

4.5 REDEMPTION GRACE PERIOD

Length:30 days
RGP Status:as described in Redemption state
Redemption Grace Period refers to the period of time the domain spends in the Redemption state, starting after a domain is deleted. The Redemption state description provides information on operations during this period.

4.6 OVERLAP OF GRACE PERIODS

The 4 possible overlapping grace periods are:
* Add Grace Period with 1 or more Renew Grace Periods.
* Renew Grace Period with 1 or more other Renew Grace Periods.
* Transfer Grace Period with 1 or more Renew Grace Periods.
* Auto-Renew Grace Period with 1 or more Renew Grace Periods.
These are treated independently with respect to timelines however action that is taken has the combined effects of all grace periods still current.

4.6.1 TRANSFER CLARIFICATION

If several billable operations, including a transfer, are performed on a domain and it is deleted in the operations' grace periods, only those operations performed after/including the latest transfer are eligible for refund.

5. TRANSITIONS

5.1. AVAILABLE 〉 REGISTERED

Triggered by the receipt of a create command to register the domain. The Sponsoring Registrar is charged for the creation amount. this transition begins the Add Grace Period.

5.2 REGISTERED 〉 PENDING TRANSFER

Triggered by the receipt of a request transfer command. The transfer must result in domain registration extension – the gaining Registrar is charged for the transfer. Requests to transfer the domain within 60 days of creation or a previous transfer are rejected.

5.3 PENDING TRANSFER 〉 REGISTERED

Triggered by 1 of 4 operations:

* Cancel: the Gaining Registrar may cancel a transfer
* Reject: the Losing Registrar may reject the transfer
* Approve: the Losing Registrar may approve the transfer.
* Auto-Approve: If after 5 days, no action has been taken, the system approves the transfer.

In case of Cancel/Reject. The Gaining Registrar is refunded the transfer fee. The registration period remains unchanged and all grace periods existing at the time of transfer request remain in effect if not elapsed.

In case of Approve / Auto-Approve if the transfer was requested during the Auto-Renew Grace Period, the extension to the registration period is reversed and the Losing Registrar is refunded the auto-renew. The registration period is extended by the amount specified. This begins the Transfer Grace Period.

5.4 REGISTERED 〉 DELETED

On receipt of a delete command if the domain is in the Add Grace Period, it is purged from the Database and immediately available for registration.

5.5 REGISTERED 〉 REDEMPTION

On receipt of a delete command if the domain is not in the Add Grace Period, it transitions to the Redemption Period state and all grace periods in effect are considered.

5.6 REDEMPTION 〉 PENDING RESTORE

On receipt of a restore command if the Redemption Period has not lapsed, the domain transitions to the Pending Restore state. The Sponsoring Registrar is charged a fee for the restore request.

5.7 PENDING RESTORE 〉 REGISTERED

During the Pending Restore period the Sponsoring Registrar may complete the restore via a restore report containing the Whois information – submitted prior to the deletion, the Whois information at the time of the report, and the reason for the restoration.

5.8 PENDING RESTORE 〉 REDEMPTION

Seven calendar days after the transition to the Pending Restore state, if no restore report is received the domain transitions to the Redemption state, which begins a new redemption period. The restore has no refund.

5.9 Redemption 〉 Pending Delete

Thirty calendar days after the transition to the Redemption state, if no restore request is received the domain transitions to the Pending Delete state.

5.10 PENDING DELETE 〉 DELETED

Five calendar days after the transition to the Pending Delete state, the domain is removed from the Database and is immediately available for registration.

6. LOCKS

Locks may be applied to the domain to prevent specific operations. The Sponsoring Registrar may set the locks prefixed with ‘client’ while locks prefixed with ‘server’ are added and removed by the Registry Operator. Locks are added and removed independently but they can be combined to facilitate the enforcement of higher processes, such as ‘Registrar Lock’, and outcomes required as part of UDRP. All locks are compatible with EPP RFCs. The available locks are:

* clientDeleteProhibited, serverDeleteProhibited - Requests to delete the object are rejected: – clientHold, serverHold - : DNS information is not published
* clientRenewProhibited, serverRenewProhibited - : Requests to renew the object are rejected. Auto-renew is allowed
* clientTransferProhibited, serverTransferProhibited - : Requests to transfer the object are rejected

* clientUpdateProhibited, serverUpdateProhibited - : Requests to update the object are rejected, unless the update removes this status

7. TYPICAL REGISTRATION LIFECYCLE

A typical domain is provisioned immediately on registration. The domain name may be updated over its lifetime to reflect changes in contact or delegation information. The domain name will remain active in the registry by automatic renewals once the registration period has lapsed however Registrars may elect to explicitly renew the domain before the automatic renewal or to extend the registration period by more than one year. The registrar may delete the domain following non-payment or request from the registrant resulting in the immediate removal from the DNS. A time-delayed set of server events will result in the purging of the name from the registry database if the name is not restored during a 30-day redemption period.

8. SPECIAL CONSIDERATIONS

8.1 ICANN-APPROVED BULK TRANSFERS

ICANN-Approved Bulk Transfers performed in accordance with Part B of the Inter-Registrar Transfer Policy do not follow the typical transfer lifecycle. Existing grace periods are invalidated and no refunds are credited to the Losing Registrar. The prohibition of transfer period on domains created or transferred within 60 days does not apply.

8.2 UNIFORM RAPID SUSPENSION

In the Uniform Rapid Suspension (URS) process, as described in the ‘gTLD Applicant Guidebook’ the following modification to the above processes is required.
Remedy allows for the addition of a year to the registration period, limited to the 10 year maximum. During this time no transform operations may be performed other than to restore the domain as allowed by Appeal. At the expiration of the registration period the domain is not automatically renewed, but proceeds to the Redemption state as per the lifecycle described above, and it is not eligible for restoration.

9. UPDATE⁄DNS

The update command does not impact the state of the domain through the Registration Lifecycle, however the command can be used to add and remove delegation information, which changes the DNS state of the domain.

10. RESOURCES

This function will be performed by the following ARI departments:
* Products and Consulting team (7 staff)
* Development Team (11 staff)
the following departments outsourced to the Directi Group:
* Abuse and Compliance Team (20 staff)

ARI’s Registry performs all time-based transitions automatically and enforces all other business rules — without requiring human resources for normal operation. If changes to the automatic behaviours or restrictions enforced by the policy system are required, ARI has a development team for this.

Domain Name Lifecycle aspects requiring human resources to manage are included in the ARI outsourcing include:
* Processing Add Grace Period exemptions as requested by Registrars.
* Processing restore reports provided by Registrars.
* Meeting the Registry Operators obligations under ICANN’s Transfer Dispute Policy.
* Performing exception processing in the case of approved transfers during the 60 day transfer prohibition window.

The Products and Consulting team is responsible for product management of the Registration Lifecycle, including working with clients and the industry to identify new features or changes required to the system.

The automated aspects of the Registration lifecycle are supported by ARI's Domain Name Registry software. ARI has a development team for maintenance and improvement of the software

Most manual tasks fall to the Abuse and Compliance teams of the Directi Group, with staff experienced in development of policy for policy rich TLD environments. They have the required legal and industry background to perform this function.

The Compliance team outsourced to the Directi Group is responsible for any abuse of the registration policies within .Web and supervising the role of any external agency involved in validation

A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q27 – ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within. A detailed list of the Abuse and Compliance desk of Directi is provided in Q28.

ARI provides registry backend services to 5 TLDs and has a vast wealth of experience in estimating the number of resources required to support a Registry System.

Based on past experience ARI estimates that the existing staff is adequate to support a Registry System that is supporting at least 50M domains. Since .Web projects 471,482 domains, 0.94% of these resources are allocated to this TLD. See attachment 'Q27 - Registry Scale Estimates & Resource Allocation.xlsx' for more information.

ARI protects against loss of critical staff by employing multiple people in each role. Staff members have a primary role plus a secondary role for protection against personnel absence. Additionally ARI can scale resources as required. Additional trained resources can be added to any of the above teams with a 2 month lead time.

The Directi Group is protected against loss of staff due to its scale of operations. This is described in further detail in Q39

11. FINANCIAL COSTS

The usage of the ARI's staff and Registry Systems is included in our contract with ARI attached to Q46. This cost is shown in the financial answers.

The usage of Directi Group's staff is included in our contract with Directi attached to Q46. This cost is shown in the financial answers.

This completes our response to Q27.

28. Abuse Prevention and Mitigation

DotWeb Inc. is a wholly owned subsidiary within the Directi Group. The Directi Group runs various businesses including several ICANN Accredited Domain Registrars (including ResellerClub.com and BigRock.com) and Web Hosting companies. The Directi Group manages centralized functions for all its businesses. We have outsourced our Abuse and Compliance functions to the Directi Group and our Abuse and Compliance desk will be staffed as a cost center by them.

This response aims to provide a 360 degree perspective on our policies and processes to prevent abusive activities, and ensure swift mitigation when abuse does occur. We have prepared this plan based on over a decade's experience of fighting abuse as a Registrar, learnings through active industry participation, best-practices from existing registry operators and expert inputs from our back-end technical partner ARI (AusRegistry International).

1. ABUSE MITIGATION EXPERIENCE AND CAPABILITIES

With over four million active domain names registered through its registrars, Directi has significant experience (over 10 years) of managing domain names and is fully cognizant of the threat that stems from their abuse.
As one of the world's top ten registrars, we equally understand our ability to make a sizable contribution towards curbing internet abuse, and believe that mitigating this threat is one of our foremost responsibilities. By instituting policies, processes and services which go significantly above and beyond our obligation as a registrar, Directi has taken various initiatives to make the Internet a safer ground.
To drive this effort, Directi has a committed function working towards identifying abusive domain names and enforcing its policies. Our Abuse Desk functions 24/7 and takes prompt and effective action (both reactively and proactively) against domains reported or co-networked to be involved in any sort of online abuse. Complaints ranging from phishing, spam, malware perpetration, 419 scams, child pornography, copyright infringement and varied forms of abuse are subject to investigation at our Abuse Desk on a daily basis. The nature of abuse and the types of complaints received are varied in nature and intensity, and are documented in more detail further.
On average we already address, 15000 reported or detected abuse cases per year. Abuse cases are addressed within pre-determined SLAs, and our team is committed to ensure that each incident is resolved satisfactorily. The Directi abuse team has been heralded on many occasions by various security groups, law enforcement organizations and the general anti-abuse community for the manner in which abuse mitigation has been handled by us. Additionally, we have always become highly involved, and continue to remain committed to industry-wide efforts to address organized abuse such as botnets (see below) and large scale phishing attacks, and any other malfeasances.

1.1 NOTABLE INSTANCES OF DIRECTI'S SUCCESSFUL ABUSE MITIGATION INITIATIVES

Our abuse mitigation team has developed strong relationships with many security groups and individuals in the abuse mitigation community, with the aim of sharing intelligence and facilitating quick action on abusive domain names. These sources provide us actionable intelligence on domains bought through our registrar. We have also participated in coordinated takedowns with such agencies in the past and are committed to doing so in the future. Please refer to Attachment 'Q28_Recommendations' which showcases letters from several global agencies including the IRS, commending our work and cooperation on several fronts. Following are some examples of cases where our efforts paid great results in abuse mitigation –

1.1.1 MARIPOSA WORKING GROUP

Directi was part of the Mariposa Working Group which was responsible for taking down the largest known botnet network at the time.
(Ref: http://defintel.com/docs/Mariposa_White_Paper.pdf)

"Directi is BY FAR THE BEST registrar we have ever worked with at taking down criminal domains in a timely, efficient and professional manner. Your team was absolutely key to the Mariposa Working Group taking down one of the largest Botnets in the history of the Internet. You and your team should be VERY proud of that :)" -- Christopher Davis, Former CEO of Defence Intelligence

1.1.2 IM WORM BOTNET TAKEDOWN COORDINATED BY IID

Since 1996, IID (Internet Identity) has been providing technology and services that secure the Internet presence for an organization and its extended enterprise. It recently introduced a number of unique approaches to secure organizations' use of Internet infrastructure with ActiveTrust® BGP, ActiveTrust DNS, and ActiveTrust Resolver with TrapTrace. Directi worked with IID, acting against problematic domain names and sharing intelligence to take down a notorious botnet that was plaguing the internet for quite some time.

"Thank you for your exceptional coordination with our team and the other providers … during the simultaneous shutdown. We wanted to follow up with you and let you know that despite the last minute unanticipated scramble, the takedown was a success and the botnet has been shutdown." -- Lauren Lamp, Manager / Service Delivery - internetidentity.com

1.1.3 FAKE PHARMACY TAKEDOWNS COORDINATED BY LEGITSCRIPT

LegitScript is the leading source of information for patients, Internet users, physicians, businesses and other third parties who need to know if an Internet pharmacy is acting in accordance with the law and accepted standards of ethics and safety. LegitScript is identified by the National Association of Boards of Pharmacy as the only Internet pharmacy verification service that adheres to its standards. After affiliating with LegitScript, we have witnessed a steep downfall in fake pharma-related registrations. ResellerClub (referred below) is our wholesale registrar brand.
(Ref:http://legitscriptblog.com/2009/03/directi-no-safe-haven-for-rogue-internet-pharmacies/)

"Some registrars claim that they cannot shut down dangerous 'no-prescription-required' and fake online pharmacies. ResellerClub has proven that this is not true. By refusing to profit from dangerous, criminal activity at the expense of Internet users, ResellerClub has established itself as a responsible example for the rest of the Internet community." John Horton, President, LegitScript.com

We have enclosed a commendation letter from LegitScript in Attachment 'Q28_Recommendations', which speaks of our leadership in fighting fake and rouge pharmacies.

1.1.4 419 FEEDBACK LOOP WITH ARTISTS AGAINST 419 (AA419.ORG)

An honorary member of the APWG (Anti-Phishing Working Group), Artists Against 419 is a premier organization with expertise in identifying, cataloging, and terminating fraud sites. Our tie-up with them has been greatly successful in eliminating fraudulent registrations within our portfolio. (Ref: http://blog.aa419.org/?p=134)

"Many registrars do respond to abuse reports and take action against them. However none do it as quickly and efficiently as Directi. If all registrars and hosters take this approach, it might then be possible to reduce internet fraud." -- aa419.org

We have enclosed a letter from Artists Against 419 in Attachment 'Q28_Recommendations' commending the speed and impact of our proactive abuse mitigation activities.

2. PROPOSED ABUSE POLICY FOR .WEB

We have fully adopted the definition of abuse developed by the Registration Abuse Policies Working Group (Registration Abuse Policies Working Group Final Report 2010).

Our abuse policies described in this section apply to initial and ongoing domain registrations, ie any domain name must comply with these policies during registration and throughout its tenure.

Abusive behaviour in a TLD may relate can be categorized into:

2.1 REGISTRATION POLICY VIOLATIONS

.Web adopts certain Registration policies and any violations of these policies would be treated as an Abuse.

2.1.1 SUNRISE POLICY VIOLATION

.Web will have a sunrise period as described in the response to Question 29. Our sunrise policy will have an overarching goal to protect interests of IP holders globally, and be based on best practices seen in previous TLD launches. We will implement the Trademark Claim Service and partner with experienced service providers to run the TM verification, Sunrise Challenge and Auction processes. All Sunrise domain names will be validated before they are activated. Hence the possibility of a Sunrise policy violation is low. However the Sunrise process provides for a Sunrise Dispute Resolution Policy, and any disputes that fall within its scope will be referred to the Sunrise Dispute Resolution provider. If the abuse desk receives any

complaints concerning a sunrise domain which violates the Sunrise eligibility policy the abuse desk will direct the complainant to the Sunrise Dispute Resolution provider

2.1.2 WHOIS INACCURACY

.Web requires Whois accuracy as per its contracts. Any domain name with inaccurate whois information will be deemed to be in violation of its contract and hence will be deemed as an abuse and handled in the manner described ahead.

2.1.3 TRADEMARK INFRINGEMENT VIOLATION AND UDRP

.Web requires registrants to abide by UDRP. If the abuse desk receives any complaints concerning a domain name which infringes upon the trademark right of a 3rd party, the abuse desk will direct the complainant to the Uniform Dispute Resolution provider.

All names registered under .Web will be subject to the UDRP and URS processes. We believe that URS will deter cybersquatting, and some malicious activities that illegitimately use brand names. We will seek to expeditiously process all URS cases, and are already equipped with mature processes and tracking systems to manage and keep track of all cases.

The URS process will be run by our compliance team, who has significant experience in processing UDRP complaints for our Registrar businesses.

While Registrars will be responsible for processing all UDRP cases related to the .Web, we will reserve the right to act on their behalf when necessary, and process all court orders that are directed to us.

2.2 ACCEPTABLE USAGE RELATED VIOLATIONS

.Web adopts certain Content and Acceptable usage policies and any violations of these would be treated as an Abuse. The following are deemed as violations of our content and acceptable usage policy

2.2.1 INTELLECTUAL PROPERTY, TRADEMARK, COPYRIGHT, AND PATENT VIOLATIONS, INCLUDING PIRACY

Intellectual property (IP) is a term referring to a number of distinct types of creations of the mind for which a set of exclusive rights are recognized—and the corresponding fields of law. Under intellectual property law, owners are granted certain exclusive rights to a variety of intangible assets, such as musical, literary, and artistic works; discoveries and inventions; and words, phrases, symbols, and designs. Common types of intellectual property rights include copyrights, trademarks, patents, industrial design rights and trade secrets in recognized jurisdictions. Any act resulting in theft, misuse, misrepresentation or any other harmful act by any individual or a company is categorized as Intellectual Property violation.

2.2.2 SPAMMING

The use of electronic messaging systems to send unsolicited bulk messages. The term applies to e-mail spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of Web sites and Internet forums. Unsolicited emails advertising legitimate and illegitimate products, services, and/or charitable requests and requests for assistance are also considered as spam.

2.2.3 PHISHING (and various forms of identity theft)

Fraudulent web services and applications meant to represent/confuse or mislead internet users into believing they represent services or products for nefarious purposes, such as illegally gaining login credentials to actual legitimate services.

2.2.4 PHARMING AND DNS HIJACKING

Redirection of DNS traffic from legitimate and intended destinations, by compromising the integrity of the relevant DNS systems. This leads unsuspecting Internet users to fraudulent web services and applications for nefarious purposes, such as illegally gaining login

credentials to actual legitimate services.

2.2.5 DISTRIBUTION OF VIRUSES OR MALWARE

Most typically the result of a security compromised web service where the perpetrator has installed a virus or “malevolent” piece of software meant to infect computers attempting to use the web service in turn. Infected computers are then security compromised for various nefarious purposes such as gaining stored security credentials or personal identity information such as credit card data. Additionally compromised computers can sometimes be remotely controlled to inflict harm on other internet services (see botnet below).

2.2.6 CHILD PORNOGRAPHY

Child pornography refers to images or films (also known as child abuse images) and, in some cases, writings depicting sexually explicit activities involving a minor.

2.2.7 USING FAST FLUX TECHNIQUES

A methodology for hiding multiple source computers delivering malware, phishing or other harmful services behind a single domain hostname, by rapidly rotating associated IP addresses of the sources computers through related rapid DNS changes. This is typically done at DNS zones delegated below the level of a TLD DNS zone.

2.2.8 RUNNING BOTNET COMMAND AND CONTROL OPERATIONS

A Botnet is a significant coordinated net of compromised (sometimes tens of thousands) computers running software services to enact various forms of harm - ranging from unsanctioned spam to placing undue transaction traffic on valid computer services such as DNS or web services. Command and control refers to a smaller number of computers that issue/distribute subsequent commands to the Botnet. Compromised botnet computers will periodically check in with a command and control computer that hides behind a list of date triggered, rotating domain registrations, which are pre-loaded in the compromised computer during its last check-in.
Registries play a key role in breaking this cycle of pre-determined domain registrations by deactivating said registrations prior to the compromised computers being able to use them to contact the command and control computer. Successful intervention results in the botnet losing contact with their command and control computers, leaving them inactive and reducing potential harms.

2.2.9 HACKING

Hacking constitutes illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of other individuals. Also includes any activity that might be used as a precursor to an attempted system penetration.

2.2.10 FINANCIAL AND OTHER CONFIDENCE SCAMS

Financial scams, including but not limited to the cases defined below, are operated by fraudsters to lure investors into fraudulent money making schemes. Prominent examples that will be treated as abusive are –
1. Ponzi Schemes. A Ponzi scheme is essentially an investment fraud wherein the operator promises high financial returns or dividends that are not available through traditional investments. Instead of investing victims' funds, the operator pays "dividends" to initial investors using the principle amounts "invested" by subsequent investors. The scheme generally falls apart when the operator flees with all of the proceeds, or when a sufficient number of new investors cannot be found to allow the continued payment of "dividends."
2. Money Laundering. Money laundering, the metaphorical "cleaning of money" with regard to appearances in law, is the practice of engaging in specific financial transactions in order to conceal the identity, source, and/or destination of money, and is a main operation of the underground economy.
3. 419 Scams. "419" scam (aka "Nigeria scam" or "West African" scam) is a type of fraud named after an article of the Nigerian penal code under which it is prosecuted. It is also known as

"Advance Fee Fraud". The scam format is to get the victim to send cash (or other items of value) upfront by promising them a large amount of money that they would receive later if they cooperate.

2.2.11 ILLEGAL PHARMACEUTICAL DISTRIBUTION

Distribution and promotion of drugs, locally within a nation or overseas, without prescription and appropriate licenses as required in the country of distribution are termed illegal.

2.2.12 OTHER VIOLATIONS

Other violations that will be expressly prohibited under the .Web include
* Network attacks
* Violation of applicable laws, government rules and other usage policies

3. PROCEDURES TO MINIMIZE ABUSIVE REGISTRATIONS

3.1 BUILDING A ZERO-TOLERANCE REPUTATION

Our Anti-Abuse Policy will put Registrants on notice of the ways in which we will identify and respond to abuse and serve as a deterrent to those seeking to register and use domain names for abusive purposes. The policy will be made easily accessible on the Abuse page of our Registry website which will be accessible and have clear links from the home page along with FAQs and contact information for reporting abuse.

Directi has vast experience in minimizing abusive registrations. Our zero tolerance procedures and aggressive proactive takedown measures as a Domain Registrar have resulted in a white-hat reputation discouraging abusive registrations to begin with. We intend on following the same approach with respect to Registry operations for .Web. Our proactive abuse procedures are geared towards building a reputation that discourages miscreants and malicious intent. Once it is known that abusive registrations and registrations in violation of our policies are suspended rapidly, both abusive registrations and abusive behavior will be discouraged.

Our Abuse policies described in section 2 above apply to new and ongoing registrations.

3.2 BUILDING AWARENESS OF OUR ANTI-ABUSE POLICY

The Abuse Policy will be published on the abuse page of our Registry website which will be accessible and have clear links from the home page. The abuse page of our Registry website will emphasise and evidence our commitment to combating abusive registrations by clearly identifying what our policy on abuse is and what effect our implementation of the policy may have on registrants. We anticipate that the clear message, which communicates our commitment to combating abusive registrations, will further serve to minimise abusive registrations in our TLD.

3.3 ICANN PRESCRIBED MEASURES

In accordance with our obligations as a Registry Operator we will comply with all requirements in the ‘gTLD Applicant Guidebook’. In particular, we will comply with the following measures prescribed by ICANN which serve to mitigate the potential for abuse in the TLD:

* DNSSEC deployment, which reduces the opportunity for pharming and other man-in-the-middle attacks. We will encourage registrars and Internet Service Providers to deploy DNSSEC capable resolvers in addition to encouraging DNS hosting providers to deploy DNSSEC in an easy to use manner in order to facilitate deployment by registrants. DNSSEC deployment is further discussed in the context of our response to Question 43;
* Prohibition on Wild Carding as required by section 2.2 of specification 6 of the Registry Agreement

* Removal of Orphan Glue records: ICANN requires a policy and procedure to take action to remove orphan glue records from the zone when provided with evidence that the glue is indeed present and aiding malicious conduct. The ARI Managed TLD Registry SRS database does not allow

orphan records. Glue records are removed when the delegation point NS record is removed. Other domains that need the glue record for correct DNS operation may become unreachable or less reachable depending on their overall DNS service architecture. It is the Registrant's responsibility to ensure that their domain name does not rely on a glue record that has been removed and that it is delegated to a valid name server. The removal of glue records upon removal of the delegation point NS record mitigates the potential for use of orphan glue records in an abusive manner

3.4 REGISTRANT DISQUALIFICATION

Abusive domain registration has historically attracted a small number of individuals and organisations that engage in high volume registrations, driven by the marginal profitability of individual abusive registrations. As specified in our Anti-Abuse Policy, we reserve the right to deny registration of a domain name to a Registrant who has repeatedly engaged in abusive behaviour in our TLD or any other TLD.

Registrants, their agents or affiliates found through the application of our Anti-Abuse Policy to have repeatedly engaged in abusive registration will be disqualified from maintaining any registrations or making future registrations. This will be triggered when our records indicate that a Registrant has had action taken against it an unusual number of times through the application of our Anti-Abuse Policy.

Registrant disqualification provides an additional disincentive for qualified registrants to maintain abusive registrations in that it puts at risk even otherwise non-abusive registrations through the possible loss of all registrations.

In addition, name servers that are found to be associated only with fraudulent registrations will be added to a local blacklist and any existing or new registration that uses such fraudulent NS record will be investigated.

The disqualification of 'bad actors' and the creation of blacklists mitigates the potential for abuse by preventing individuals known to partake in such behaviour from registering domain names.

3.5 PROACTIVE DETERMINATION OF POTENTIAL ABUSE

There are several tell-tale signs which are indicative of abusive intent. The following are examples of the data variables will serve as indicators that we will monitor with the help of our registry technical partner.

* Unusual Domain Name Registration Practices: practices such as registering hundreds of domains at a time, registering domains which are unusually long or complex or include an obvious series of numbers tied to a random word (abuse40, abuse50, abuse60) may when considered as a whole be indicative of abuse

* Domains or IP addresses identified as members of a Fast Flux Service Network (FFSN): Our service provider ARI uses the formula developed by the University of Mannheim and tested by participants of the Fast Flux PDP WG to determine members of this list. IP addresses appearing within identified FFSN domains, as either NS or A records shall be added to this list.

* An Unusual Number of Changes to the NS record: the use of fast-flux techniques to disguise the location of web sites or other Internet services, to avoid detection and mitigation efforts, or to host illegal activities is considered abusive in the TLD. Fast flux techniques use DNS to frequently change the location on the Internet to which the domain name of an Internet host or name server resolves. As such an unusual number of changes to the NS record may be indicative of the use of fast-flux techniques given that there is little, if any, legitimate need to change the NS record for a domain name more than a few times a month.

* Results of Monthly Checks: The random monthly checks to promote Whois accuracy (described ahead) are not limited to serving that purpose but may also be used to identify abusive behaviour given the strong correlation between inaccurate Whois data and abuse.

* Analysis of Cross Validation of Registrant Whois data against Whois Data Known to be

Fraudulent.

* Analysis of Domain Names belonging to Registrant subject to action under the Anti-Abuse policy: in cases where action is taken against a registrant through the application of our Anti-Abuse policy, we will also investigate other domain names by the same registrant (same name, nameserver IP address, email address, postal address etc).

4. PROCEDURES FOR HANDLING COMPLAINTS

4.1 MECHANISMS FOR REPORTING COMPLAINTS

In order to make it easy for security agencies, law enforcement bodies and vigilant users to report incidents of abusive behavior within .Web, we shall enable several channels of communication.

4.1.1 SINGLE POINT OF CONTACT

In accordance with section 4.1 of specification 6 of the Registry Agreement we will establish a single abuse point of contact (SAPOC) responsible for addressing and providing a timely response to abuse complaints concerning all names registered in the TLD through all registrars of record, including those involving a reseller. Complaints may be received from members of the general public, other registries, registrars, LEA (Law Enforcement Agencies), government and quasi governmental agencies and recognised members of the anti-abuse community.

The SAPOC’s accurate contact details (email, fax and mailing address) will be provided to ICANN and published on the abuse page of our Registry website. The SAPOC will in turn represent the entire compliance desk operated by the Directi group on behalf of .Web as an outsourced function.

The Registry website will additionally also include:

* All public facing policies in relation to the TLD including the Anti-Abuse Policy described in section 2
* A web based submission service for reporting inaccuracies in Whois information
* Registrant Best Practices
* Conditions that apply to proxy registration services and direction to the SAPOC to report domain names that violate the conditions

As such, the SAPOC may receive complaints regarding a range of matters concerning the abuse policy defined in section 2

The SAPOC will be the primary method by which we will receive notification of abusive behaviour from third parties. It must be emphasised that the SAPOC will be the initial point of contact following which other processes will be triggered depending on the identity of the reporting organization and the type of abuse. Accordingly, separate processes for identifying abuse will exist for reports by LEA/government and quasi governmental agencies and members of the general public.

When any party makes a report via the Abuse POC e-mail address or the abuse web form, he or she will receive back a ticket number from a ticketing system. Our abuse team will then examine these reports, and use a ticketing system to track each issue. This process will leverage a dedicated software that we have used for handling abuse reports to our registrar businesses. It is our goal to provide a timely response to all abuse complaints concerning domains registered in the TLD, as per the SLAs defined by us.

4.1.2 LAW ENFORCEMENT AGENCIES

We recognise that LEA, governmental and quasi governmental agencies may be privy to information beyond the reach of others which may prove critical in the identification of abusive behaviour in our TLD. As such, we will provide an expedited process which serves as a channel of communication for law enforcement, government and quasi-governmental agencies to, amongst other things, report illegal conduct in connection with the use of the TLD.

The process will involve prioritization and prompt investigation of reports identifying abuse from those organizations. The steps in the expedited process are summarised as follows:

1. We will identify relevant LEA, government and quasi governmental agencies who may take part in the expedited process
2. We will establish back channel communication with each of the identified agencies in order to obtain information that may be used to verify the identity of the agency upon receipt of a report utilising the expedited process;
3. We will publish contact details on the abuse page of the Registry website for the SAPOC to be utilised by only those taking part in the expedited process;
4. All calls to this number will be responded to by a member of our 24⁄7 Compliance Team
5. We will verify the identity of the reporting agency employing methods specific to that agency established during back channel communication;
6. Upon verification of the reporting agency, we will obtain the details necessary to adequately investigate the report of abusive behaviour in the TLD;
7. Reports from verified agencies may be provided in the Incident Object Description Exchange Format (IODEF) as defined in RFC 5070. Provision of information in the IODEF will improve our ability to resolve complaints by simplifying collaboration and data sharing
8. The report identifying abuse will then be dealt with in accordance to our process defined in subsequent sections of this answer

4.2 EVALUATION OF COMPLAINTS

The next step is for our abuse desk staff to review each complaint. The abuse team looks at the facts of each complaint in order to verify the complaint. The goals are accuracy, good record-keeping, and a zero false-positive rate so as not to harm innocent registrants while at the same time, taking timely action to mitigate abusive behaviour and to minimize impact.

Evaluation of complaints thus forms a very important part of the process. The following factors are considered for each case:

* Type, Severity and immediacy of the abuse: Upon initial review, all incoming complaints will face an initial evaluation on the basis of severity and harm cased due to the abuse. While we will adhere to the SLAs laid down for our abuse mitigation processes, regardless of the type of complaint, there will be some complaints that will be considered relatively more severe and of greater malicious impact than others. Complaints with a higher severity⁄malicious impact and immediacy will be processed with greater urgency than others.

* Determining the origin of the complaint: a credible complainant e.g. a law enforcement agency, a security group etc. automatically lends genuineness to a complaint while a complaint from a previously unknown source will require a background check to ensure that the complaint is not from a miscreant looking to create unnecessary trouble for a domain owner. Thus while we may take immediate action complaints from reliable sources, those from other sources, not backed by enough evidence, may require further due-diligence before action is taken.

* Evaluating proof submitted along with a complaint: A complaint is also evaluated based on the supporting evidence provided which further determines the validity of a complaint. At this stage we will also attempt to establish a clear link between the activity reported and the alleged type of abusive behaviour. This is done to ensure that addressing the reported activity will address the abusive behaviour. In some cases the abuse is evident, which will result in immediate processing of the complaint from our side without much further due-diligence. In some cases, where the abuse may not be evident upfront, our desk will rely on supplementary evidence provided by the complainant which may be further ratified. While not limited to this list, supporting evidence could range from links, screen-shots of websites, copy right ⁄ trademark details, emails, email headers, whois information, ID proof etc.

* Evaluating historical data: As mentioned before, we will maintain a log of all complaints received, including the contact details of complainants, the whois details of the abusers, the nameservers of abusive domain registrations, the type of domain names, the IPs of spamming domains etc. This will further help us in establishing trends for further action as required. A registration that re-sounds alarms from previously seen abusive trends will ascertain the necessary pre-emptive mitigation processes.

Assessing abuse reports requires good judgment, and we will rely upon our, specially trained abuse desk staff.

While we recognise that each incident of abuse represents a unique security threat and should be mitigated accordingly, we also recognise that prompt action justified by objective criteria are key to ensuring that mitigation efforts are effective. With this in mind, we have categorised the actions that we may take in response to various types of abuse by reference to the severity and immediacy of harm. This categorisation will be applied to each validated report of abuse and actions will be taken accordingly. It must be emphasised that the actions to mitigate the identified type of abuse in the section/s below are merely intended to provide a rough guideline and may vary upon further investigation.

4.3 CATEGORIZATION OF COMPLAINTS

Each confirmed case of abuse is bucketed into one of the following categories

4.3.1 CATEGORY 1

Probable Severity or Immediacy of Harm - Low
Examples of types of abusive behaviour – Small Scale Spam, Whois Inaccuracy

Mitigation steps:

1. Preliminary Investigation
2. Delegate to Registrar
3. Monitor response time-frame vis-à-vis SLA
4. Take direct action in case of Registrar non-conformance.

4.3.2 CATEGORY 2

Probable Severity or Immediacy of Harm - Medium
Examples of types of abusive behaviour – Medium scale spam, inactive botnets and other forms of abuse which have a higher degree of impact than the ones bucketed as category 1, but still relatively limited in terms of potential damage.

Mitigation steps:

1. Preliminary Investigation
2. Delegate to Registrar
3. Monitor response time-frame vis-à-vis SLA
4. Take direct action in case of Registrar non-conformance.

4.3.3 CATEGORY 3

Probable Severity or Immediacy of Harm - High
Examples of types of abusive behaviour – Fast Flux Hosting, Phishing, Large scale hacking, Pharming, Botnet command and control, Child Pornography and all other cases deemed to carry a very high risk of large scale impact

Mitigation steps for Abuse policy violation:

1. Suspend domain name
2. Investigate
3. Restore or terminate domain name

4.4 MITIGATION OF COMPLAINTS

The mitigation steps for each category will now be described:

4.4.1 CATEGORY 1

Types of abusive behaviour that fall into this category include those that represent a low

severity or immediacy of harm to registrants and internet users. These generally include behaviours that result in the dissemination of unsolicited information or the publication of illegitimate information. While undesirable, these activities do not generally present such an immediate threat as to justify suspension of the domain name in question. Each of these cases will be delegated down to the Registrar and the registrar's performance, in terms of response and resolution rate, will be monitored and recorded by us. In case of non-conformance by the Registrar, we will take-over the issue.

We will also continually monitor the issue to track possible increases in the severity of harm. In case the threat level is above what was originally anticipated, we will escalate the issue to category two or three and act in accordance.

4.4.2 CATEGORY 2

Types of abusive behaviour that fall into this category include those that represent a medium severity or immediacy of harm to registrants and internet users. These generally include medium scale spam, network intrusion, inactive botnets etc. Following the notification of the existence of such behaviours, our compliance team will delegate the issue to registrars and envoke the more aggressive SLAs that apply to this category of risk.

As was the case with category 1, we will continue to monitor the registrar's conformance with the SLAs and take direct action when necessary. We will also check for possible increases in risk levels and escalate the abuse category if required.

4.4.3 CATEGORY 3

Highly serious, sensitive and large scale issues like phishing, child pornography and large-scale botnet are considered to be a serious violation of the Anti-Abuse Policy owing to its fraudulent exploitation of consumer vulnerabilities, high level of risk and far-reaching consequences. Given the direct relationship between the uptime of these activities, and extent of harm caused, we recognise the urgency required to execute processes that handle these cases directly, without any delegation.
As soon as the abuse is substantiated, we will proceed to suspend the domain name pending further investigation to determine whether the domain name should be unsuspended or cancelled. Cancellation will result if upon further investigation, the behaviour is determined to be one of the types of abuse defined in the Anti Abuse Policy.

In some cases we may change the nameservers associated with the domain and/or use EPP prohibited statuses in appropriate combinations to restrict activity against the domain such as contact updates, deletes or transfers.

In the past we have modified Nameservers to sinkhole malicious domains, so research partners can measure botnets and monitor malware activity. We believe this to be an extremely effective mechanism which takes down large scale attacks from the source, and assists researchers to build processes and tools which prevent future attacks from the same source. Our team will follow the same process for domains belonging to our registry.

We have built special systems to suspend individual and bulk batches of domains. This will allow us to quickly take care of cases where criminals have obtained bulk batches of domain names. This will be of use if malware designers use generation algorithms to register domains.

Reactivation of the domain name will result where further investigation determines that abusive behaviour, as defined by the Anti Abuse Policy, does not exist and that the domain name is not causing any harm.

4.5 PROPOSED RESOLUTION METRICS AND SERVICE LEVEL AGREEMENTS

SLA RESPONSE CONSIDERATIONS FOR REPORTED ABUSE CASES

As described earlier, each abuse case and goes into one of three response categories depending on the severity and immediacy of the harm caused by the abuse. In the case of any failed SLA

responses, the Registry reserves the right to act directly to suspend and/or lock the domains associated with a given abuse case. Additionally, highly serious, sensitive and large scale issues are ranked as category 3 and prioritized above all other cases.

Attachment 'Q28_Abuse Mitigation SLA', shows the flowchart and SLA response for each category of abuse complaint

4.5.1 CATEGORY 1

Some examples of abuses cases that will be categorized as 1 include:

* Low scale Spam
* Whois Inaccuracy
* Low scale Malware
* Any other abuse case deemed as low risk

RESPONSE SLA COMMITMENTS:

* Initial Registry Response to Complainant: 2 business days from the time of receipt of the complaint
* Registry Notification to Registrar: 2 business days from the time of receipt of the complaint
* Initial Response from Registrar: 3 business days from the time that the complaint notification is sent to the Registrar
* Update from Registrar as action taken or intended: 7 business days from the time that the complaint notification is sent to the Registrar
* Final Resolution: 15 business days from the time the issue was reported to us

4.5.2 CATEGORY 2

Some examples of abuses cases that will be categorized as 2 include:

* Medium scale Spam
* Confirmed but inactive botnet domains
* All other abuse cases deemed as medium scale

RESPONSE SLA COMMITMENTS:

* Initial Registry Response to Complainant: 2 business days from the time of receipt of the complaint
* Registry Notification to Registrar: 2 business days from the time of receipt of the complaint
* Initial Response from Registrar: 2 business days from the time that the complaint notification is sent to the Registrar by the Registry
* Update from Registrar as action taken or intended: 3 business days from the time that the complaint notification is sent to the Registrar by the Registry
* Final Resolution: 8 business days from the time of receipt of the complaint

4.5.3 CATEGORY 3

Some examples of abuses cases that will be categorized as 3 include:

* Confirmed Cases of child pornography
* Confirmed cases of Phishing
* Confirmed and active botnets domains
* Any other case deemed as large scale

RESPONSE SLA COMMITMENTS:

* Initial Registry Response to Complainant: 1 business day from the time of receipt of the complaint
* Registry time to direct takedown: 3 business days from the time of receipt of the complaint

4.6 FOLLOW-UP AND CAPTURE OF METRICS

The abuse staff will track each abuse complaint ticket to resolution. Our ticketing system allows us to capture many metrics. We will measure resolution times, and we can see what percentage of abuse reports could be confirmed. We will also capture how many domains were suspended, and we will break down statistics by registrar in the TLD. This will help us identify registrars that have regular problems, and we can work with them to systematically identify and act against bad actors.

4.7 CONTRACTUAL PROVISIONS

As the registry operator, we will use the Registry-Registrar Agreement (RRA) to establish the registry's right to act against abusive registrations as described in the preceding sections. We will also use the contract to impose certain obligations on the registrars, and make some obligations binding on the registrants by obligating specific terms in the registrar-registrant contract. The contract will be a mandatory part of the Registrar accreditation process with the Registry. Production access to the Registry will not be granted until the contract is duly signed AND the registrar has provided copy of their Registry Registrant Agreement to demonstrate the inclusion of any required pass-through provisions. The registrar is also fully obligated to their accreditation contracts with ICANN (via the RAA) which includes elements such as the UDRP.

In general, the contracts will establish that the registry operator may reject a registration request, or can delete, revoke, update, suspend, cancel, or transfer a registration for violations of our anti-abuse policies. The terms in our proposed agreement will empower us to take necessary action including, but not limited to:

* Discretionary action against domain names that are not accompanied by complete and accurate information as required by ICANN Requirements and/or Registry Policies or where required information is not updated and/or corrected as required by ICANN Requirements and/or Registry Policies;

* Action as may be required to protect the integrity and stability of the Registry, its operations, and the TLD system;

* Action as may be required to comply with any applicable law, regulation, holding, order, or decision issued by a court, administrative authority, or dispute resolution service provider with jurisdiction over the Registry;

* Action as may be required to establish, assert, or defend the legal rights of the Registry or a third party or to avoid any civil or criminal liability on the part of the Registry and/or its affiliates, subsidiaries, officers, directors, representatives, employees, contractors, and stockholders;

* Action as may be required to correct mistakes made by the Registry or any Accredited Registrar in connection with a registration; or

* Enforcement of Registry policies and ICANN requirements; each as amended from time to time;

* Actions as otherwise provided in the Registry-Registrar Agreement and/or the Registry-Registrant Agreement.

Below are some additional points that we will look to cover in the RRA. These clauses will enable us to enforce some additional, proactive measures to curb and deter abuse:

* We will reserve the right to deny registration of a domain name to a registrant who has repeatedly engaged in abusive behaviour in our TLD or any other TLD.

* We will reserve the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute.

* We may amend or otherwise modify this policy to keep abreast of changes in consensus policy

or new and emerging types of abusive behaviour in the Internet.

* Relevant language that enforces Registrars to conform with the SLAs provided for abuse cases delegated to them and provides the Registry with rights to take relevant actions in those cases.

* Relevant language for sanctions against a Registrar leading to termination with respect to repeated offences and violations of their obligations with respect to abuse mitigation.

* Relevant language that requires Registrars to provide for the following in their agreement with the Registrants
** Whois accuracy provisions
** Acceptable content and usage policy
** Sunrise policy and submission to SDRP
** UDRP
** Rights granted to the Registrar and Registry to take necessary action wrt abuse prevention including sharing information with regulatory bodies and LEA and domain takedowns where appropriate
** Indemnification

All of the contracts above will be regularly reviewed (atleast once a year) based on the experience gained by the Registry during actual operation and any relevant changes required to mitigate abuse will be appropriately introduced in consultation with ICANN and the Registrars

4.8 ADDITIONAL MITIGATION MEASURES

Based on our experience of running a leading Registrar, we have also devised some powerful mechanisms which will prevent possible abuse, and quickly diffuse abusive domains. These mechanisms include:

4.8.1 PROFILING & BLACKLISTING

This process, currently in practice for our registrar businesses within the Directi Group, is used for gathering intelligence on known offenders. We maintain abuse ratios for each of the 1,000,000 plus registrants and 65,000 plus resellers who use Directi.

Experience has enabled us to use these ratios accurately to uncover registrants who are known and repeated offenders. Expert offenders rarely reuse the same registrant profile and often maintain a myriad number of profiles to mask their true identity. Through pattern mapping we try and group registrant profiles that we believe belong to the same operator.

The same process is followed at the reseller level too, to identify those resellers who are knowingly harboring offenders, or are themselves involved in abuse.
When a registrant profile is confirmed to be involved in organized abuse, including but not limited to cybersquatting, phishing, pharming etc., our immediate step is to suspend that customer’s control over his abusive domain portfolio. Our compliance team then carefully analyzes each domain name to identify those which are abusive and not already taken-down. The necessary action is undertaken to diffuse any ongoing abuse.

We plan to adopt the ‘Profiling and Blacklisting’ process within our registry operations. Since all of our compliance resources will be trained and experienced in running this process, its implementation into .Web will be simple. Specifics of this policy and process, as it applies to our registry business, will be drawn out.

4.8.2 PROACTIVE QUALITY REVIEW

As a preventive safeguard against abusive domain registration, we follow a consistent review process for domain registrations on our registrar, where a sample of newly registered domain names are analyzed for potential abusive activity. Coupled with our profiling process (described above), it enables us to take proactive measures against domain names that are registered solely to perpetrate malicious activities such as phishing, or otherwise infringe on the rights of others. This helps us curb abusive activity before it can affect too many Internet users. We shall seek to implement similar safeguards for .Web, and encourage

registrars to incorporate this practice as part of their abuse mitigation processes.

4.9 INDUSTRY COLLABORATION AND INFORMATION SHARING

Upon obtaining Registry Accreditation, we will join the Registry Internet Safety Group (RISG), whose mission is to facilitate data exchange and promulgate best practices to address internet identity theft, especially phishing and malware distribution. In addition, Directi coordinates with the Anti-Phishing Working Group (APWG), other DNS abuse prevention organizations and is subscribed to the NXdomain mailing list.
Directi's strong participation in the industry facilitates collaboration with relevant organizations on abuse related issues and ensures that Directi is responsive to new and emerging domain name abuses.

The information shared as a result of this industry participation will be used to identify domain names registered or used for abusive purposes. Information shared may include a list of registrants known to partake in abusive behavior in other TLDs. While presence on such lists will not directly constitute grounds for registrant disqualification, we will investigate domain names registered to those listed registrants and take appropriate action. In addition, information shared regarding practices indicative of abuse will facilitate detection of abuse by our own monitoring activities.

5. PROMOTING AND ENSURING WHOIS ACCURACY

All registrants shall be required, via required language in every Registrar – Registrant Agreement, to provide accurate Registrar Data Directory Services, RDDS (WHOIS) contact details, and to keep those details current. Additionally, Registrars shall have direct responsibility to ensure Whois accuracy through their accreditation contracts with ICANN. Whois Data Reminder Policy or WDRP is an example of a direct Registrar⁄ICANN contractual obligation to monitor that RDDS (WHOIS) information is accurate and up to date – it includes requiring Registrars to notify their registrants at least once a year to ensure their RDDS (WHOIS) data is correct and up to date.

The threat of inaccurate Whois information significantly hampers the ability to enforce policies in relation to abuse in the TLD by allowing the registrant to remain anonymous. In addition, LEA's rely on the integrity and accuracy of Whois information in their investigative processes to identify and locate wrongdoers.

In recognition of this, we propose that .Web have the following measures to promote RDDS (WHOIS) accuracy.

5.1 WHOIS INACCURACY REPORTING SYSTEM

On the abuse page of our Registry website, we will provide a web based submission service for reporting Whois accuracy issues. Each of these issues will then be resolved as per the process detailed in the previous sections.

5.2 REGULAR MONITORING & SAMPLING

Registrants of randomly selected domain names will be contacted by telephone using the provided Whois information by a member of our team in order to verify the phone number and confirm other Whois information. Where the registrant is not contactable by telephone, alternative contact details (email, postal address) will be used to contact the registrant who must then provide a contact number that is verified by our team. In the event that the registrant is not able to be contacted by any of the methods provided in Whois, the domain name will be cancelled following five contact attempts or one month after the initial contact attempt (based on the premise that a failure to respond is indicative of inaccurate Whois information and is grounds for terminating the registration agreement)

5.3 ANALYSIS OF REGISTRY DATA

We will adopt some processes to identify patterns and correlations indicative of inaccurate Whois (e.g. repetitive use of fraudulent details).

5.4 PROMOTING ACCURATE WHOIS DATA

WDRP (Whois Data Reminder Policy) implemented by ICANN at the Registrar level, mandates regular e-mail communication to registrants reminding them to keep their whois data accurate and updated. In addition, we will also identify effective mediums to remind registrants to update Whois information and inform them of the ramifications of a failure to respond to our random monthly checks. Ramifications include but are not limited to termination of the registration agreement.

5.5 ENFORCEMENT AT REGISTRAR LEVEL

Registrars will also be contractually required to promptly investigate reports of RDDS (WHOIS) accuracy submitted to them, and resolve each case within a predefined time-frame stipulated through our SLA.

For all cases where inaccuracy is confirmed, we will record the registrar from whom the domain was sourced. We will use this data to capture the ratio of inaccuracies as a percentage of total domains managed, and identify the registrars that seem to attract an abnormally high number of inaccuracy issues. We will then work with those registrars to find potential ways in which they can progressively reduce the number of whois inaccuracy incidents.

The measures to promote Whois accuracy described above strike a balance between the need to maintain the integrity of the Whois service, which facilitates the identification of those taking part in illegal or fraudulent behaviour, and the operating practices of the Registry Operator and Registrars which aim to offer domain names to registrants in an efficient and timely manner.

Awareness among registrants that we will actively take steps to maintain the accuracy of Whois information mitigates the potential for abuse in the TLD. It deters abusive behaviour given that registrants may be identified, located and held liable for all actions in relation to their domain name.

5.6 PROXY ⁄ PRIVACY PROTECTION

We have designed a policy that will maximize the legitimate use of proxy and privacy services, and will minimize use by criminals and abusers.

.Web will allow the use of proxy and privacy services, where permitted by ICANN policies and requirements. These services have legitimate uses. Millions of registrants use them to protect their privacy and personal data from spammers and other parties that mine zone files and RDDS (WHOIS) data.

It is undeniable that criminals also use whois proxy services, to hide their true identities. To deter that practice, our policy will require that:

* Registrants must use only a privacy⁄proxy service operated, contracted or owned by the domain’s sponsoring registrar, and cannot use third-party proxy services unaffiliated with the domain’s sponsoring registrar. This means that a domain’s sponsoring registrar will always be in possession of the underlying contact data.

*. Registrars and resellers must provide the underlying registrant information to the registry operator upon request, and⁄or upon a legitimate law-enforcement request, within 24 hours. The registry operator will keep this data confidential, unless #3 below applies.

* Registrars and resellers must remove the proxy protection and publish the underlying registrant information in the RDDS (WHOIS) if it is determined by the registry operator and⁄or the registrar that the registrant has breached any terms of service, such as anti-abuse policies.

The registrar obligations outlined above shall apply with equal force to all registrations sponsored by a registrar, whether those registrations were placed directly with the registrar or through a reseller.

These conditions will be implemented contractually by inclusion of corresponding clauses in the RRA as well as being published on the abuse page of our Registry website. Individuals and organisations will be encouraged through our abuse page to report any domain names they believe violate the restriction on the availability of proxy registrations, following which appropriate action may be taken by us. Publication of these conditions on the abuse page of our Registry website ensures that registrants are aware that despite utilisation of a proxy registration service, actual Whois information will be provided to LEA upon request in order to hold registrants liable for all actions in relation to their domain name. The certainty of Whois disclosure of domain names which draw the attention of LEA, deters those seeking to register domain names for abusive purposes.

6. CONTROLS FOR PROPER ACCESS TO DOMAIN FUNCTIONS

We realize that registrants often do not willfully use their domain names for abusive purposes, but domain names end up being compromised because of a lapse in security. Though this cannot always be controlled or mitigated by the registry, we are nevertheless committed to ensure that adequate safeguards are implemented to prevent domain names from being compromised and thereby making them prone to abuse.

6.1 MULTI-FACTOR AUTHENTICATION AND SECURE CONNECTIVITY FOR REGISTRARS

Through the contractual agreement with the registry, registrars will be expected to develop and employ in their domain name registration business, all necessary technology and restrictions to ensure that their connection to the registry is secure. All data exchanged between the registrar's system and the registry shall be protected to avoid unintended disclosure of information. Each EPP session shall be authenticated and encrypted using two-way secure socket layer ("SSL") protocol. Registrars will also agree to authenticate every EPP client connection with the registry using both an X.509 server certificate issued by a commercial Certification Authority identified by the registry and their registrar password, disclosed only to their respective employees on a need-to-know basis. Registrars will also access the SRS Web interface by utilizing an additional two-factor authentication token. Further details on this is provided in the response to Question 24 and 25

6.2 ENFORCEMENT OF STRONG AUTHCODES

Every domain name will have a strong authorization (authinfo) code, composed of alphabets, numerals, and special characters. An inter-registrar domain name transfer will not be permitted unless the registrant provides this authorization code at the time of executing the transfer process.

6.3 NOTIFICATION FOR EVERY UPDATE

We plan to notify the domain name holder upon any update made to a domain name. The notification will be committed through email to either or both of the registrant and technical contact of the domain name.

6.4 REGISTRY LOCK

Certain mission-critical domain names such as transactional sites, email systems and site supporting applications may warrant a higher level of security. 'Registry locking' is a feature which allows registrants to prohibit any updates at the Registry Operator level. This service will be available programmatically via EPP, so all registrars will be able to offer it in real-time to their registrants. The feature will prevent unintentional transfer, modification or deletion of the domain name, and mitigates the potential for abuse by prohibiting any unauthorised updates that may be associated with fraudulent behaviour. For example, an attacker may update name servers of a mission critical domain name, thereby redirecting customers to an illegitimate website without actually transferring control of the domain name. This is described in detail in our response to Question 27

6.5 AWARENESS PROGRAMS

In accordance with our commitment to operating a secure and reliable TLD, we will attempt to improve registrant awareness of the threats of domain name hijacking, registrant impersonation

and fraud, and emphasize the need for registrants to keep registration information accurate and confidential. Awareness will be raised by:

* Publishing the necessary information on the Abuse page of our Registry website in the form of videos, presentations and FAQs;

* Developing and providing to registrants, resellers and Registrars Best Common Practices that describe appropriate use and assignment of domain auth info codes and risks of misuse when the uniqueness property of this domain name password is not preserved.

7. RESOURCING PLANS

7.1 PERSONNEL

Functions described herein will be performed by -
* Directi Group staff under contract with us -
** Abuse & Compliance Team
* Dispute Resolution Service Providers that are selected wrt UDRP and SDRP

Directi Group possesses an exemplary track record of diffusing abuse on 4 million plus domains under their Registrar. The abuse mitigation function of our Registry will be handled by the same team that currently manages this process for the registrar businesses.

The existing compliance team comprises of:
* 1 Compliance Manager
* 1 Team Supervisor
* 4 Cyber Security Analysts
* 9 Compliance Officers

The compliance function is staffed on a 24⁄7⁄365 basis and capable of handling up to a peak of 52,800 unique abuse incidents per year. Each incident by itself can relate to a few to hundreds of domain names.

While this team is trained to investigate and verify all types of issues, they can also fall back on support from our technical staff when required. Similarly, abuse cases following new or unexpected parameters may also be escalated to legal support staff for expert counsel.

Our estimates of resource sizing are directly derived from the abuse case incident volumes currently experienced. On a base of 4 million domains across our Registrar businesses within Directi, each year we experience approximately:

* 6000 malware related abuses
* 1600 phishing abuses
* 1200 spam cases
* 600 pharmacy related abuses
* 5600 large botnet related abuse cases annually

This averages an incident rate of approximately 15,000 cases of abuse per year or 3.75 incidents per 1000 names

Since registries delegate a large portion of their abuse responsibilities to registrars, it is fair to assume that our registry’s abuse incident ratio will be lower than what we experience as registrars. In fact, in our case 2⁄3 categories of incidents will be delegated to the registrar and our direct involvement is expected in only 25%-35% of all incidents. However, given our proactive approach, importance on ensuring a clean and secure namespace, and aggressive SLAs, we choose to be conservative by assuming that we will be involved in 75% of all incidents.

Based on our projections, we expect .Web to reach 471,482 domain names at the end of the 3rd year. Extrapolating from our current rate of 3.75 incidents per 1000 names, we can expect around 1,768 abuse incidents yearly and be involved in 1,326 (75%) of them. Including the estimated 78 RPM incidents (details in our response to Q29), brings our total projected incident count to 1,404. This conservative estimate also accounts for the aggressive SLAs at

multiple levels, law enforcement interfacing and having a single POC available at all times.

The Compliance desk works as a centralized team and all team members are responsible for all abuse complaints across all businesses of Directi. Costs of the Compliance team are then allocated to each business based on the % utilization of the compliance team by each business. We have assumed 25% of 2 compliance officers' time towards .Web. Given that our 15 people team has the capacity to handle 52,800 incidents yearly, 2 officers with 25% of their time, will have a total capacity to handle 1,760 incidents annually. . It is important to point out that 25% of the 2 officers is merely a cost allocation method and in actuality all 15 members and more of the Compliance team will be available to resolve abuse issues for TLD.

Our planning provides us redundant capacity of 250%+ in Y1, 85% in Y2 and 25% in Y3, to handle both abuse as well as RPM related cases such as those involving URS. This leaves substantial headroom for rapid growth of domains under management, or a sudden surge in abuse incident rates per domain.

It is also important to note that there exists some economies of scale in our operations since a large number of these cases are dealt with in bulk, or large batches, as they relate to the same instigator(s).

The abuse team has a structured training program in place which enables them to rapidly scale-up resources when required. Typically a team of recruits are given four weeks of training and two weeks on the floor before they are fully activated.

Given the rapid growth rate of Directi businesses, Directi will continue to hire and maintain a sizable buffer over and above anticipated growth.

7.2 FINANCIAL CONSIDERATIONS

The usage of Directi Group's staff is included in our contract with Directi attached to Q46 ('Q46_References: Service and Facilities Commitment Agreement'). This cost is shown in the financial answers.

This completes our response to Q28.

29. Rights Protection Mechanisms

DotWeb Inc. is a wholly owned subsidiary within the Directi Group. The Directi Group runs various businesses including several ICANN Accredited Domain Registrars (including ResellerClub.com and BigRock.com) and Web Hosting companies. At Directi, through our decade long experience as a domain name registrar, we have consciously strived to ensure that domain registrations through our platform do not violate the intellectual property or other rights of any person or organization.

Our experience as a domain name registrar gives us insight into the necessity and importance of rights protection, and the mechanisms that must be employed to assure it. With .Web, we shall leverage our experience to implement a comprehensive set of policies and procedures that will uphold intellectual property rights to the greatest possible extent.

The protection of trademark rights is a core goal of .Web. .Web will have a professional plan for rights protection. It will incorporate best practices of existing TLDs, going above and beyond the ICANN mandated RPMs to prevent abusive registrations and rapidly take-down abuse when it does occur.

1. PREVENT ABUSIVE REGISTRATIONS

We will put into place the following measures to ensure prevention of registrations that infringe the IP rights of others

1.1 SUNRISE PROCESS

Our sunrise registration service will provide trademark holders with atleast a 30-day priority period in which to register their trademarks as domain names.

Sunrise Timeline -
Day 1:Single sunrise round opens
Day 30:Sunrise round closes
Day 31:Sunrise allocation begins and Sunrise period ends

1.1.1 SUNRISE POLICY SUMMARY AND SDRP SUMMARY

This section provides a summary of our Sunrise Policy and SDRP. We have formulated our policies and processes based on existing guidance concerning Sunrise and TMCH provided by ICANN. Any additional guidance in the future that requires changes to our process and policies will be implemented.

Through our Sunrise Policy we will offer atleast one 30-day sunrise round in which trademark holders satisfying the Sunrise eligibility requirements proposed in the ‘gTLD Applicant Guidebook’ will be eligible to apply for a domain name. This sunrise period will be the first opportunity for registration of domain names in .Web. Trademarks upon which sunrise applications are based must meet the criteria defined in the ‘gTLD Applicant Guidebook’ and be supported by an entry in the TMCH.

Sunrise allocation will start at the end of the 30-day sunrise period. If one validated application is received for a domain name, the same will be allocated to the applicant in the 10-day period following the end of the sunrise period. Where multiple validated applications are received for a domain name, the name will be allocated by auction. Domain names registered during the sunrise period will have a min. term of 2 yrs.

We will adopt a Sunrise Dispute Resolution Policy (‘SDRP’) to allow any party to raise a challenge on the four grounds identified in the ‘gTLD Applicant Guidebook’. All registrants will be required to submit to proceedings under the SDRP. SDRP claims may be raised at any time after registration of a domain name.

1.1.2 IMPLEMENTATION

1.1.2.1 SUNRISE PRICING

We plan to charge a non-refundable Sunrise application fee or validation fee of $80 for every Sunrise application. We have arrived at the fee to offset the cost of the trademark validation and other administrative over-heads.

1.1.2.2 SUNRISE IMPLEMENTATION PLAN

1. Prior to sunrise, trademark holders should apply for inclusion of their marks in the TMCH database.
2. Our Sunrise Policy and SDRP will be published on our website.
3. A trademark holder satisfying the sunrise eligibility requirements will pay the non-refundable sunrise application fee and submit its application corresponding to its TMCH entry to a registrar along with evidence of the corresponding TMCH entry.
4. Registrars will send the sunrise applications to ARI. They will be charged the application fee at this time.
5. ARI will perform standard checks to ensure that the domain name is technically valid and hold the application for subsequent allocation.
6. Upon conclusion of the 30-day sunrise period, ARI will compile a list of applied-for names and reserve these from registration in land rush and general availability.
7. Sometime during this process ARI or the registrar (as prescribed) will identify all sunrise applications which constitute an ‘Identical Match’ (as defined in the ‘gTLD Applicant Guidebook’) with a TMCH entry and provide notice to the holders of the filing of a sunrise registration.
8. Where a single sunrise application exists for a particular domain name ARI will enable the sponsoring registrar to CREATE the domain name and we will charge the sunrise registration fee to the registrar.

9. Where multiple sunrise applications exist for a domain name, ARI will compile and communicate to a 3rd-party auction services provider appointed by us a list of competing applicants, who will be invited to participate in an auction for the domain name.
10. The auction services provider will facilitate the auction process and upon completion of the auction will notify all participants of the outcome and collect the auction payment from the winning participant.
11. Upon payment of the auction bid, the auction services provider will communicate to ARI the details of the winning auction participant and will submit the revenue collected to ARI. ARI will validate the communication from the auction services provider and enable the sponsoring registrar to CREATE the domain name.

1.1.1.3 SDRP IMPLEMENTATION PLAN

When a domain is awarded and granted to a registrant, that domain will be available for lookup in the public WHOIS.

After a Sunrise name is awarded it will also remain under a “Sunrise Lock” status for at least 60 days. During this period the domain will not resolve and cannot be modified, transferred, or deleted by the sponsoring registrar. A domain name will be unlocked at the end of that lock period only if it is not the subject of a Sunrise Challenge. Challenged domains will remain locked until the dispute resolution provider has issued a decision, which the registry operator will promptly execute.

SDRP filings will be handled by an appropriate service provider as per ICANN guidance and policy.

1.1.1.4 IMPLEMENTATION THROUGH CONTRACTUAL RELATIONSHIPS

The following features of the Sunrise and SDRP implementation plans described above will be executed by the inclusion of corresponding clauses in our RRA, which will require inclusion in registrars’ Domain Name Registration Agreements:
* By making a sunrise application the applicant agrees to purchase the domain name if that name is allocated to the applicant.
* The sunrise application fee is non-refundable.
* All sunrise applicants must submit to proceedings under the SDRP.

1.2 TRADEMARK CLAIMS SERVICE

For atleast 60 days during general availability we will offer the trademark claims service as described in the ‘gTLD Application Guidebook’.

1.2.1 IMPLEMENTATION

1.2.1.1 TRADEMARK CLAIMS SERVICE IMPLEMENTATION PLAN
This process will be executed for atleast the first 60 days of general availability:
1. an applicant will make an application to a registrar for a domain name.
2. Registrars will be required to communicate land rush application information to our registry backend provider - ARI.
3. ARI or Registrars (as prescribed) will interface with the TMCH to determine whether an applied-for domain name constitutes an ‘Identical Match’ with a trademark in the TMCH. If an ‘Identical Match’ is identified, the registrar will provide to the land rush applicant a Trademark Claims Notice in the form prescribed by the ‘gTLD Applicant Guidebook’. Following receipt of this notice a land rush applicant must communicate to the registrar its decision either to proceed with or abandon the registration.
4. ARI or Registrar (as prescribed) will interface with the TMCH to promptly notify relevant mark holders of the registration of a domain name constituting an ‘Identical Match’ to their TMCH entry.

1.2.1.2 IMPLEMENTATION THROUGH CONTRACTUAL RELATIONSHIPS

The following features of our Trademark Claims Service Implementation Plan described above will be executed by the inclusion of corresponding clauses in our RRA:
* Registrars must comply with the TMCH as required by ICANN and the TMCH Service Provider⁄s.

* Registrars must not in their provision of the trademark claims service make use of any other trademark information aggregation, notification or validation service other than the TMCH.
* In order to prevent a chilling effect on registration, registrars must ensure that land rush applicants are not prevented from registering domain names considered an 'Identical Match' with a mark in the TMCH.
* Registrars must provide clear notice in the specific form provided by the 'gTLD Applicant Guidebook' to the prospective registrant of relevant entries in the TMCH.
* Registrars must interface with the TMCH as prescribed to relevant mark holders of the registration of a domain name constituting an 'Identical Match' to their TMCH entry.

2. ONGOING RIGHTS PROTECTION AND ABUSE PREVENTION

Below we describe ongoing RPMs which we will implement to mitigate cybersquatting and other types of abusive behaviour such as phishing and pharming.

2.1 UNIFORM RAPID SUSPENSION (URS)

The URS (Uniform Rapid Suspension) procedure is a new RPM the implementation of which is mandated in all new gTLDs. Understanding that a fundamental aim of the URS is expediency, all of the steps in our Implementation Plan below will be undertaken as soon as practical but without compromising security or accuracy.

2.1.1 IMPLEMENTATION

2.1.1.1 URS IMPLEMENTATION PLAN

1. We will provide to each URS provider an email address to which URS-related correspondence can be sent. On an ongoing basis, our compliance desk will monitor this email address for receipt of communications from URS providers, including the Notice of Complaint, Notice of Default, URS Determination, Notice of Appeal and Appeal Panel Findings.
2. We will validate correspondence from a URS provider to ensure that it originates from the URS Provider.
3. We will within 24 hours of receipt of a URS Notice of Complaint lock the domain name/s the subject of that complaint by restricting all changes to the registration data, including transfer and deletion of the domain name. The domain name will continue to resolve while in this locked status.
4. We will immediately notify the URS provider in the manner requested by the URS provider once the domain name/s have been locked.
5. Upon receipt of a favourable URS Determination we will unlock the domain name and redirect the nameservers to an informational web page provided by the URS provider. While a domain name is locked, our backend provider - ARI - will continue to display all of the WHOIS information of the original registrant except for the redirection of the nameservers and the additional statement that the domain name will not be able to be transferred, deleted or modified for the life of the registration.
6. Upon receipt of notification from the URS provider of termination of a URS proceeding we will promptly unlock the domain name and return full control to the registrant.
7. Where a default has occurred (because a registrant has not submitted an answer to a URS complaint in accordance with the 'gTLD Applicant Guidebook') and a Determination has been made in favour of the complainant, in the event that we receive notice from a URS provider that a Response has been filed in accordance with the 'gTLD Applicant Guidebook', we will as soon as practical restore a domain name to resolve to the original IP address while preserving the domain's locked status until a Determination from de novo review is notified to us.
8. We will ensure that no changes are made to the resolution of a registration the subject of a successful URS Determination until expiry of the registration or the additional registration year unless otherwise instructed by a UDRP provider.
9. We will make available to successful URS complainants an optional extension of the registration period for one additional year.

2.1.1.2 IMPLEMENTATION OF THE URS THROUGH CONTRACTUAL RELATIONSHIPS

The following features of our URS Implementation Plan described above will be executed by the inclusion of corresponding clauses in our RRA:

* In the event that a Registrant does not submit an answer to a URS complaint in accordance with the ‘gTLD Applicant Guidebook’, registrars must prevent registrants from making changes to the WHOIS information of a registration while it is in URS default.
* Registrars must prevent changes to a domain name when a domain is in locked status to ensure that both the Registrar’s systems and Registry’s systems contain the same information for the locked domain name.
* Registrars must not take any action relating to a URS proceeding except as in accordance with a validated communication from us or a URS provider.

2.2 UDRP

The UDRP (Uniform Domain Name Dispute Resolution Policy) is applicable to domain name registrations in all new gTLDs. It is available to parties with rights in valid and enforceable trade or service marks and is actionable on proof of all of the following three grounds:
1. The registrant’s domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights.
2. The registrant has no rights or legitimate interests in respect of the domain name.
3. The registrant’s domain name has been registered and is being used in bad faith.

The remedies offered by the UDRP are cancellation of a domain name or transfer of a domain name registration to a successful UDRP claimant.

2.2.1 IMPLEMENTATION

2.2.1.1 UDRP IMPLEMENTATION PLAN

We have two responsibilities in order to facilitate registrars’ implementation of the UDRP -
1. Our backend provider – ARI - will maintain awareness of UDRP requirements and be capable of taking action when required and sufficiently skilled and flexible to respond to any changes to UDRP policy arising from future consensus policy reviews.
2. We will provide EPP and the SRS web interfaces to enable registrars to perform required UDRP functions in accordance with the Policy on Transfer of Registrations between Registrars.

2.2.1.2 IMPLEMENTATION OF THE UDRP THROUGH CONTRACTUAL RELATIONSHIPS

The UDRP is applicable to domain name registrations in all new gTLDs by force of a contractual obligation on Registry Operators to use only ICANN-accredited registrars, who in turn are contractually required to incorporate the UDRP in their Domain Name Registration Agreements.

3. ADDITIONAL RIGHTS PROTECTION MECHANISMS

The protection of trademark rights is a core goal of .Web. Our Right Protection Mechanisms, policies and procedures go significantly above and beyond the minimum mandated RPMs to prevent abusive registrations, rapidly take-down abuse when it occurs, and foster a clean namespace for .Web

This section describes several other RPMs that .Web will implement that exceed the minimum requirements for RPMs and align with our goal of creating a namespace that provides maximum protection to trademark holders.

3.1 OPTIONAL TRADEMARK DECLARATION

This is a unique feature of our .Web TLD. During General Availability, we will continue to make available, the EPP Trademark extension fields that are provided during sunrise. Registrants will be able to specify their IPR details against their domain names even after sunrise. The fields will include – word mark, registration number, applied date, registration date, jurisdiction, class. These fields will be editable by the Registrant and visible in Whois.

The ability for a Registrant to voluntarily declare Trademark data even during general availability will reduce potential confusion amongst mark holders and the general public and

reduce unnecessary UDRP procedures.

3.2 PROFILING & BLACKLISTING

This process, currently in practice for our registrar businesses within the Directi Group, is used for gathering intelligence on known offenders. We maintain abuse ratios for each of the 1,000,000 plus registrants and 65,000 plus resellers who use Directi.

Experience has enabled us to use these ratios accurately to uncover registrants who are known and repeated offenders. Expert offenders rarely reuse the same registrant profile and often maintain a myriad number of profiles to mask their true identity. Through pattern mapping we try and group registrant profiles that we believe belong to the same operator.

The same process is followed at the reseller level too, to identify those resellers who are knowingly harboring offenders, or are themselves involved in abuse.
When a registrant profile is confirmed to be involved in organized abuse, including but not limited to cybersquatting, phishing, pharming etc., our immediate step is to suspend that customer's control over his abusive domain portfolio. Our compliance team then carefully analyzes each domain name to identify those which are abusive and not already taken-down. The necessary action is undertaken to diffuse any ongoing abuse.

We plan to adopt the 'Profiling and Blacklisting' process within our registry operations. Since all of our compliance resources will be trained and experienced in running this process, its implementation into .Web will be simple. Specifics of this policy and process, as it applies to our registry business, will be drawn out.

3.3 PROACTIVE DOMAIN QUALITY ASSURANCE

As a preventive safeguard against abusive domain registration, we follow a consistent review process for domain registrations on our registrar, where a sample of newly registered domain names are analyzed for potential abusive activity. Coupled with our profiling process (described above), it enables us to take proactive measures against domain names that are registered solely to perpetrate malicious activities such as phishing, or otherwise infringe on the rights of others. This helps us curb abusive activity before it can affect too many Internet users. We shall seek to implement similar safeguards for .Web, and encourage registrars to incorporate this practice as part of their abuse mitigation processes.

3.4 INDUSTRY COLLABORATION

3.4.1 ACTIVE INVOLVEMENT WITH SECURITY AGENCIES

In order to mitigate abuse of domain names on our registrar business, our abuse team has active involvement in helping security vendors and researchers fight domain abuse. They provide us a constant feed of abuse instances and help us identify domain names involved in activities like phishing or pharming. Some of the prominent organizations we work with include PhishLabs (phishing), LegitScript (illegal pharmaceutical distribution), Artists Against 419 (financial scams), Knujon (spam) etc. We will leverage these relationships to ensure oversight for all domain names registered within .Web.

3.4.2 APWG REVIEW

Every six months, the Anti-Phishing Working Group (APWG) publishes its latest Global Phishing Survey [See http://www.apwg.org/resources.html#apwg]. This study contains an analysis of phishing per TLD. We will review the performance of our anti-abuse program against the APWG reports, and other metrics created by the security community. We will work closely with APWG to combat phishing within .Web

3.4.3. MESSAGE OF ZERO TOLERANCE

Our Anti-Abuse Policy will put Registrants on notice of the ways in which we will identify and respond to abuse and serve as a deterrent to those seeking to register and use domain names for abusive purposes. The policy will be made easily accessible on the Abuse page of our Registry website which will be accessible and have clear links from the home page along with

FAQs and contact information for reporting abuse.

The Directi Group has vast experience in minimizing abusive registrations. Our zero tolerance procedures and aggressive proactive takedown measures as a Domain Registrar have resulted in a white-hat reputation discouraging abusive registrations to begin with. We intend on following the same approach with respect to Registry operations for .Web. Our proactive abuse procedures are geared towards building a reputation that discourages miscreants and malicious intent. Once it is known that abusive registrations and registrations in violation of our policies are suspended rapidly, this will directly result in discouraging abusive registrations and creating a clean namespace. While following this path will mean a higher compliance and abuse vigilance cost for us, we believe this effort will pay us long term rewards through abusers keeping away and .Web becoming recognized as a reputable namespace.

4. REDUCING PHISHING AND PHARMING

All of the measures we have described in the preceding sections significantly reduce phishing and pharming within .Web. These include RPMs like URS and UDRP.

Over and above this our coordination with APWG, Industry Collaboration, Profiling and Blacklisting processes and Proactive measures described in Section 3 above will go a long way in ensuring a clean namespace for .Web and considerably reduced phishing and pharming activities.

5. PREVENTING TRADEMARK INFRINGEMENT IN OPERATING THE REGISTRY

We take seriously our responsibilities in running a registry and we understand that while offering a sunrise registration service and the trademark claims service during start-up of our TLD and the URS and UDRP on an ongoing basis serves to minimise abuse by others, this does not necessarily serve to minimise trademark infringement in our operation of the TLD. This responsibility is now clearly expressed and imposed upon registries through the new Trademark PDDRP [Post-Delegation Dispute Resolution Procedure], which targets infringement arising from the Registry Operator’s manner of operation or use of its TLD.

Whilst we will as required under the Registry Agreement agree to participate in all Trademark PDDRP procedures and be bound by the resulting determinations, we will also have in place procedures to identify and address potential conflicts before they escalate to the stage of a Trademark PDDRP claim.

5.1 IMPLEMENTATION

1. We will notify to the Trademark PDDRP provider⁄s contact details to which communications regarding the Trademark PDDRP can be sent.
2. We will publish our Anti-Abuse Policy on a website specifically dedicated to abuse handling in our TLD.
3. Using the single abuse point of contact discussed in detail in our response to Q28, a complainant can notify us of its belief that that one or more of its marks have been infringed and harm caused by our manner of operation or use of our TLD
4. We will receive complaints submitted through the single abuse point of contact.
5. The Compliance Team will acknowledge receipt of the complaint and commence investigation of the subject matter of the complaint and good faith negotiations with the complainant in accordance with the ‘gTLD Applicant Guidebook’.
6. On an ongoing basis, our Compliance Team will monitor the email address notified to the Trademark PDDRP provider⁄s for all communications from the Trademark PDDRP provider, including the threshold determination, Trademark PDDRP complaint, complainant’s reply, notice of default, expert panel determinations, notice of appeal and determinations of an appeal panel.
7. In the event that a complaint cannot be resolved and a Trademark PDDRP claim is made, we will do the following:

* File a response to the complaint in accordance with Trademark PDDRP policy section 10 (thus avoiding, whenever possible, a default situation).
* Where appropriate, make and communicate to the Trademark PDDRP provider decisions regarding the Trademark PDDRP proceeding, including whether to request a three-person Trademark PDDRP Expert Panel, request discovery, request and attend a hearing, request a de novo appeal,

challenge an ICANN-imposed Trademark PDDRP remedy, initiate dispute resolution under the Registry Agreement, or commence litigation in the event of a dispute arising under the Trademark PDDRP.
* Where appropriate, undertake discovery in compliance with Trademark PDDRP policy section 15, attend hearings raised under section 16 if required, and gather evidence in compliance with sections 20.5 and 20.6.
8. We will upon notification of an Expert Panel finding in favour of the Claimant (Trademark PDDRP policy section 14.3), reimburse the Trademark PDDRP Claimant.
9. We will implement any remedial measures recommended by the expert panel pursuant to Trademark PDDRP policy and take all steps necessary to cure violations found by the expert panel and notified by ICANN.

6. RESOURCING PLANS

6.1 PERSONNEL

Functions described herein will be performed by:

* Directi Group Abuse and Compliance team under contract with us -
** Overseeing Sunrise process
** URS
** Abuse complaints concerning RPM

* ARI’s backend Registry
* Service Providers that are selected wrt TMCH, UDRP, URS and SDRP

* Director of Technology at .Web & Account Management staff at .Web
** Overseeing Sunrise process
** Communication of the sunrise process to Registrars

Directi Group possesses an exemplary track record of diffusing abuse on 4 million plus domains under their Registrar business. The Rights protection and abuse mitigation function of our Registry will be handled by the same team that currently manages this process for the registrar businesses.

The existing compliance team comprises of:

* 1 Compliance Manager
* 1 Team Supervisor
* 4 Cyber Security Analysts
* 9 Compliance Officers

The compliance function is staffed on a 24⁄7⁄365 basis and capable of handling up to a peak of 52,800 unique abuse incidents per year. Each incident by itself can relate to a few to hundreds of domain names.

While this team is trained to investigate and verify all types of issues, they can also fall back on support from our technical staff when required. Similarly, abuse cases following new or unexpected parameters may also be escalated to legal support staff for expert counsel.

Our estimates of resource sizing are directly derived from the abuse case incident volumes currently experienced. On a base of 4 million domains as a Registrar, we experience approximately the following incidents per year:
* UDRP Cases - 200
* Other RPM incidents - 20 cases

This averages an incident rate of approximately 220 cases of abuse per year or 0.055 incidents per 1000 names. Given that this is based on a more mature base of names, it would be prudent to assume a higher rate of activity for .Web. Based on our experience we have assumed the increase in activity rate to be three fold (300% of the current rate) and increase it to 0.165 per 1000 names.

Based on our projections, we expect .Web to reach 471,482 domain names at the end of the third

year. Extrapolating from our estimated rate of 0.165 incidents per 1000 names, we can expect around 78 incidents yearly. Including the estimated 1,326 Abuse incidents that the registry will handle (details in our response to Q28), brings our total projected incident count to 1404.

The Compliance desk works as a centralized team and all team members are responsible for all abuse complaints across all businesses of Directi. Costs of the Compliance team are then allocated to each business based on the % utilization of the compliance team by each business. We have assumed 25% of 2 compliance officers' time towards .Web. Given that our 15 people team has the capacity to handle 52,800 incidents yearly, 2 officers with 25% of their time, will have a total capacity to handle 1,760 incidents annually which is more than adequate for the Registry. It is important to point out that 25% of the 2 officers is merely a cost allocation method and in actuality all 15 members and more of the Compliance team will be available to resolve abuse issues for TLD.

Our planning provides us redundant capacity of 250%+ in Y1, 85% in Y2 and 25% in Y3, to handle both abuse as well as RPM related cases such as those involving URS. This leaves substantial headroom for rapid growth of domains under management, or a sudden surge in abuse incident rates per domain.

It is also important to note that there exist some economies of scale in our operations since a large number of these cases are dealt with in bulk, or large batches, as they relate to the same instigator(s).

The Abuse and Compliance team has a structured training program in place which enables them to rapidly scale-up resources when required. Typically a team of recruits are given four weeks of training and two weeks on the floor before they are fully activated.

Given our rapid growth rate and business expansion plans, we will continue to hire and maintain a sizable buffer over and above anticipated growth.

6.2 FINANCIAL COSTS

The usage of Directi Group's staff is included in our contract with Directi attached to Q46. This cost is shown in the financial answers.

This completes our response to Q29.

30(a). Security Policy: Summary of the security policy for the proposed registry

We have engaged ARI Registry Services (ARI) to deliver services for this TLD. ARI provide registry services for a number of TLDs including the .au ccTLD. For more background information on ARI please see the attachment 'Q30a – ARI Background & Roles.pdf'. This response describes Security as implemented by ARI under direction from us taking into account any specific needs for this TLD.

1. SECURITY POLICY SUMMARY

ARI operates an ISO27001 compliant Information Security Management System (ISMS) for Domain Name Registry Operations; see attachment 'Q30a – SAI Global Certificate of Compliance.pdf'. The ISMS is an organisation-wide system encompassing all levels of Information Security policy, procedure, standards, and records. Full details of all the policies and procedures included in the ISMS are included in the attachment to Question 30b.

1.1 THE ISMS

ARI's ISMS's governing policy:
* Defines the scope of operations to be managed (Domain Name Registry Operations).
* Designates the responsible parties (COO, CTO and Information Security Officer) for governance, Production Support Group for implementation and maintenance, and other departments

for supporting services.
* Requires a complete Risk Assessment (a developed Security Threat Profile for the Service – in this case registry services for the TLD – and a Risk Analysis tracing threats and vulnerabilities through to Risks) and Risk Treatment Plan (each major risk in the Risk Assessment references the Statement of Applicability indicating controls to be implemented, responsible parties, and the effectiveness metrics for each).
* Includes a series of major sub policies governing security, which include but are not limited to:
 ** ICT acceptable use policy and physical security policies.
 ** PSG Security Policy which outlines the registry operations policies, the management of end-user devices, classification of networks and servers according to the classification of information they contain, networking, server & database configuration and maintenance guidelines, vulnerability and patch management, data integrity controls, access management, penetration testing, third party management, logging and monitoring, and cryptography.
* Requires ongoing review:
 ** Of risks, threats, the Risk Treatment Plan, client requirements and commitments, process and policy compliance, process and policy effectiveness, user etc.
 ** Regular internal and external penetration testing & vulnerability scanning.
 ** Ad-hoc review raised during normal operations, common sources being change management processes, scheduled maintenance or project debriefs, and security incidents.
 ** Yearly review cycle which includes both internal and external audits, including external surveillance audits for compliance.
 ** Additional yearly security controls assessment reviews, which include analysis of the security control implementations themselves (rather than compliance with any particular standard).
 ** At 24 month intervals, external penetration testing of selected production services.
 ** Periodic ISO reaccreditation
ARI's ISMS encompasses the following ARI standards:
* Configuration standards for operating systems, networking devices and databases based on several key publications, including those released by NIST (e.g. SP800-123, SP800-44v2, SP-800-40, SP800-41) and the NSA, staff testing and experience, and vendor supplied standards.
* Security Incident Classification, which identifies the various classifications of security incidents and events to ensure that events that qualify as security incidents.
* Information Classification and Handling which specifies the information classification scheme and the specific requirements of handling, labelling, management and destruction for each level of classification.

1.2 SECURITY PROCESSES

Processes are used to implement the policies. These include, but are not limited to:

1.2.1 CHANGE MANAGEMENT

This includes change management and its sub-processes for access management, software deployment, release of small changes and scheduled maintenance. This process includes:
* The classification of changes and the flow into sub processes by classification.
* The release and deployment process for change control into production environments, outlining peer review, testing steps, approval points, checklist sets, staging requirements and communication requirements.
* The software release and deployment process with its specific testing and staged rollout requirements.
* The scheduled maintenance process and its various review points.

1.2.2 INCIDENT MANAGEMENT

This includes incident management process and its sub-process for unplanned outages. These outline:
* How incidents are managed through escalation points, recording requirements, communication requirements etc.
* The unplanned outage procedure which applies directly to situations where the registry itself or other critical services are unexpectedly offline.

1.2.3 PROBLEM MANAGEMENT

The goal of problem management is to drive long term resolution of underlying causes of incidents. This process centres on finding and resolving the root causes of incidents. It defines escalation points to third parties or other ARI departments such as Development, as well as verification of the solution prior to problem closure.

1.2.4 SECURITY INCIDENT MANAGEMENT

This process deals with the specific handling of security incidents. It outlines the requirements and decision points for managing security incidents. Decision points, escalation points to senior management and authorities are defined, along with evidence-gathering requirements, classification of incidents and incident logging.

1.2.5 ACCESS MANAGEMENT

This process handles all access changes to systems. HR must authorize new users, and access changes are authorized by departmental managers and approved by the Information Security Officer.
When staff leave or significantly change roles, a separation process is followed which ensures all access that may have been granted during their employment (not just their initially granted access) is checked and where appropriate, revoked.
Finally, quarterly review of all access is undertaken by the ISO, reviewing and approving or rejecting (with an action ticket) as appropriate.

2. ARI’s SECURITY INFRASTRUCTURE SOLUTIONS

ARI has developed a layered approach to IT security infrastructure. At a high level, some of the layers are as follows:
* DDoS countermeasures are employed outside ARI networks. These include routing traps for DDoS attacks, upstream provider intervention, private peering links and third party filtering services.
* Routing controls at the edge of the network at a minimum ensures that only traffic with valid routing passes into ARI networks.
* Over-provisioning and burstable network capabilities help protect against DoS and DDoS attacks.
* Network firewalls filter any traffic not pre-defined by network engineering staff as valid.
* Application layer firewalls then analyse application level traffic and filter any suspicious traffic. Examples of these would be an attempt at SQL injection, script injection, cross-site scripting, or session hijacking.
* Server firewalls on front-end servers again filter out any traffic that is not strictly defined by systems administrators during configuration as valid traffic.
* Only applications strictly necessary for services are running on the servers.
* These applications are kept up-to-date with the latest security patches, as are all of the security infrastructure components that protect them or that they run on.
* ARI infrastructure is penetration-tested by external tools and contracted security professionals for vulnerabilities to known exploits.
* ARI applications are designed, coded and tested to security standards such as OWASP and penetration-tested for vulnerabilities to common classes of exploits by external tools and contracted security professionals.
* ARI configures SELinux on its production servers. Specific details of this configuration is confidential; essentially any compromised application is extremely limited in what it can do.
* Monitoring is used to detect security incidents at all layers of the security model. Specifically
** Network Intrusion Detection systems are employed to monitor ARI networks for suspicious traffic.
** ARI maintains its own host-based Intrusion Detection system based on tripwire, which has now undergone four years of development. Specific details are confidential, but in summary, the system can detect any unusual activity with respect to configuration, program files, program processes, users, or network traffic.
** More generic monitoring systems are used as indicators of security incidents. Any behaviour outside the norm across over 1,100 individual application, database, systems, network and environmental checks is investigated.
* Capacity management components of the monitoring suite are also used to detect and classify

security incidents. Some examples are:
** Network traffic counts, packet counts and specific application query counts.
** Long term trend data on network traffic vs. specific incident windows.
** CPU, Storage, Memory and Process monitors on servers.
* A second layer of hardware firewalling separates application and middle tier servers from database servers.
* Applications only have as much access to database information as is required to perform their function.
* Finally, database servers have their own security standards, including server-based firewalls, vulnerability management for operating system and RDBMS software, and encryption of critical data.

2.1 PHYSICAL SECURITY INFRASTRUCTURE

ARI maintains a series of physical security infrastructure measures including but not limited to biometric and physical key access control to secured areas and security camera recording, alarm systems and monitoring.

3. COMMITMENTS TO REGISTRANTS

We commit to the following:
* Safeguarding the confidentiality, integrity and availability of registrant's data.
* Compliance with the relevant regulation and legislation with respect to privacy.
* Working with law enforcement where appropriate in response to illegal activity or at the request of law enforcement agencies.
* Maintaining a best practice information security management system that continues to be ISO27001-compliant.
* Validating requests from external parties requesting data or changes to the registry to ensure the identity of these parties and that their request is appropriate. This includes requests from ICANN.
* That access to DNS and contact administrative facilities requires multi-factor authentication by the Registrar on behalf of the registrant.
** That Registry data cannot be manipulated in any fashion other than those permitted to authenticated Registrars using the EPP or the SRS web interface. Authenticated Registrars can only access Registry data of domain names sponsored by them.
** A Domain transfer can only be done by utilizing the AUTH CODE provided to the Domain Registrant.
* That emergency procedures are in place and tested to respond to extraordinary events affecting the integrity, confidentiality or availability of data within the registry.

4. AUGMENTED LEVEL OF SECURITY

This TLD is a generic TLD and as such requires security considerations that are commensurate with its purpose. Our goal with this TLD is to provide registrants with adequate protections against unauthorized changes to their names, without making the registration process too onerous and thus increasing costs.
The following attributes describe the security with respect to the TLD:
* ARI, follows the highest security standards with respect to its Registry Operations. ARI is ISO 27001 certified and has been in the business of providing a Registry backend for 10 years. ARI have confirmed their adherence to all of the security standards as described in this application.
* Registrant will only be permitted to make changes to their domain name after authenticating to their Registrar.
* Registrants will only be able to access all interfaces for domain registration and management via HTTPS. A reputed digital certificate vendor will provide the SSL certificate of the secure site.
* Registrar identity will be manually verified before they are accredited within this TLD. This will include verification of corporate identity, identity of individuals involved / mentioned, and verification of contact information
* Registrars will only be permitted to connect with the SRS via EPP after a multi-factor authentication that validates their digital identity. This is described further ahead.
* Registrars will only be permitted to use a certificate signed by ARI to connect with the Registry systems. Self-signed certificates will not be permitted.

* The Registry is DNSSEC enabled and the TLD zone will be DNSSEC enabled. This is described in detail in our response to question 43.
* Registrar access to all Registry Systems will be via TLS and secured with multi-factor authentication. This is described in detail in our responses to Question 24 and Question 25. Where these requirements put controls on Registrars these will be enforced through the RRA.

5. RESOURCES

This function will be performed by ARI. The following resources are allocated to performing the tasks required to deliver the services described:
* Executive Management Team (4 staff)
* Production Support Group (27 staff)
ARI has ten years' experience designing, developing, deploying, securing and operating critical Registry systems, as well as TLD consulting and technology leadership.
As a technology company, ARI's senior management are technology and methodology leaders in their respective fields who ensure the organization maintains a focus on technical excellence and hiring, training and staff management.
Executive Management are heavily involved in ensuring security standards are met and that continued review and improvement is constantly undertaken. This includes the:
* Chief Operations Officer
* Chief Technology Officer
A detailed list of the departments, roles and responsibilities in ARI is provided as attachment 'Q30a – ARI Background & Roles.pdf'. This attachment describes the functions of the above teams and the exact number and nature of staff within.

ARI provides registry backend services to 5 TLDs and has a wealth of experience in estimating the number of resources required to support a registry system.

Based on past experience ARI estimates that the existing staff is adequate to support a registry system that supports in excess of 50M domains. Since this TLD projects 471,482 domains, 0.94% of these resources are allocated to this TLD. See attachment 'Q30a – Registry Scale Estimates & Resource Allocation.xlsx' for more information.

The Production Support Group is responsible for the deployment and operation of TLD registries.

ARI employs a rigorous hiring process and screening (Police background checks for technical staff and Australian Federal Government 'Protected' level security clearances for registry operations staff).

This completes our response to Q30(a).

© Internet Corporation For Assigned Names and Numbers.

EXHIBIT JMR-18

InetServices
Complete Internet Solutions

INSIDE THE HIGH STAKES AUCTION FOR .WEB

JULY 25, 2016 BY DEREK VAUGHAN

Inside the High Stakes Auction for .Web

Some very deep-pocketed internet giants are facing off on July 27, 2016 for a high stakes game of poker. The pot isn't cash but the rights to sell the coveted .web top level domain (TLD) extension to eager website owners, domain speculators, online entrepreneurs, developers, designers and digital ad agencies. Google, Web.com, United Internet and Afilias are among the seven competing entities who will bid in real time on July 27 via an online auction conducted by the non-profit organization ICANN (Internet Corporation for Assigned Names and Number) to confer the rights to sell .web.

The auction

If you have a ton of time on your hands and want to brush up on the legal details of how the auction process works you can read all about it here. For those who aren't lawyers here's a tl;dr version of how it works.

Step 1 – Become eligible for participating in the auction. The criteria are basically you must have an extra large sum of American dollars (auctions are all conducted in American dollars regardless of the top level domain) and be in good standing with ICANN.

Step 2 – Login to the auction interface on the day of the auction to bid. The larger your deposit is, the higher you can bid. A deposit of $2 million gives you an unlimited bidding potential. The bids are made through a series of ”rounds” where the floor and ceiling of that round are specified. If all bidders meet the ceiling of the round then a new round is started after a short break with the floor being set at the ceiling of the previous round. The rounds continue at higher and higher floors until there is only one bidder remaining. That bidder pays the second place bidder’s highest bid.

Big money bids and big money profits

So exactly what would the rights to sell the .web TLD be worth and what might the winning bid be? Consider that on Jan. 27, 2016 a number of large firms including Amazon, were bidding via an ICANN auction for the rights to the .shop TLD. After 14 rounds of bidding GMO Registry, Inc. won the rights with a winning bid of $41,501,000. Clearly the expectation is that the revenues derived from the .shop domains would well exceed the price paid. Note also that the current champion of newly minted TLDs is .xyz which has registered a total of nearly 6.5 million domains as of July 20, 2016. At a conservative estimate of only a one year registration period and an average price of $10 per domain that works out to around $65 million so far. Clearly the current bidders for .web hope that the number of .web registrations surpass those of .xyz making it potential worth in excess of $65 million.

So what could a winning bid look like? Using .shop as a proxy – it is certainly possible that .web could fetch a higher bid that .shop ($41,501,000) – but how much higher? Only the bidders know what their upper limits are. It is clear that the bidders all have substantial funds to bring to bear on the auction. Here are the recent market caps of three of the bidders who are publicly traded:

Alphabet Inc Class A (Google) – $514 Billion
United Internet AG – $8 Billion
Web.com – $950 Million

Would Google with its massive war chest of cash even blink at paying $50 million or more? Not likely. In fact Google paid over $18 million just to submit a list of TLDs that it wanted to pursue before ever arriving at the final sale price.

Could .Web become the new .Com

Is it likely that .web will be a standout among new TLDs? Here are a few points that may indicate .web is poised to gain traction relative to other recently introduced TLDs.

1. We’re already used to using the term ‘web’ for internet-related activities. We refer to online properties as ‘websites’ or ‘web pages’ and the talent who create them are ‘web designers’ and ‘web developers’. We use ‘web servers’ and ‘web browsers’ and even ‘web apps’. The common references make a transition to a .web domain a natural activity for a mass online and mobile audience.

2. .Web is short and memorable. With the explosion of new top level domains, it’s literally hard to keep track of them all or their proper use. A short generic term like .web could cut through all the clutter. It’s just simpler to type: yourcomany.web than say: yourcompany.company or yourcompany.solutions. It’s certainly less prone to confusion as well. Was it yourcompany.solution or yourcompany.solutions?

3. Large companies set standards. Imagine if Google won the auction and decided that every time someone searched for anything related to ‘domain names’ on Google – they would suggest trying the .web TLD as an alternative to .com. Standard set.

4. Dictionary names and short phrases are still available on .web. This is true of all new TLDs so it’s not unique to .web. However, simply offering a short, memorable and generic alternative to .com could be enough if the momentum gets behind this new domain.

Stuart Melling is co-founder of UK domain name firm 34SP.com with decades of domain name experience and he offered up his expert opinion on whether .web could be the next .com.

”There’s such a huge array of new domains available to buyers now making it very difficult for them to really understand the selection on offer. Likewise, I’ve yet to see any registrar (ourselves included) deliver a domain search tool that really nails domain discovery,” he says. “It boils down to marketing might at this point. The registries that will win are most likely going to be those that have the heftiest budgets to market and promote their domains. I personally see .com being the de facto domain for any new website for some time to come. Right now, the new TLDs seem to represent a fallback, a secondary area to secure a relevant domain if the .com space isn’t viable. I’d imagine it would take years to unseat this kind of approach; but then this is the web, and making predictions is really a fools game.”

What other domain experts think

Mark Medina, Director of Product, Domain Names with Dreamhost has been selling domain names to web businesses for over 15 years. Medina has some strong predictions for .web: “The winning bid for .shop was $41.5M, so I think the winning bid will definitely be north of $50M. Because there are multiple bidders, one of them being the mighty Google, I can foresee some pretty aggressive bids, which I think will take the final winning bid into the $80M – $100M range.”

”Everyone still wants a .com. We’ve done user testing on people searching for domains, where users speak their thoughts during the test, and almost all of them say ‘Where’s the .com?’ With that said, I can’t foresee .web becoming the new .com, but I think it will be one of the more popular new TLDs that could overtake .net in a few years,” Medina says. “The .net TLD has been losing its popularity, and I think TLDs like a .web or a .xyz could become more popular than .net in a few years time. .Com will remain number 1 but number 2 is up for the taking.”

Chris Sheridan is currently Head of Channel Sales at Weebly.com and has also held senior positions at domain registrars eNom and VeriSign.

Sheridan shares his take: ”When new TLDs first launched, the larger registrars had to dedicate themselves to just focusing on the integration of hundreds of new TLDs per quarter. I look at 2014 as a year basically focused on integrating as many of the new TLDs as possible so that 2015 and 2016 could be more focused on marketing and sales. What I see today is more focus by the larger registrars on marketing the new TLDs and raising their visibility to their existing customer base. Since new TLDs are typically priced higher than a ‘.com’ they give the advantage to the registrars of driving higher revenue sales and allowing them to capture more margin on each individual domain name sale as well.”

He continues: “I think the .web TLD has big potential. For starters, there is no consumer education hurdle here. I think people will just get it…so that is a major advantage. I think we will have to see how the future .web registry addresses two key areas: pricing and marketing.”

“In regards to pricing, the wholesale cost to registrars will be key to adoption by larger registrars and its inclusion in key hosting bundles managed by the larger registrars (which impacts distribution). In regards to marketing, there will need to be a big effort to raise awareness of .web globally. This will require the help of the larger registrars (marketing programs) but will also require the .web registry to be involved as well,” Sheridan says. “The manner in which the future .web registry address pricing and marketing could potentially dictate its success. The future delegation of .web to a registry provider represents the final batch of remaining new TLDs to go live. I think it is great to have a big TLD like .web being delegated toward the end of this long new TLD rollout. It generates more media attention to the overall program and re-ignites excitement around domains. So that is good thing on all levels.”

Source: TheWHIR

Share Tweet Share

THIS ENTRY WAS POSTED IN **INDUSTRY INSIGHTS & NEWS**. BOOKMARK THE **PERMALINK**.

← SERVERHUB BRINGS SIXTH GLOBAL LOCATION ONLINE IN NEW YORK

WOULD GOOGLE CLOUD WIN SPELL DOOM FOR MSPS? →

Search …

RECENT POSTS

3 big data platforms look beyond Hadoop

IDG Contributor Network: Data lakes: Just a swamp without data governance and catalog

How to get real value from big data in the cloud

What is Julia? A fresh approach to numerical computing

IDG Contributor Network: In an age of fake news, is there really such a thing as fake data?

ARCHIVES

July 2018

June 2018

EXHIBIT JMR-19

BRAND TLDS & DIGITAL STRATEGIES

.WEB Acquired for $135 Million. Too much? How does it compare?

At $135 million, .WEB is the highest valued first round new Top Level Domain registry sold at auction. It sets a new high bar on the value of TLDs. Nu Dot Co and its investors, prevailed in an ICANN auction and are now the proud owners of the .WEB Registry. Industry tea leaves point to Verisign as the backer but that has yet to be confirmed.

In the past two years, other TLD registries have sold for millions of dollars. Now that the big one (.WEB) is done, it is interesting to look at the relative value of these acquisitions and consider how these investments make sense for the buyers. The top 5 new TLD acquisition prices are listed below and a discussion follows.

TLD	VALUE (USD)	BUYER
.WEB	$135,000,000	Nu Dot Co
.SHOP	$41,500,000	GMO Registry, Inc.
.APP	$25,000,000	Charleston Road Registry Inc. (Google)
.BLOG (1)	$19,000,000	Automattic Inc. (Wordpress)
.TECH	$6,760,000	Dot Tech LLC (Radix)

SOURCE ~~HTTPS://GTLDRESULT.ICANN.ORG/APPLICATIONRESULT/APPLICATIONSTATUS/AUCTIONRESULTS~~
[1] **REPORTED BUT UNVERIFIED**

BLOG CATEGORIES

WATCH OUR WEBINAR ON

WHEN IT COMES TO YOUR DOMAINS AND DNS

WATCH NOW

RECENT POSTS

09/10/2018

05/15/2018

05/10/2018

WANT TO LEARN MORE ABOUT THIS TOPIC? GET IN TOUCH WITH US.

In March 2015, I wrote an article; Did Google Overpay for .APP? The conclusion was, "no they did not overpay". This was based on Google's leading mobile app market position and .APP would allow them to own a new channel, introduce a new paradigm on app discoverability, and leverage Google's Android market position in the application distribution market.

Then there was .SHOP, purchased for $41.5 million by GMO Registry. This one, I find to be a head scratcher in terms of the valuation. It is a good TLD, no question. It has clear meaning as an ecommerce destination but $41.5 million for a niche or single purpose TLD seems rich to me. .SHOP operators and investors will need to take a long view, dedicate significant marketing spend to develop a value proposition to deliver a new, better, and different offering to ecommerce merchants, and gain market traction. Did GMO overpay? Probably.

How about .BLOG, purchased for a reported $19 million by Automattic Inc., parent of WordPress? Wordpress is a leading website building and blogging software company. By various reports 25 – 27% of all websites use WordPress and millions of bloggers use their tools. WordPress is a big deal. There are parallels with .APP and .BLOG. Both were purchased by industry leaders in their respective lines of business. Each can use the TLD as a differentiator to leverage and extend their market position to drive growth. They can offer services that are unique in the market, increasing the value of their entire business. Secondly, as a defensive position, they ensure competitors are not armed with a powerful digital asset to disrupt their respective positions. .BLOG gets a thumbs up and in my view a good buy for Automattic. Not only will they sell millions of .BLOG domains, they will dramatically increase the worldwide awareness of new TLDs. That's a win for the industry as well.

Where .APP and .BLOG have explicit meanings and added power due to the market positions of the acquirers, .SHOP is seeking to carve a new extension as an ecommerce destination alternative. This all makes sense but $41.5 million is a big number to dig out of, from a return on investment perspective.

.WEB is a different animal. This acquisition valuation is proof. .WEB is what we call a "super generic" and arguably the best new TLD alternative to .COM. It is a word that is commonly used with intuitive meaning. WEB could make a serious dent to .COM over the long run. With an initial investment of $135 million you have to assume the owners will follow their acquisition capital with serious marketing spend. Domain speculation in the .WEB space will be furious at launch. Premium domain sales for .WEB are likely to be orders of magnitude larger than in any other TLD introduced and as the .WEB space matures, those premium values will rise. Of course, this assumes Nu Dot Co drives forward with the now familiar premium domain strategy.

$135 million is a shocking number. It can be a winner assuming funds to support a major marketing and communication plan as the best alternative to .COM, or if Verisign, a cozy super-generic companion to .COM. .CO positioned as a viable alternative and currently have under 2 million registrations versus .COM at 126 million. Recall, Neustar acquired .CO for $109 million on $21 million in revenue with approximately 1.5 million domains under management.

Let's assume Verisign is indeed the .WEB backer. Today, Verisign generates over $1 billion in revenue and a +60% operating profit. Nice business. The challenge for Verisign is not EBITDA or cash flow, it is growth. In their recent quarterly financial release, Verisign grew by 9% in the quarter compared to the same quarter in 2015. Not bad but not enough to excite and drive up shareholder value, where a single digit CAGR

Name
example@example
How Can We Help
Subm t

READ OUR
FOR REAL WORLD "BEFORE & AFTER" STORIES
READ MORE

and cash generation is already baked into their market cap. The company is trading at ±9 times revenue and ±15 times EBITDA. If they did indeed acquire .WEB, the company now owns a new growth engine and they are uniquely positioned to drive it. Some suggest they would bury it to protect .COM. That is not in the best interest of shareholders. .COM is still king, will be for some time and .WEB can immediately contribute healthy operating profits out of the gate. If well executed, .WEB can add significant shareholder value.

If the tea leaves are misleading and everybody is wrong about Verisign, then we will have to write another blog on those implications. If it is Neustar, for example, then the market dynamics are entirely different. We are also likely to see a gun fight on how this all materialized with the secret backer of Nu Dot Co.

THE ECONOMICS OF A TLD REGISTRY

Let's now assume it is not Verisign, the economics of a TLD registry are very good at scale from 1 million to 100 million Domains Under Management (DUM).

This chart models Domain Under Management (DUM), an assumed registry price of $8, the annual revenue, (ignoring one-time premium domain revenues) and assumed EBITDA improving from 10% to 50% as economies of scale kick in for a well run registry. Then apply business valuations at 5 times revenue (conservative low bar) or 20 times EBITDA, whichever you prefer.

DUM	1,000,000	2,000,000	5,000,000	10,000,000	100,000,000
Registry Price	$8.00	$8.00	$8.00	$8.00	$8.00
Revenue	$8,000,000	$16,000,000	$40,000,000	$80,000,000	$800,000,000
EBITDA	$800,000	$3,200,000	$12,000,000	$32,000,000	$400,000,000
Operating Margins	10%	20%	30%	40%	50%
Value @ 5x Revenue	$40,000,000	$80,000,000	$200,000,000	$400,000,000	$4,000,000,000
Value @ 20x Profit	$16,000,000	$64,000,000	$240,000,000	$640,000,000	$8,000,000,000

For comparison, Verisign with 126 million DUM, $1B in revenue, generates 60% in profit and a $9B Market Cap and .CO was acquired by Neustar for $109 with revenue at $21 million and 1.6 million DUM.

The trick of course is getting to scale, how much additional investment will be required to get to scale and will the market demand exist for .WEB. For the investors at Nu Dot Co, you now own a valuable asset that will take time and skilled execution to monetize. We will need a few years to determine if $135 million was too much, just right or a home run investment. The potential to create a highly valuable business that generates tremendous profit and cash is there if they drive to scale.

If it is Verisign, it is a brilliant move, not unlike .BLOG and .APP, it extends Verisign's .COM position and is the growth engine they need.

The new TLD market continues be increasingly dynamic and interesting with each passing day.

Thanks for checking in – Peter

SHARE THIS

twitterTWITTER linkedin-in LINKEDIN google-plus-gGOOGLE PLUS facebook-fFACEBOOK envelopeMAIL

EXHIBIT JMR-20

DOMAIN INCITE

Get a great domain at a great price .SK

DI PRO | TLD HEALTH CHECK | ABOUT | ADVERTISE

RSS Feed

Twitter Feed

Enter Search Query

Verisign likely $135 million winner of .web gTLD

Kevin Murphy, August 1, 2016, 08:51:12 (UTC), Domain Registries

Verisign has emerged as the likely winner of the .web gTLD auction, which closed on Thursday with a staggering $135 million winning bid.

The shell company Nu Dot Co LLC was the prevailing applicant in the auction, which ran for 23 rounds over two days.

Just hours after the auction closed, Domain Name Wire scooped that Verisign had quietly informed investors that it has committed to pay $130 million for undisclosed "contractual rights".

In its Securities and Exchange Commission quarterly report, filed after the markets closed on Thursday, Verisign said:

> Subsequent to June 30, 2016, the Company incurred a commitment to pay approximately $130.0 million for the future assignment of contractual rights, which are subject to third-party consent. The payment is expected to occur during the third quarter of 2016.

There seems to be little doubt that the payment is to be made to NDC (or one of its shell company parents) in exchange for control of the .web Registry Agreement.

The "third-party consent" is likely a reference to ICANN, which must approve RA reassignments.

We speculated on July 14 that Verisign would turn out to be NDC's secret sugar daddy, which seems to have been correct.

Rival .web applicant Donuts had sued ICANN for an emergency temporary restraining order, claiming it had not done enough to uncover the identity of NDC's true backers, but was rebuffed on multiple grounds by a California judge.

Donuts, and other applicants, had wanted the contention set settled privately, but NDC was the only hold-out.

Had it been settled with a private auction, and the $135 million price tag had been reached, each of the seven losing applicants would have walked away with somewhere in the region of $18.5 million in their pockets.

This draws the battle lines for some potentially interesting legal fallout.

It remains to be seen if Donuts will drop its suit against ICANN or instead add Verisign in as a defendant with new allegations.

There's also the possibility of action from Neustar, which is currently NDC's named back-end provider.

Assuming Verisign plans to switch .web to its own back-end, Neustar may be able to make similar claims to those leveled by Verisign against XYZ.com.

Overall, Verisign controlling .web is sad news for the new gTLD

RECENT POSTS

Afilias gets Guinness record for .au migration

KSK vote was NOT unanimous

ICANN turns 20 today (or maybe not)

Van der Laan to leave ICANN board

Set buttocks to clench! ICANN approves risky KSK rollover

Mediators hired as Whois reformers butt heads

US scraps fucking stupid "seven dirty words" ban

Beginning of the end for DomainTools? Court orders it to scrub Whois records

stop stressing about volume
.CLUB sees spam double after China promotion
Com Laude acquires Scottish rival
CentralNic acquired yet another company
Empty Whois a threat to the US elections?
Donuts gets bought by former ICANN CEO's firm
.tel's second-biggest registrar gets canned
Whois privacy did NOT increase spam volumes
Afilias finally admits it's American
Could a new US law make GDPR irrelevant?
No more free ride for ICANN Fellows?
Afilias sues India to block $12 million Neustar back-end deal
More consolidation? Endurance said to be up for sale
ICANN faces critical choice as security experts warn against key rollover
.CLUB revenue not all that
Microsoft seizes "Russian election hacking" domains
New gTLDs rebound in Q2
.CLUB revenue reportedly $7.2 million
How a single Whois complaint got this registrar shitcanned
38th dot-brand bows out after acquisition
ICANN CTO: no reason to delay KSK rollover
DomainTools tracks its one billionth domain
ICANN closes GoDaddy Whois probe
Allstate dumps a dot-brand
I was wrong, Famous Four bosses WERE kicked out
No Verfügungsanspruch for ICANN in GDPR lawsuit
Famous Four is DEAD! New registry promises spam crackdown
auDA car crash continues as director quits over foreign members
New ICANN director named
My brain explodes trying to understand MMX's new blockchain deal for .luxe
Fight over Whois access starts early
Blacknight calls for Ireland to slash domain prices
Chaotic scenes as 'Grumpies' lose auDA board fight
These 33 people will decide the future of Whois
Wix.com obtains ICANN accreditation — bad news for Web.com?
Two companies "capture" auDA
Facebook clashes with registrars after massive

industry, in my view.

.web has been seen, over the years, as the string that is both most sufficiently generic, sufficiently catchy, sufficiently short and of sufficient semantic value to provide a real challenge to .com.

I've cooled on .web since I launched DI six years ago. Knowing what we now know about how many new gTLD domains actually sell, and how they have to be priced to achieve volume, I was unable to see how even a valuation of $50 million was anything other than a long-term (five years or more) ROI play.

Evidently, most of the applicants agreed. According to ICANN's log of the auction (pdf) only two applicants — NDC and another (Google?) — submitted bids in excess of $57.5 million.

But for Verisign, .web would have been a risk in somebody else's hands.

I don't think the company cares about making .web a profitable TLD, it instead is chiefly concerned with being able to control the impact it has on .com's mind-share monopoly.

Verisign makes about a billion dollars a year in revenue, with analyst-baffling operating margins around 60%, and that's largely because it runs .com.

In 2015, its cash flow was $651 million.

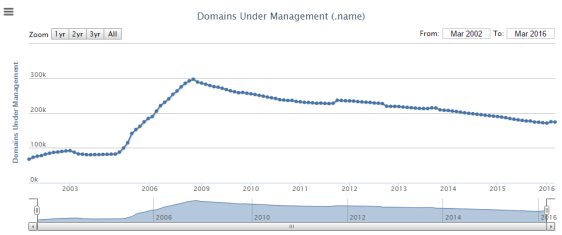
So Verisign has dropped a couple of months' cash to secure .web — chickenfeed if the real goal is .com's continued hegemony.

In the hands of a rival new gTLD company's marketing machine, in six months we might have been seeing (naive) headlines along the lines of "Forget .com, .web is here!".

That won't happen now.

I'm not privy to Verisign's plans for .web, but its track record supporting the other TLDs it owns is not fantastic.

Did you know, or do you remember, that Verisign runs .name? I sometimes forget that too. It bought it from Global Name Registry in late 2008, at the high point of its domains under management in this chart.



I don't think I expect Verisign to completely bury .web, but I don't think we're going to see it aggressively promoted either.

It will never be positioned as a competitor to .com.

If .web never makes $135 million, that would be fine. Just as long as it doesn't challenge the perception that you need a .com to be successful, Verisign's purchase was worth the money.

EXHIBIT JMR-21

JMR-21

Technology

How a $135 million auction affects the domain name industry and your business

The cost of protecting assets and creating a new revenue stream

By Cybele Negris | August 10, 2016, 11:24am

niroworld/Shutterstock

On July 27, the Internet Corporation for Assigned Names and Numbers (ICANN) ran an auction for the generic top-level domain (gTLD) .web that culminated in a winning bid of $135 million. Nu Dot Co LLC produced the winning bid and on August 1, Verisign, a global leader in domain names and

internet security, confirmed in a #4f81bd;">press release that they provided the necessary funds for Nu Dot Co's successful bid. But wait one second, let's back this up - $135 million for .web?

The previous highest public price for a gTLD happened just over seven months ago when GMO Registry of Japan acquired the .shop gTLD for $41.5 million. While not a number to sneeze at, Verisign blew away the previous record high. And while we're making comparisons, remember that $100 million venture capital investment in Shopify back in 2013? Shopify is now a public company and an absolute force in the e-commerce game while its value is soaring past a billion dollars.

So that brings us back to Verisign and their brand new $135-million baby. What exactly are Verisigns plans for .web? To turn the new investment into a billion-dollar web sensation? According to their press release, "as the most experienced and reliable registry operator, Verisign is well-positioned to widely distribute .web." They plan on utilizing their "expertise, infrastructure, and partner relationships to quickly grow .web and establish it as an additional option for registrants worldwide." This can certainly hold true as .web is widely considered the gTLD with the most potential out of 1,930 applications for new domain extensions ICANN received to battle .com and .net for widespread adoption.

In the past 30 years, Verisign has registered over 127 million .com domain names and nearly 16 million .net domain names. These are two of the most popular top-level domains available while the most adopted new gTLD, .xyz, has garnered over six million registrations since entering the market a little over two years ago. If Verisign is able to average three million .web registrations year-over-year, like .xyz, at a guesstimated price of $10 USD, with an annual renewal rate of 50%, they would break even on their investment in about 3 years ($30,000,000 in year one, $45,000,000 in year two and $52,500,000 in year three). Of course, if renewal rates are lower or Versign cannot achieve three million domains a year, it will take longer to reach break-even.

The runner-up in the .web auction, potentially a giant with immense resources such as Google, could eat into Verisign's top-level domain

market share, taking aim at its .com and .net properties. Let's say Verisign bowed out of the auction early and allowed another registry to directly compete against .net with a synonymous .web domain name. With a stagnating stock price, Verisign would not be in a fantastic position to improve on that with a strong competitor nipping at its heels. From this perspective, the cost of doing business for Verisign is more than worthwhile, even if they happen to not generate a single dollar of revenue from .web for years to come.

What does this all mean for your business and web presence?

.Web will not be publicly available for some time; and while Verisign may or may not have acquired the gTLD mainly to keep competitors away, most pundits believe that they will make it publicly available. Once released, it would be prudent for all businesses that already own a .com and/or .net to register the .web variation for their business to avoid resellers from scooping them up and charging a premium.

Be sure to #4f81bd;">pre-register for .web domain names as soon as you can so that you are alerted as soon as .web launches and becomes publicly available.

If you are a trademark owner, be sure to register with the #4f81bd;">Trademark Clearinghouse in advance to ensure that yourtrademark.web can be secured during the "#4f81bd;">sunrise period." This stretch of time is designed specifically for trademark holders to reserve their domain names before anyone else has access.

Perhaps you missed out on the .com or .net variation of your business; now you have an excellent opportunity to grab the .web version of your domain name and once you register the domain, a simple 301 redirect from your existing domain to the .web variation will provide a seamless transition to your ideal domain name.

Put your thinking cap on and begin generating lists of relevant generic domain names for your industry that will not infringe on another businesses' trademarks. Once .web launches, consider registering these domain names under the .web gTLD. These could be incredibly useful as landing pages for search engine marketing tactics or as a new revenue

stream for your business as others may start knocking on your door looking to take these domain names off your hands for a price.

If you have a .com or .net domain name, keep a close eye on the costs of these as Verisign might be looking to boost their margins on these assets. While #4f81bd;">Verisign cannot increase their price for .com under their current contract with ICANN which ends in 2018, they are able to increase the price of .net by 10% every year until the end of that agreement in 2017.

Cybele Negris (Contact Information Redacted is president, CEO and co-founder of Webnames.ca, Canada's original .CA registrar. She serves on the boards of Small Business BC, Small Business Roundtable of BC, Capilano University and the Capilano University Foundation.

0 Comments Business in Vancouver Login
Recommend Share Sort by Newest
Start the discussion…
LOG IN WITH
OR SIGN UP WITH DISQUS
Name
Be the first to comment.
Subscribe Add Disqus to your siteAdd DisqusAdd

EXHIBIT JMR-22

JMR-22

THIS WEEK IN SEO 60

BRANDS, DOMAINS, AND YOUTUBE

THE DEATH OF GENERICS AND THE DOMINANCE OF BRANDS

http://www.seobook.com/brands-beat-generics

Aaron Wall, the Cormac McCarthy of SEO (google it), published a great post looking at how generic domains like cooking.com and drugstore.com have failed to thrive, but the big brands behind them (Target and Walgreens, respectively) are doing just fine.

> *If you invest in zero-sum markets there needs to be some point of differentiation to drive switching. There might be opportunity for a cooking.com or a drugstore.com targeting emerging and frontier markets where brands are under-represented online (much like launching Drugstore.com in the US back in 1999), but it is unlikely pure-play ecommerce sites will be able to win in established markets if they use generically descriptive domains which make building brand awareness and perceived differentiation next to impossible.*

Digging in to how brands succeed/fail in SEO (and business in general) is one of the topics that hasn't yet been beaten to death by the SEO conference-circuit (R.I.P., my interest in reading about content marketing).

I enjoyed this article, definitely give it a read.

THE NEXT BIG DOMAIN EXTENSION

http://domainnamewire.com/2016/07/29/verisign-paid-135-million-web-top-level-domain/

Learn How To Rank Your Site

Speaking of domain names...

Verisign, the juggernaut of a company behind .com/.net (a.k.a.the big 3) just paid $135,000,000 to acquire the .web extension.

You've seen these new extensions over the last few years–.ninja, .rent, .guru (side note: still waiting for http://seo.guru to be developed...).

Some of these new extensions are kind of garbage, like .FYI, but .web makes sense to a lot of people, and is poised to be one of the most popular new extensions.

Here's why Verisign paid 3x as much as any other new gTLD for .web:

> ***It views it as competitive to .com*** *– a handful of industry watchers and top level domain name companies have said that .web is the one domain that could unseat .com. While that's open to debate, Verisign might have viewed this as an opportunity to take the greatest threat from the new TLD program off the table.*
>
> ***It views it as competitive of .net*** *– this might sound odd, but keep in mind .net is a 9-figure-a-year business*

EXHIBIT JMR-23

Search ICANN.org

ICANN

Resources

BYLAWS FOR INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS | A California Nonprofit Public-Benefit Corporation

As amended 18 June 2018

ANNEX G-1

ANNEX G-2

ARTICLE 1 MISSION, COMMITMENTS AND CORE VALUES

Section 1.1. MISSION

(a) The mission of the Internet Corporation for Assigned Names and Numbers ("**ICANN**") is to ensure the stable and secure operation of the Internet's unique identifier systems as described in this Section 1.1(a) (the "**Mission**"). Specifically, ICANN:

(i) Coordinates the allocation and assignment of names in the root zone of the Domain Name System ("**DNS**") and coordinates the development and implementation of policies concerning the registration of second-level domain names in generic top-level domains ("**gTLDs**"). In this role, ICANN's scope is to coordinate the development and implementation of policies:

- For which uniform or coordinated resolution is reasonably necessary to facilitate the openness, interoperability, resilience, security and/or stability of the DNS including, with respect to gTLD registrars and registries, policies in the areas described in Annex G-1 and Annex G-2; and
- That are developed through a bottom-up consensus-based multistakeholder process and designed to ensure the stable and secure operation of the Internet's unique names systems.

The issues, policies, procedures, and principles addressed in Annex G-1 and Annex G-2 with respect to gTLD registrars and registries shall be deemed to be within ICANN's Mission.

(ii) Facilitates the coordination of the operation and evolution of the DNS root name server system.

(iii) Coordinates the allocation and assignment at the top-most level of Internet Protocol numbers and Autonomous System numbers. In service of its Mission, ICANN (A) provides registration services and open access for global number registries as requested by the Internet Engineering Task Force ("**IETF**") and the Regional Internet Registries ("**RIRs**") and (B) facilitates the development of global number registry policies by the affected community and other related tasks as agreed with the RIRs.

(iv) Collaborates with other bodies as appropriate to provide registries needed for the functioning of the Internet as specified by Internet protocol standards development organizations. In service of its Mission, ICANN's scope is to provide registration services and open access for registries in the public domain requested by Internet protocol development organizations.

(b) ICANN shall not act outside its Mission.

(c) ICANN shall not regulate (i.e., impose rules and restrictions on) services that use the Internet's unique identifiers or the content that such services carry or provide, outside the express scope of Section 1.1(a). For the avoidance of doubt, ICANN does not hold any governmentally authorized regulatory authority.

(d) For the avoidance of doubt and notwithstanding the foregoing:

(i) the foregoing prohibitions are not intended to limit ICANN's authority or ability to adopt or implement policies or procedures that take into account the use of domain names as natural-language identifiers;

(ii) Notwithstanding any provision of the Bylaws to the contrary, the terms and conditions of the documents listed in subsections (A) through (C) below, and ICANN's performance of its obligations or duties thereunder, may not be challenged by any party in any proceeding against, or process involving, ICANN (including a request for reconsideration or an independent review process pursuant to Article 4) on the basis that such terms and conditions conflict with, or are in violation of, ICANN's Mission or otherwise exceed the scope of ICANN's authority or powers pursuant to these Bylaws ("**Bylaws**") or ICANN's Articles of Incorporation ("**Articles of Incorporation**"):

(A)

(1) all registry agreements and registrar accreditation agreements between ICANN and registry operators or registrars in force on 1 October 2016 [1], including, in each case, any terms or conditions therein that are not contained in the underlying form of registry agreement and registrar accreditation agreement;

> (2) any registry agreement or registrar accreditation agreement not encompassed by (1) above to the extent its terms do not vary materially from the form of registry agreement or registrar accreditation agreement that existed on 1 October 2016;

(B)any renewals of agreements described in subsection (A) pursuant to their terms and conditions for renewal; and

(C)ICANN's Five-Year Strategic Plan and Five-Year Operating Plan existing on 10 March 2016.

(iii) Section 1.1(d)(ii) does not limit the ability of a party to any agreement described therein to challenge any provision of such agreement on any other basis, including the other party's interpretation of the provision, in any proceeding or process involving ICANN.

(iv) ICANN shall have the ability to negotiate, enter into and enforce agreements, including public interest commitments, with any party in service of its Mission.

Section 1.2. COMMITMENTS AND CORE VALUES

In performing its Mission, ICANN will act in a manner that complies with and reflects ICANN's Commitments and respects ICANN's Core Values, each as described below.

(a) **COMMITMENTS**

In performing its Mission, ICANN must operate in a manner consistent with these Bylaws for the benefit of the Internet community as a whole, carrying out its activities in conformity with relevant principles of international law and international conventions and applicable local law, through open and transparent processes that enable competition and open entry in Internet-related markets. Specifically, ICANN commits to do the following (each, a "**Commitment**," and collectively, the "**Commitments**"):

> (i) Preserve and enhance the administration of the DNS and the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet;

(ii) Maintain the capacity and ability to coordinate the DNS at the overall level and work for the maintenance of a single, interoperable Internet;

(iii) Respect the creativity, innovation, and flow of information made possible by the Internet by limiting ICANN's activities to matters that are within ICANN's Mission and require or significantly benefit from global coordination;

(iv) Employ open, transparent and bottom-up, multistakeholder policy development processes that are led by the private sector (including business stakeholders, civil society, the technical community, academia, and end users), while duly taking into account the public policy advice of governments and public authorities. These processes shall (A) seek input from the public, for whose benefit ICANN in all events shall act, (B) promote well-informed decisions based on expert advice, and (C) ensure that those entities most affected can assist in the policy development process;

(v) Make decisions by applying documented policies consistently, neutrally, objectively, and fairly, without singling out any particular party for discriminatory treatment (i.e., making an unjustified prejudicial distinction between or among different parties); and

(vi) Remain accountable to the Internet community through mechanisms defined in these Bylaws that enhance ICANN's effectiveness.

(b) **CORE VALUES**

In performing its Mission, the following "**Core Values**" should also guide the decisions and actions of ICANN:

(i) To the extent feasible and appropriate, delegating coordination functions to or recognizing the policy role of, other responsible entities that reflect the interests of affected parties and the roles of bodies internal to ICANN and relevant external expert bodies;

(ii) Seeking and supporting broad, informed participation reflecting the functional, geographic, and cultural diversity of the Internet at all levels of policy development and decision-making to ensure that the bottom-up, multistakeholder policy development process is used to ascertain the global public interest and that those processes are accountable and transparent;

(iii) Where feasible and appropriate, depending on market mechanisms to

promote and sustain a competitive environment in the DNS market;

(iv) Introducing and promoting competition in the registration of domain names where practicable and beneficial to the public interest as identified through the bottom-up, multistakeholder policy development process;

(v) Operating with efficiency and excellence, in a fiscally responsible and accountable manner and, where practicable and not inconsistent with ICANN's other obligations under these Bylaws, at a speed that is responsive to the needs of the global Internet community;

(vi) While remaining rooted in the private sector (including business stakeholders, civil society, the technical community, academia, and end users), recognizing that governments and public authorities are responsible for public policy and duly taking into account the public policy advice of governments and public authorities;

(vii) Striving to achieve a reasonable balance between the interests of different stakeholders, while also avoiding capture; and

(viii) Subject to the limitations set forth in Section 27.2, within the scope of its Mission and other Core Values, respecting internationally recognized human rights as required by applicable law. This Core Value does not create, and shall not be interpreted to create, any obligation on ICANN outside its Mission, or beyond obligations found in applicable law. This Core Value does not obligate ICANN to enforce its human rights obligations, or the human rights obligations of other parties, against other parties.

(c) The Commitments and Core Values are intended to apply in the broadest possible range of circumstances. The Commitments reflect ICANN's fundamental compact with the global Internet community and are intended to apply consistently and comprehensively to ICANN's activities. The specific way in which Core Values are applied, individually and collectively, to any given situation may depend on many factors that cannot be fully anticipated or enumerated. Situations may arise in which perfect fidelity to all Core Values simultaneously is not possible. Accordingly, in any situation where one Core Value must be balanced with another, potentially competing Core Value, the result of the balancing must serve a policy developed through the bottom-up multistakeholder process or otherwise best serve ICANN's Mission.

ARTICLE 2 POWERS

Section 2.1. GENERAL POWERS

Except as otherwise provided in the Articles of Incorporation or these Bylaws, the powers of ICANN shall be exercised by, and its property controlled and its business and affairs conducted by or under the direction of, the Board (as defined in Section 7.1). With respect to any matters that would fall within the provisions of Section 3.6(a)-(c), the Board may act only by a majority vote of all Directors. In all other matters, except as otherwise provided in these Bylaws or by law, the Board may act by majority vote of the Directors present at any annual, regular, or special meeting of the Board. Any references in these Bylaws to a vote of the Board shall mean the vote of only those Directors present at the meeting where a quorum is present unless otherwise specifically provided in these Bylaws by reference to "of all Directors."

Section 2.2. RESTRICTIONS

ICANN shall not act as a Domain Name System Registry or Registrar or Internet Protocol Address Registry in competition with entities affected by the policies of ICANN. Nothing in this Section 2.2 is intended to prevent ICANN from taking whatever steps are necessary to protect the operational stability of the Internet in the event of financial failure of a Registry or Registrar or other emergency.

Section 2.3. NON-DISCRIMINATORY TREATMENT

ICANN shall not apply its standards, policies, procedures, or practices inequitably or single out any particular party for disparate treatment unless justified by substantial and reasonable cause, such as the promotion of effective competition.

ARTICLE 3 TRANSPARENCY

Section 3.1. OPEN AND TRANSPARENT

ICANN and its constituent bodies shall operate to the maximum extent feasible in an open and transparent manner and consistent with procedures designed to ensure fairness, including implementing procedures to (a) provide advance notice to facilitate stakeholder engagement in policy development decision-making and cross-community deliberations, (b) maintain responsive consultation procedures that provide detailed explanations of the basis for decisions (including how comments have influenced the development of policy considerations), and (c) encourage fact-based policy development work. ICANN shall also implement procedures for the documentation and public disclosure of the rationale for decisions made by the Board and ICANN's constituent bodies (including the detailed explanations discussed above).

Section 3.2. WEBSITE

ICANN shall maintain a publicly-accessible Internet World Wide Web site (the "**Website**"), which may include, among other things, (a) a calendar of scheduled meetings of the Board, the EC (as defined in Section 6.1(a)), Supporting Organizations (as defined in Section 11.1), and Advisory Committees (as defined in Section 12.1); (b) a docket of all pending policy development matters, including their schedule and current status; (c) specific meeting notices and agendas as described below; (d) information on the ICANN Budget (as defined in Section 22.4(a)(i)), the IANA Budget (as defined in Section 22.4(b)(i)), annual audit, financial contributors and the amount of their contributions, and related matters; (e) information about the availability of accountability mechanisms, including reconsideration, independent review, and Ombudsman activities, as well as information about the outcome of specific requests and complaints invoking these mechanisms; (f) announcements about ICANN activities of interest to significant segments of the ICANN community; (g) comments received from the community on policies being developed and other matters; (h) information about ICANN's physical meetings and public forums; and (i) other information of interest to the ICANN community.

Section 3.3. MANAGER OF PUBLIC PARTICIPATION

There shall be a staff position designated as Manager of Public Participation, or such other title as shall be determined by the President, that shall be responsible, under the direction of the President, for coordinating the various aspects of public participation in ICANN, including the Website and various other means of communicating with and receiving input from the general community of Internet users.

Section 3.4. MEETING NOTICES AND AGENDAS

At least seven days in advance of each Board meeting (or if not practicable, as far in advance as is practicable), a notice of such meeting and, to the extent known, an agenda for the meeting shall be posted.

Section 3.5. MINUTES AND PRELIMINARY REPORTS

a. All minutes of meetings of the Board, the Advisory Committees and Supporting Organizations (and any councils thereof) shall be approved promptly by the originating body and provided to the ICANN Secretary ("**Secretary**") for posting on the Website. All proceedings of the EC Administration (as defined in Section 6.3) and the EC shall be provided to the Secretary for posting on the Website.

b. No later than 11:59 p.m. on the second business day after the conclusion of each meeting (as calculated by local time at the location of ICANN's principal office), any resolutions passed by the Board at that meeting shall be made publicly available on the Website; provided, however, that any actions relating to personnel or employment matters, legal matters (to the extent the Board determines it is necessary or appropriate to protect the interests of ICANN), matters that ICANN is prohibited by law or contract from disclosing publicly, and other matters that the Board determines, by a three-quarters (3/4) vote of Directors present at the meeting and voting, are not appropriate for public distribution, shall not be included in the resolutions made publicly available. The Secretary shall send notice to the Board and the Chairs of the Supporting Organizations (as set forth in Article 9 through Article 11) and Advisory Committees (as set forth in Article 12) informing them that the resolutions have been posted.

c. No later than 11:59 p.m. on the seventh business days after the conclusion of each meeting (as calculated by local time at the location of ICANN's principal office), any actions taken by the Board shall be made publicly available in a preliminary report on the Website, subject to the limitations on disclosure set forth in Section 3.5(b) above. For any matters that the Board determines not to disclose, the Board shall describe in general terms in the relevant preliminary report the reason for such nondisclosure.

d. No later than the day after the date on which they are formally approved by the Board (or, if such day is not a business day, as calculated by local time at the location of ICANN's principal office, then the next immediately following business day), the minutes of the Board shall be made publicly available on the Website; provided, however, that any minutes of the Board relating to personnel or employment matters, legal matters (to the extent the Board determines it is necessary or appropriate to protect the interests of ICANN), matters that ICANN is prohibited by law or contract from disclosing publicly, and other matters that the Board determines, by a three-quarters (3/4) vote of Directors present at the meeting and voting, are not appropriate for public distribution, shall not be included in the minutes made publicly available. For any matters that the Board determines not to disclose, the Board shall describe in general terms in the relevant minutes the reason for such nondisclosure.

Section 3.6. NOTICE AND COMMENT ON POLICY ACTIONS

(a) With respect to any policies that are being considered by the Board for adoption that substantially affect the operation of the Internet or third parties, including the imposition of any fees or charges, ICANN shall:

(i) provide public notice on the Website explaining what policies are being considered for adoption and why, at least twenty-one days (and if practical, earlier) prior to any action by the Board;

(ii) provide a reasonable opportunity for parties to comment on the adoption of the proposed policies, to see the comments of others, and to reply to those comments (such comment period to be aligned with ICANN's public comment practices), prior to any action by the Board; and

(iii) in those cases where the policy action affects public policy concerns, to request the opinion of the Governmental Advisory Committee ("**GAC**" or "**Governmental Advisory Committee**") and take duly into account any advice timely presented by the Governmental Advisory Committee on its own initiative or at the Board's request.

(b) Where both practically feasible and consistent with the relevant policy development process, an in-person public forum shall also be held for discussion of any proposed policies as described in Section 3.6(a)(ii), prior to any final Board action.

(c) After taking action on any policy subject to this Section 3.6, the Board shall publish in the meeting minutes the rationale for any resolution adopted by the Board (including the possible material effects, if any, of its decision on the global public interest, including a discussion of the material impacts to the security, stability and resiliency of the DNS, financial impacts or other issues that were considered by the Board in approving such resolutions), the vote of each Director voting on the resolution, and the separate statement of any Director desiring publication of such a statement.

(d) Where a Board resolution is consistent with GAC Consensus Advice (as defined in Section 12.2(a)(x)), the Board shall make a determination whether the GAC Consensus Advice was a material factor in the Board's adoption of such resolution, in which case the Board shall so indicate in such resolution approving the decision (a "**GAC Consensus Board Resolution**") and shall cite the applicable GAC Consensus Advice. To the extent practical, the Board shall ensure that GAC Consensus Board Resolutions only relate to the matters that were the subject of the applicable GAC Consensus Advice and not matters unrelated to the applicable GAC Consensus Advice. For the avoidance of doubt: (i) a GAC Consensus Board Resolution shall not have the effect of making any other Board resolutions in the same set or series so designated, unless other resolutions are

specifically identified as such by the Board; and (ii) a Board resolution approving an action consistent with GAC Consensus Advice received during a standard engagement process in which input from all Supporting Organizations and Advisory Committees has been requested shall not be considered a GAC Consensus Board Resolution based solely on that input, unless the GAC Consensus Advice was a material factor in the Board's adoption of such resolution.

(e) GAC Carve-out

(i) Where a Board resolution is consistent with GAC Consensus Advice and the Board has determined that the GAC Consensus Advice was a material factor in the Board's adoption of such resolution as described in the relevant GAC Consensus Board Resolution, the Governmental Advisory Committee shall not participate as a decision-maker in the EC's exercise of its right to challenge the Board's implementation of such GAC Consensus Advice. In such cases, the Governmental Advisory Committee may participate in the EC in an advisory capacity only with respect to the applicable processes described in Annex D, but its views will not count as support or an objection for purposes of the thresholds needed to convene a community forum or exercise any right of the EC ("**GAC Carve-out**"). In the case of a Board Recall Process (as defined in Section 3.3 of Annex D), the GAC Carve-out shall only apply if an IRP Panel has found that, in implementing GAC Consensus Advice, the Board acted inconsistently with the Articles of Incorporation or these Bylaws.

(ii) When the GAC Carve-out applies (A) any petition notice provided in accordance with Annex D or Approval Action Board Notice (as defined in Section 1.2 of Annex D) shall include a statement that cites the specific GAC Consensus Board Resolution and the line item or provision that implements such specific GAC Consensus Board Resolution ("**GAC Consensus Statement**"), (B) the Governmental Advisory Committee shall not be eligible to support or object to any petition pursuant to Annex D or Approval Action (as defined in Section 1.1 of Annex D), and (C) any EC Decision (as defined in Section 4.1(a) of Annex D) that requires the support of four or more Decisional Participants (as defined in Section 6.1(a)) pursuant to Annex D shall instead require the support of three or more Decisional Participants with no more than one Decisional Participant objecting.

(iii) For the avoidance of doubt, the GAC Carve-out shall not apply to the exercise of the EC's rights where a material factor in the Board's decision

> was advice of the Governmental Advisory Committee that was not GAC Consensus Advice.

Section 3.7. TRANSLATION OF DOCUMENTS

As appropriate and to the extent provided in the ICANN Budget, ICANN shall facilitate the translation of final published documents into various appropriate languages.

ARTICLE 4 ACCOUNTABILITY AND REVIEW

Section 4.1. PURPOSE

In carrying out its Mission, ICANN shall be accountable to the community for operating in accordance with the Articles of Incorporation and these Bylaws, including the Mission set forth in Article 1 of these Bylaws. This Article 4 creates reconsideration and independent review processes for certain actions as set forth in these Bylaws and procedures for periodic review of ICANN's structure and operations, which are intended to reinforce the various accountability mechanisms otherwise set forth in these Bylaws, including the transparency provisions of Article 3 and the Board and other selection mechanisms set forth throughout these Bylaws.

Section 4.2. RECONSIDERATION

(a) ICANN shall have in place a process by which any person or entity materially affected by an action or inaction of the ICANN Board or Staff may request ("**Requestor**") the review or reconsideration of that action or inaction by the Board. For purposes of these Bylaws, "**Staff**" includes employees and individual long-term paid contractors serving in locations where ICANN does not have the mechanisms to employ such contractors directly.

(b) The EC may file a Reconsideration Request (as defined in Section 4.2(c)) if approved pursuant to Section 4.3 of Annex D ("**Community Reconsideration Request**") and if the matter relates to the exercise of the powers and rights of the EC of these Bylaws. The EC Administration shall act as the Requestor for such a Community Reconsideration Request and shall act on behalf of the EC for such Community Reconsideration Request as directed by the Decisional Participants, as further described in Section 4.3 of Annex D.

(c) A Requestor may submit a request for reconsideration or review of an ICANN action or inaction ("**Reconsideration Request**") to the extent that the Requestor

has been adversely affected by:

> (i) One or more Board or Staff actions or inactions that contradict ICANN's Mission, Commitments, Core Values and/or established ICANN policy(ies);
>
> (ii) One or more actions or inactions of the Board or Staff that have been taken or refused to be taken without consideration of material information, except where the Requestor could have submitted, but did not submit, the information for the Board's or Staff's consideration at the time of action or refusal to act; or
>
> (iii) One or more actions or inactions of the Board or Staff that are taken as a result of the Board's or staff's reliance on false or inaccurate relevant information.

(d) Notwithstanding any other provision in this Section 4.2, the scope of reconsideration shall exclude the following:

> (i) Disputes relating to country code top-level domain ("**ccTLD**") delegations and re-delegations;
>
> (ii) Disputes relating to Internet numbering resources; and
>
> (iii) Disputes relating to protocol parameters.

(e) The Board has designated the Board Accountability Mechanisms Committee to review and consider Reconsideration Requests. The Board Accountability Mechanisms Committee shall have the authority to:

> (i) Evaluate Reconsideration Requests;
>
> (ii) Summarily dismiss insufficient or frivolous Reconsideration Requests;
>
> (iii) Evaluate Reconsideration Requests for urgent consideration;
>
> (iv) Conduct whatever factual investigation is deemed appropriate;
>
> (v) Request additional written submissions from the affected party, or from

other parties; and

(vi) Make a recommendation to the Board on the merits of the Reconsideration Request, if it has not been summarily dismissed.

(f) ICANN shall absorb the normal administrative costs of the Reconsideration Request process. Except with respect to a Community Reconsideration Request, ICANN reserves the right to recover from a party requesting review or reconsideration any costs that are deemed to be extraordinary in nature. When such extraordinary costs can be foreseen, that fact and the reasons why such costs are necessary and appropriate to evaluating the Reconsideration Request shall be communicated to the Requestor, who shall then have the option of withdrawing the request or agreeing to bear such costs.

(g) All Reconsideration Requests must be submitted by the Requestor to an email address designated by the Board Accountability Mechanisms Committee:

(i) For Reconsideration Requests that are not Community Reconsideration Requests, such Reconsideration Requests must be submitted:

(A)for requests challenging Board actions, within 30 days after the date on which information about the challenged Board action is first published in a resolution, unless the posting of the resolution is not accompanied by a rationale. In that instance, the request must be submitted within 30 days from the initial posting of the rationale;

(B)for requests challenging Staff actions, within 30 days after the date on which the Requestor became aware of, or reasonably should have become aware of, the challenged Staff action; or

(C)for requests challenging either Board or Staff inaction, within 30 days after the date on which the Requestor reasonably concluded, or reasonably should have concluded, that action would not be taken in a timely manner.

(ii) For Community Reconsideration Requests, such Community Reconsideration Requests must be submitted in accordance with the timeframe set forth in Section 4.3 of Annex D.

(h) To properly initiate a Reconsideration Request, all Requestors must review, complete and follow the Reconsideration Request form posted on the Website at

https://www.icann.org/resources/pages/accountability/reconsideration-en. Requestors must also acknowledge and agree to the terms and conditions set forth in the form when filing.

(i) Requestors shall not provide more than 25 pages (double-spaced, 12-point font) of argument in support of a Reconsideration Request, not including exhibits. Requestors may submit all documentary evidence necessary to demonstrate why the action or inaction should be reconsidered, without limitation.

(j) Reconsideration Requests from different Requestors may be considered in the same proceeding so long as: (i) the requests involve the same general action or inaction; and (ii) the Requestors are similarly affected by such action or inaction. In addition, consolidated filings may be appropriate if the alleged causal connection and the resulting harm is substantially the same for all of the Requestors. Every Requestor must be able to demonstrate that it has been materially harmed and adversely impacted by the action or inaction giving rise to the request.

(k) The Board Accountability Mechanisms Committee shall review each Reconsideration Request upon its receipt to determine if it is sufficiently stated. The Board Accountability Mechanisms Committee may summarily dismiss a Reconsideration Request if: (i) the Requestor fails to meet the requirements for bringing a Reconsideration Request; or (ii) it is frivolous. The Board Accountability Mechanisms Committee's summary dismissal of a Reconsideration Request shall be documented and promptly posted on the Website.

(l) For all Reconsideration Requests that are not summarily dismissed, except Reconsideration Requests described in Section 4.2(l)(iii) and Community Reconsideration Requests, the Reconsideration Request shall be sent to the Ombudsman, who shall promptly proceed to review and consider the Reconsideration Request.

> (i) The Ombudsman shall be entitled to seek any outside expert assistance as the Ombudsman deems reasonably necessary to perform this task to the extent it is within the budget allocated to this task.
>
> (ii) The Ombudsman shall submit to the Board Accountability Mechanisms Committee his or her substantive evaluation of the Reconsideration Request within 15 days of the Ombudsman's receipt of the Reconsideration Request. The Board Accountability Mechanisms Committee shall thereafter promptly proceed to review and consideration.
>
> (iii) For those Reconsideration Requests involving matters for which the

> Ombudsman has, in advance of the filing of the Reconsideration Request, taken a position while performing his or her role as the Ombudsman pursuant to Article 5 of these Bylaws, or involving the Ombudsman's conduct in some way, the Ombudsman shall recuse himself or herself and the Board Accountability Mechanisms Committee shall review the Reconsideration Request without involvement by the Ombudsman.

(m) The Board Accountability Mechanisms Committee may ask ICANN Staff for its views on a Reconsideration Request, which comments shall be made publicly available on the Website.

(n) The Board Accountability Mechanisms Committee may request additional information or clarifications from the Requestor, and may elect to conduct a meeting with the Requestor by telephone, email or, if acceptable to the Requestor, in person. A Requestor may also ask for an opportunity to be heard. The Board Accountability Mechanisms Committee's decision on any such request is final. To the extent any information gathered in such a meeting is relevant to any recommendation by the Board Accountability Mechanisms Committee, it shall so state in its recommendation.

(o) The Board Accountability Mechanisms Committee may also request information relevant to the Reconsideration Request from third parties. To the extent any information gathered is relevant to any recommendation by the Board Accountability Mechanisms Committee, it shall so state in its recommendation. Any information collected by ICANN from third parties shall be provided to the Requestor.

(p) The Board Accountability Mechanisms Committee shall act on a Reconsideration Request on the basis of the public written record, including information submitted by the Requestor, by the ICANN Staff, and by any third party.

(q) The Board Accountability Mechanisms Committee shall make a final recommendation to the Board with respect to a Reconsideration Request within 30 days following its receipt of the Ombudsman's evaluation (or 30 days following receipt of the Reconsideration Request involving those matters for which the Ombudsman recuses himself or herself or the receipt of the Community Reconsideration Request, if applicable), unless impractical, in which case it shall report to the Board the circumstances that prevented it from making a final recommendation and its best estimate of the time required to produce such a final recommendation. In any event, the Board Accountability Mechanisms Committee shall endeavor to produce its final recommendation to the Board within 90 days of

receipt of the Reconsideration Request. The final recommendation of the Board Accountability Mechanisms Committee shall be documented and promptly (i.e., as soon as practicable) posted on the Website and shall address each of the arguments raised in the Reconsideration Request. The Requestor may file a 10-page (double-spaced, 12-point font) document, not including exhibits, in rebuttal to the Board Accountability Mechanisms Committee's recommendation within 15 days of receipt of the recommendation, which shall also be promptly (i.e., as soon as practicable) posted to the Website and provided to the Board for its evaluation; provided, that such rebuttal shall: (i) be limited to rebutting or contradicting the issues raised in the Board Accountability Mechanisms Committee's final recommendation; and (ii) not offer new evidence to support an argument made in the Requestor's original Reconsideration Request that the Requestor could have provided when the Requestor initially submitted the Reconsideration Request.

(r) The Board shall not be bound to follow the recommendations of the Board Accountability Mechanisms Committee. The final decision of the Board and its rationale shall be made public as part of the preliminary report and minutes of the Board meeting at which action is taken. The Board shall issue its decision on the recommendation of the Board Accountability Mechanisms Committee within 45 days of receipt of the Board Accountability Mechanisms Committee's recommendation or as soon thereafter as feasible. Any circumstances that delay the Board from acting within this timeframe must be identified and posted on the Website. In any event, the Board's final decision shall be made within 135 days of initial receipt of the Reconsideration Request by the Board Accountability Mechanisms Committee. The Board's decision on the recommendation shall be posted on the Website in accordance with the Board's posting obligations as set forth in Article 3 of these Bylaws. If the Requestor so requests, the Board shall post both a recording and a transcript of the substantive Board discussion from the meeting at which the Board considered the Board Accountability Mechanisms Committee's recommendation. All briefing materials supplied to the Board shall be provided to the Requestor. The Board may redact such briefing materials and the recording and transcript on the basis that such information (i) relates to confidential personnel matters, (ii) is covered by attorney-client privilege, work product doctrine or other recognized legal privilege, (iii) is subject to a legal obligation that ICANN maintain its confidentiality, (iv) would disclose trade secrets, or (v) would present a material risk of negative impact to the security, stability or resiliency of the Internet. In the case of any redaction, ICANN will provide the Requestor a written rationale for such redaction. If a Requestor believes that a redaction was improper, the Requestor may use an appropriate accountability mechanism to challenge the scope of ICANN's redaction.

(s) If the Requestor believes that the Board action or inaction for which a Reconsideration Request is submitted is so urgent that the timing requirements of the process set forth in this Section 4.2 are too long, the Requestor may apply to

the Board Accountability Mechanisms Committee for urgent consideration. Any request for urgent consideration must be made within two business days (as calculated by local time at the location of ICANN's principal office) of the posting of the resolution at issue. A request for urgent consideration must include a discussion of why the matter is urgent for reconsideration and must demonstrate a likelihood of success with the Reconsideration Request.

(t) The Board Accountability Mechanisms Committee shall respond to the request for urgent consideration within two business days after receipt of such request. If the Board Accountability Mechanisms Committee agrees to consider the matter with urgency, it will cause notice to be provided to the Requestor, who will have two business days after notification to complete the Reconsideration Request. The Board Accountability Mechanisms Committee shall issue a recommendation on the urgent Reconsideration Request within seven days of the completion of the filing of the Reconsideration Request, or as soon thereafter as feasible. If the Board Accountability Mechanisms Committee does not agree to consider the matter with urgency, the Requestor may still file a Reconsideration Request within the regular time frame set forth within these Bylaws.

(u) The Board Accountability Mechanisms Committee shall submit a report to the Board on an annual basis containing at least the following information for the preceding calendar year:

> (i) the number and general nature of Reconsideration Requests received, including an identification if the Reconsideration Requests were acted upon, summarily dismissed, or remain pending;
>
> (ii) for any Reconsideration Requests that remained pending at the end of the calendar year, the average length of time for which such Reconsideration Requests have been pending, and a description of the reasons for any Reconsideration Request pending for more than ninety (90) days;
>
> (iii) an explanation of any other mechanisms available to ensure that ICANN is accountable to persons materially affected by its decisions; and
>
> (iv) whether or not, in the Board Accountability Mechanisms Committee's view, the criteria for which reconsideration may be requested should be revised, or another process should be adopted or modified, to ensure that all persons materially affected by ICANN decisions have meaningful access to a review process that ensures fairness while limiting frivolous claims.

Section 4.3. INDEPENDENT REVIEW PROCESS FOR COVERED ACTIONS

(a) In addition to the reconsideration process described in Section 4.2, ICANN shall have a separate process for independent third-party review of Disputes (defined in Section 4.3(b)(iii)) alleged by a Claimant (as defined in Section 4.3(b)(i)) to be within the scope of the Independent Review Process ("**IRP**"). The IRP is intended to hear and resolve Disputes for the following purposes ("**Purposes of the IRP**"):

(i) Ensure that ICANN does not exceed the scope of its Mission and otherwise complies with its Articles of Incorporation and Bylaws.

(ii) Empower the global Internet community and Claimants to enforce compliance with the Articles of Incorporation and Bylaws through meaningful, affordable and accessible expert review of Covered Actions (as defined in Section 4.3(b)(i)).

(iii) Ensure that ICANN is accountable to the global Internet community and Claimants.

(iv) Address claims that ICANN has failed to enforce its rights under the IANA Naming Function Contract (as defined in Section 16.3(a)).

(v) Provide a mechanism by which direct customers of the IANA naming functions may seek resolution of PTI (as defined in Section 16.1) service complaints that are not resolved through mediation.

(vi) Reduce Disputes by creating precedent to guide and inform the Board, Officers (as defined in Section 15.1), Staff members, Supporting Organizations, Advisory Committees, and the global Internet community in connection with policy development and implementation.

(vii) Secure the accessible, transparent, efficient, consistent, coherent, and just resolution of Disputes.

(viii) Lead to binding, final resolutions consistent with international arbitration norms that are enforceable in any court with proper jurisdiction.

(ix) Provide a mechanism for the resolution of Disputes, as an alternative to legal action in the civil courts of the United States or other jurisdictions.

This Section 4.3 shall be construed, implemented, and administered in a manner consistent with these Purposes of the IRP.

(b) The scope of the IRP is defined with reference to the following terms:

> (i) A **"Claimant"** is any legal or natural person, group, or entity including, but not limited to the EC, a Supporting Organization, or an Advisory Committee that has been materially affected by a Dispute. To be materially affected by a Dispute, the Claimant must suffer an injury or harm that is directly and causally connected to the alleged violation.
>
> (A)The EC is deemed to be materially affected by all Covered Actions. ICANN shall not assert any defenses of standing or capacity against the EC in any forum.
>
> (B)ICANN shall not object to the standing of the EC, a Supporting Organization, or an Advisory Committee to participate in an IRP, to compel an IRP, or to enforce an IRP decision on the basis that it is not a legal person with capacity to sue. No special pleading of a Claimant's capacity or of the legal existence of a person that is a Claimant shall be required in the IRP proceedings. No Claimant shall be allowed to proceed if the IRP Panel (as defined in Section 4.3(g)) concludes based on evidence submitted to it that the Claimant does not fairly or adequately represent the interests of those on whose behalf the Claimant purports to act.
>
> (ii) "**Covered Actions**" are defined as any actions or failures to act by or within ICANN committed by the Board, individual Directors, Officers, or Staff members that give rise to a Dispute.
>
> (iii) "**Disputes**" are defined as:

(A)Claims that Covered Actions constituted an action or inaction that violated the Articles of Incorporation or Bylaws, including but not limited to any action or inaction that:

(1) exceeded the scope of the Mission;

(2) resulted from action taken in response to advice or input from any Advisory Committee or Supporting Organization that are claimed to be inconsistent with the Articles of Incorporation or Bylaws;

(3) resulted from decisions of process-specific expert panels that are claimed to be inconsistent with the Articles of Incorporation or Bylaws;

(4) resulted from a response to a DIDP (as defined in Section 22.7(d)) request that is claimed to be inconsistent with the Articles of Incorporation or Bylaws; or

(5) arose from claims involving rights of the EC as set forth in the Articles of Incorporation or Bylaws.

(B)Claims that ICANN, the Board, individual Directors, Officers or Staff members have not enforced ICANN's contractual rights with respect to the IANA Naming Function Contract, and

(C)Claims regarding PTI service complaints by direct customers of the IANA naming functions that are not resolved through mediation.

(c) Notwithstanding any other provision in this Section 4.3, the IRP's scope shall exclude all of the following:

> (i) EC challenges to the result(s) of a PDP, unless the Supporting Organization(s) that approved the PDP supports the EC bringing such a challenge;
>
> (ii) Claims relating to ccTLD delegations and re-delegations;
>
> (iii) Claims relating to Internet numbering resources, and
>
> (iv) Claims relating to protocol parameters.

(d) An IRP shall commence with the Claimant's filing of a written statement of a Dispute (a "**Claim**") with the IRP Provider (described in Section 4.3(m) below). For the EC to commence an IRP ("**Community IRP**"), the EC shall first comply with the procedures set forth in Section 4.2 of Annex D.

(e) Cooperative Engagement Process

> (i) Except for Claims brought by the EC in accordance with this Section 4.3 and Section 4.2 of Annex D, prior to the filing of a Claim, the parties are strongly encouraged to participate in a non-binding Cooperative Engagement Process ("**CEP**") for the purpose of attempting to resolve

and/or narrow the Dispute. CEPs shall be conducted pursuant to the CEP Rules to be developed with community involvement, adopted by the Board, and as amended from time to time.

(ii) The CEP is voluntary. However, except for Claims brought by the EC in accordance with this Section 4.3 and Section 4.2 of Annex D, if the Claimant does not participate in good faith in the CEP and ICANN is the prevailing party in the IRP, the IRP Panel shall award to ICANN all reasonable fees and costs incurred by ICANN in the IRP, including legal fees.

(iii) Either party may terminate the CEP efforts if that party: (A) concludes in good faith that further efforts are unlikely to produce agreement; or (B) requests the inclusion of an independent dispute resolution facilitator ("**IRP Mediator**") after at least one CEP meeting.

(iv) Unless all parties agree on the selection of a particular IRP Mediator, any IRP Mediator appointed shall be selected from the members of the Standing Panel (described in Section 4.3(j) below) by its Chair, but such IRP Mediator shall not thereafter be eligible to serve as a panelist presiding over an IRP on the matter.

(f) ICANN hereby waives any defenses that may be afforded under Section 5141 of the California Corporations Code ("**CCC**") against any Claimant, and shall not object to the standing of any such Claimant to participate in or to compel an IRP, or to enforce an IRP decision on the basis that such Claimant may not otherwise be able to assert that a Covered Action is ultra vires.

(g) Upon the filing of a Claim, an Independent Review Process Panel ("**IRP Panel**", described in Section 4.3(k) below) shall be selected in accordance with the Rules of Procedure (as defined in Section 4.3(n)(i)). Following the selection of an IRP Panel, that IRP Panel shall be charged with hearing and resolving the Dispute, considering the Claim and ICANN's written response ("**Response**") in compliance with the Articles of Incorporation and Bylaws, as understood in light of prior IRP Panel decisions decided under the same (or an equivalent prior) version of the provision of the Articles of Incorporation and Bylaws at issue, and norms of applicable law. If no Response is timely filed by ICANN, the IRP Panel may accept the Claim as unopposed and proceed to evaluate and decide the Claim pursuant to the procedures set forth in these Bylaws.

(h) After a Claim is referred to an IRP Panel, the parties are urged to participate in conciliation discussions for the purpose of attempting to narrow the issues that are to be addressed by the IRP Panel.

(i) Each IRP Panel shall conduct an objective, de novo examination of the Dispute.

(i) With respect to Covered Actions, the IRP Panel shall make findings of fact to determine whether the Covered Action constituted an action or inaction that violated the Articles of Incorporation or Bylaws.

(ii) All Disputes shall be decided in compliance with the Articles of Incorporation and Bylaws, as understood in the context of the norms of applicable law and prior relevant IRP decisions.

(iii) For Claims arising out of the Board's exercise of its fiduciary duties, the IRP Panel shall not replace the Board's reasonable judgment with its own so long as the Board's action or inaction is within the realm of reasonable business judgment.

(iv) With respect to claims that ICANN has not enforced its contractual rights with respect to the IANA Naming Function Contract, the standard of review shall be whether there was a material breach of ICANN's obligations under the IANA Naming Function Contract, where the alleged breach has resulted in material harm to the Claimant.

(v) For avoidance of doubt, IRPs initiated through the mechanism contemplated at Section 4.3(a)(iv) above, shall be subject to a separate standard of review as defined in the IANA Naming Function Contract.

(j) Standing Panel

(i) There shall be an omnibus standing panel of at least seven members (the "**Standing Panel**") each of whom shall possess significant relevant legal expertise in one or more of the following areas: international law, corporate governance, judicial systems, alternative dispute resolution and/or arbitration. Each member of the Standing Panel shall also have knowledge, developed over time, regarding the DNS and ICANN's Mission, work, policies, practices, and procedures. Members of the Standing Panel shall receive at a minimum, training provided by ICANN on the workings and management of the Internet's unique identifiers and other appropriate training as recommended by the IRP Implementation Oversight Team (described in Section 4.3(n)(i)).

(ii) ICANN shall, in consultation with the Supporting Organizations and Advisory Committees, initiate a four-step process to establish the Standing Panel to ensure the availability of a number of IRP panelists that is sufficient to allow for the timely resolution of Disputes consistent with the Purposes of the IRP.

(A)ICANN, in consultation with the Supporting Organizations and Advisory Committees, shall initiate a tender process for an organization to provide administrative support for the IRP Provider (as defined in Section 4.3(m)), beginning by consulting the "**IRP Implementation Oversight Team**" (described in Section 4.3(n)(i)) on a draft tender document.

(B)ICANN shall issue a call for expressions of interest from potential panelists, and work with the Supporting Organizations and Advisory Committees and the Board to identify and solicit applications from well-qualified candidates, and to conduct an initial review and vetting of applications.

(C)The Supporting Organizations and Advisory Committees shall nominate a slate of proposed panel members from the well-qualified candidates identified per the process set forth in Section 4.3(j)(ii)(B).

(D)Final selection shall be subject to Board confirmation, which shall not be unreasonably withheld.

(iii) Appointments to the Standing Panel shall be made for a fixed term of five years with no removal except for specified cause in the nature of corruption, misuse of position, fraud or criminal activity. The recall process shall be developed by the IRP Implementation Oversight Team.

(iv) Reasonable efforts shall be taken to achieve cultural, linguistic, gender, and legal tradition diversity, and diversity by Geographic Region (as defined in Section 7.5).

(k) IRP Panel

(i) A three-member IRP Panel shall be selected from the Standing Panel to hear a specific Dispute.

(ii) The Claimant and ICANN shall each select one panelist from the Standing Panel, and the two panelists selected by the parties will select the third panelist from the Standing Panel. In the event that a Standing Panel is

not in place when an IRP Panel must be convened for a given proceeding or is in place but does not have capacity due to other IRP commitments or the requisite diversity of skill and experience needed for a particular IRP proceeding, the Claimant and ICANN shall each select a qualified panelist from outside the Standing Panel and the two panelists selected by the parties shall select the third panelist. In the event that no Standing Panel is in place when an IRP Panel must be convened and the two party-selected panelists cannot agree on the third panelist, the IRP Provider's rules shall apply to selection of the third panelist.

(iii) Assignment from the Standing Panel to IRP Panels shall take into consideration the Standing Panel members' individual experience and expertise in issues related to highly technical, civil society, business, diplomatic, and regulatory skills as needed by each specific proceeding, and such requests from the parties for any particular expertise.

(iv) Upon request of an IRP Panel, the IRP Panel shall have access to independent skilled technical experts at the expense of ICANN, although all substantive interactions between the IRP Panel and such experts shall be conducted on the record, except when public disclosure could materially and unduly harm participants, such as by exposing trade secrets or violating rights of personal privacy.

(v) IRP Panel decisions shall be made by a simple majority of the IRP Panel.

(l) All IRP proceedings shall be administered in English as the primary working language, with provision of translation services for Claimants if needed.

(m) IRP Provider

(i) All IRP proceedings shall be administered by a well-respected international dispute resolution provider ("**IRP Provider**"). The IRP Provider shall receive and distribute IRP Claims, Responses, and all other submissions arising from an IRP at the direction of the IRP Panel, and shall function independently from ICANN.

(n) Rules of Procedure

(i) An IRP Implementation Oversight Team shall be established in consultation with the Supporting Organizations and Advisory Committees and comprised of members of the global Internet community. The IRP

> Implementation Oversight Team, and once the Standing Panel is established the IRP Implementation Oversight Team in consultation with the Standing Panel, shall develop clear published rules for the IRP ("**Rules of Procedure**") that conform with international arbitration norms and are streamlined, easy to understand and apply fairly to all parties. Upon request, the IRP Implementation Oversight Team shall have assistance of counsel and other appropriate experts.
>
> (ii) The Rules of Procedure shall be informed by international arbitration norms and consistent with the Purposes of the IRP. Specialized Rules of Procedure may be designed for reviews of PTI service complaints that are asserted by direct customers of the IANA naming functions and are not resolved through mediation. The Rules of Procedure shall be published and subject to a period of public comment that complies with the designated practice for public comment periods within ICANN, and take effect upon approval by the Board, such approval not to be unreasonably withheld.
>
> (iii) The Standing Panel may recommend amendments to such Rules of Procedure as it deems appropriate to fulfill the Purposes of the IRP, however no such amendment shall be effective without approval by the Board after publication and a period of public comment that complies with the designated practice for public comment periods within ICANN.
>
> (iv) The Rules of Procedure are intended to ensure fundamental fairness and due process and shall at a minimum address the following elements:

(A) The time within which a Claim must be filed after a Claimant becomes aware or reasonably should have become aware of the action or inaction giving rise to the Dispute;

(B)Issues relating to joinder, intervention, and consolidation of Claims;

(C)Rules governing written submissions, including the required elements of a Claim, other requirements or limits on content, time for filing, length of statements, number of supplemental statements, if any, permitted evidentiary support (factual and expert), including its length, both in support of a Claimant's Claim and in support of ICANN's Response;

(D)Availability and limitations on discovery methods;

(E)Whether hearings shall be permitted, and if so what form and structure such hearings would take;

(F)Procedures if ICANN elects not to respond to an IRP; and

(G)The standards and rules governing appeals from IRP Panel decisions, including which IRP Panel decisions may be appealed.

(o) Subject to the requirements of this Section 4.3, each IRP Panel shall have the authority to:

> (i) Summarily dismiss Disputes that are brought without standing, lack substance, or are frivolous or vexatious;
>
> (ii) Request additional written submissions from the Claimant or from other parties;
>
> (iii) Declare whether a Covered Action constituted an action or inaction that violated the Articles of Incorporation or Bylaws, declare whether ICANN failed to enforce ICANN's contractual rights with respect to the IANA Naming Function Contract or resolve PTI service complaints by direct customers of the IANA naming functions, as applicable;
>
> (iv) Recommend that ICANN stay any action or decision, or take necessary interim action, until such time as the opinion of the IRP Panel is considered;
>
> (v) Consolidate Disputes if the facts and circumstances are sufficiently similar, and take such other actions as are necessary for the efficient resolution of Disputes;
>
> (vi) Determine the timing for each IRP proceeding; and
>
> (vii) Determine the shifting of IRP costs and expenses consistent with Section 4.3(r).

(p) A Claimant may request interim relief. Interim relief may include prospective relief, interlocutory relief, or declaratory or injunctive relief, and specifically may include a stay of the challenged ICANN action or decision until such time as the opinion of the IRP Panel is considered as described in Section 4.3(o)(iv), in order to maintain the *status quo*. A single member of the Standing Panel ("**Emergency Panelist**") shall be selected to adjudicate requests for interim relief. In the event that no Standing Panel is in place when an Emergency Panelist must be selected, the IRP Provider's rules shall apply to the selection of the Emergency Panelist. Interim relief may only be provided if the Emergency Panelist determines that the Claimant has established all of the following factors:

(i) A harm for which there will be no adequate remedy in the absence of such relief;

(ii) Either: (A) likelihood of success on the merits; or (B) sufficiently serious questions related to the merits; and

(iii) A balance of hardships tipping decidedly toward the party seeking relief.

(q) Conflicts of Interest

(i) Standing Panel members must be independent of ICANN and its Supporting Organizations and Advisory Committees, and so must adhere to the following criteria:

(A)Upon consideration for the Standing Panel and on an ongoing basis, Panelists shall have an affirmative obligation to disclose any material relationship with ICANN, a Supporting Organization, an Advisory Committee, or any other participant in an IRP proceeding.

(B)Additional independence requirements to be developed by the IRP Implementation Oversight Team, including term limits and restrictions on post-term appointment to other ICANN positions.

(ii) The IRP Provider shall disclose any material relationship with ICANN, a Supporting Organization, an Advisory Committee, or any other participant in an IRP proceeding.

(r) ICANN shall bear all the administrative costs of maintaining the IRP mechanism, including compensation of Standing Panel members. Except as otherwise provided in Section 4.3(e)(ii), each party to an IRP proceeding shall bear its own legal expenses, except that ICANN shall bear all costs associated with a Community IRP, including the costs of all legal counsel and technical experts. Nevertheless, except with respect to a Community IRP, the IRP Panel may shift and provide for the losing party to pay administrative costs and/or fees of the prevailing party in the event it identifies the losing party's Claim or defense as frivolous or abusive.

(s) An IRP Panel should complete an IRP proceeding expeditiously, issuing an

early scheduling order and its written decision no later than six months after the filing of the Claim, except as otherwise permitted under the Rules of Procedure. The preceding sentence does not provide the basis for a Covered Action.

(t) Each IRP Panel shall make its decision based solely on the documentation, supporting materials, and arguments submitted by the parties, and in its decision shall specifically designate the prevailing party as to each part of a Claim.

(u) All IRP Panel proceedings shall be conducted on the record, and documents filed in connection with IRP Panel proceedings shall be posted on the Website, except for settlement negotiation or other proceedings that could materially and unduly harm participants if conducted publicly. The Rules of Procedure, and all Claims, petitions, and decisions shall promptly be posted on the Website when they become available. Each IRP Panel may, in its discretion, grant a party's request to keep certain information confidential, such as trade secrets, but only if such confidentiality does not materially interfere with the transparency of the IRP proceeding.

(v) Subject to this Section 4.3, all IRP decisions shall be written and made public, and shall reflect a well-reasoned application of how the Dispute was resolved in compliance with the Articles of Incorporation and Bylaws, as understood in light of prior IRP decisions decided under the same (or an equivalent prior) version of the provision of the Articles of Incorporation and Bylaws at issue, and norms of applicable law.

(w) Subject to any limitations established through the Rules of Procedure, an IRP Panel decision may be appealed to the full Standing Panel sitting en banc within sixty (60) days of issuance of such decision.

(x) The IRP is intended as a final, binding arbitration process.

> (i) IRP Panel decisions are binding final decisions to the extent allowed by law unless timely and properly appealed to the en banc Standing Panel. En banc Standing Panel decisions are binding final decisions to the extent allowed by law.
>
> (ii) IRP Panel decisions and decisions of an en banc Standing Panel upon an appeal are intended to be enforceable in any court with jurisdiction over ICANN without a *de novo* review of the decision of the IRP Panel or en banc Standing Panel, as applicable, with respect to factual findings or conclusions of law.
>
> (iii) ICANN intends, agrees, and consents to be bound by all IRP Panel

decisions of Disputes of Covered Actions as a final, binding arbitration.

(A)Where feasible, the Board shall consider its response to IRP Panel decisions at the Board's next meeting, and shall affirm or reject compliance with the decision on the public record based on an expressed rationale. The decision of the IRP Panel, or en banc Standing Panel, shall be final regardless of such Board action, to the fullest extent allowed by law.

(B)If an IRP Panel decision in a Community IRP is in favor of the EC, the Board shall comply within 30 days of such IRP Panel decision.

(C)If the Board rejects an IRP Panel decision without undertaking an appeal to the en banc Standing Panel or rejects an en banc Standing Panel decision upon appeal, the Claimant or the EC may seek enforcement in a court of competent jurisdiction. In the case of the EC, the EC Administration may convene as soon as possible following such rejection and consider whether to authorize commencement of such an action.

(iv) By submitting a Claim to the IRP Panel, a Claimant thereby agrees that the IRP decision is intended to be a final, binding arbitration decision with respect to such Claimant. Any Claimant that does not consent to the IRP being a final, binding arbitration may initiate a non-binding IRP if ICANN agrees; provided that such a non-binding IRP decision is not intended to be and shall not be enforceable.

(y) ICANN shall seek to establish means by which community, non-profit Claimants and other Claimants that would otherwise be excluded from utilizing the IRP process may meaningfully participate in and have access to the IRP process.

Section 4.4. PERIODIC REVIEW OF ICANN STRUCTURE AND OPERATIONS

(a) The Board shall cause a periodic review of the performance and operation of each Supporting Organization, each Supporting Organization Council, each Advisory Committee (other than the Governmental Advisory Committee), and the Nominating Committee (as defined in Section 8.1) by an entity or entities independent of the organization under review. The goal of the review, to be undertaken pursuant to such criteria and standards as the Board shall direct, shall be to determine (i) whether that organization, council or committee has a continuing purpose in the ICANN structure, (ii) if so, whether any change in structure or operations is desirable to improve its effectiveness and (iii) whether that organization, council or committee is accountable to its constituencies,

stakeholder groups, organizations and other stakeholders.

These periodic reviews shall be conducted no less frequently than every five years, based on feasibility as determined by the Board. Each five-year cycle will be computed from the moment of the reception by the Board of the final report of the relevant review Working Group.

The results of such reviews shall be posted on the Website for public review and comment, and shall be considered by the Board no later than the second scheduled meeting of the Board after such results have been posted for 30 days. The consideration by the Board includes the ability to revise the structure or operation of the parts of ICANN being reviewed by a two-thirds vote of all Directors, subject to any rights of the EC under the Articles of Incorporation and these Bylaws.

(b) The Governmental Advisory Committee shall provide its own review mechanisms.

Section 4.5. ANNUAL REVIEW

ICANN will produce an annual report on the state of the accountability and transparency reviews, which will discuss the status of the implementation of all review processes required bySection 4.6 and the status of ICANN's implementation of the recommendations set forth in the final reports issued by the review teams to the Board following the conclusion of such review (**"Annual Review Implementation Report"**). The Annual Review Implementation Report will be posted on the Website for public review and comment. Each Annual Review Implementation Report will be considered by the Board and serve as an input to the continuing process of implementing the recommendations from the review teams set forth in the final reports of such review teams required in Section 4.6.

Section 4.6. SPECIFIC REVIEWS

(a) Review Teams and Reports

> (i) Review teams will be established for each applicable review, which will include both a limited number of members and an open number of observers. The chairs of the Supporting Organizations and Advisory Committees participating in the applicable review shall select a group of up to 21 review team members from among the prospective members nominated by the Supporting Organizations and Advisory Committees,

balanced for diversity and skill. In addition, the Board may designate one Director or Liaison to serve as a member of the review team. Specific guidance on the selection process is provided within the operating standards developed for the conduct of reviews under this Section 4.6 (the "**Operating Standards**"). The Operating Standards shall be developed through community consultation, including public comment opportunities as necessary that comply with the designated practice for public comment periods within ICANN. The Operating Standards must be aligned with the following guidelines:

(A)Each Supporting Organization and Advisory Committee participating in the applicable review may nominate up to seven prospective members for the review team;

(B)Any Supporting Organization or Advisory Committee nominating at least one, two or three prospective review team members shall be entitled to have those one, two or three nominees selected as members to the review team, so long as the nominees meet any applicable criteria for service on the team; and

(C)If any Supporting Organization or Advisory Committee has not nominated at least three prospective review team members, the Chairs of the Supporting Organizations and Advisory Committees shall be responsible for the determination of whether all 21 SO/AC member seats shall be filled and, if so, how the seats should be allocated from among those nominated.

(ii) Members and liaisons of review teams shall disclose to ICANN and their applicable review team any conflicts of interest with a specific matter or issue under review in accordance with the most recent Board-approved practices and Operating Standards. The applicable review team may exclude from the discussion of a specific complaint or issue any member deemed by the majority of review team members to have a conflict of interest. Further details on the conflict of interest practices are included in the Operating Standards.

(iii) Review team decision-making practices shall be specified in the Operating Standards, with the expectation that review teams shall try to operate on a consensus basis. In the event a consensus cannot be found among the members of a review team, a majority vote of the members may be taken.

(iv) Review teams may also solicit and select independent experts to render advice as requested by the review team. ICANN shall pay the reasonable

fees and expenses of such experts for each review contemplated by this Section 4.6 to the extent such fees and costs are consistent with the budget assigned for such review. Guidelines on how review teams are to work with and consider independent expert advice are specified in the Operating Standards.

(v) Each review team may recommend that the applicable type of review should no longer be conducted or should be amended.

(vi) Confidential Disclosure to Review Teams

(A) To facilitate transparency and openness regarding ICANN's deliberations and operations, the review teams, or a subset thereof, shall have access to ICANN internal information and documents pursuant to the Confidential Disclosure Framework set forth in the Operating Standards (the "**Confidential Disclosure Framework**"). The Confidential Disclosure Framework must be aligned with the following guidelines:

(1) ICANN must provide a justification for any refusal to reveal requested information. ICANN's refusal can be appealed to the Ombudsman and/or the ICANN Board for a ruling on the disclosure request.

(2) ICANN may designate certain documents and information as "for review team members only" or for a subset of the review team members based on conflict of interest. ICANN's designation of documents may also be appealed to the Ombudsman and/or the ICANN Board.

(3) ICANN may require review team members to sign a non-disclosure agreement before accessing documents.

(vii) Reports

(A) Each report of the review team shall describe the degree of consensus or agreement reached by the review team on each recommendation contained in such report. Any member of a review team not in favor of a recommendation of its review team (whether as a result of voting against a matter or objecting to the consensus position) may record a minority dissent to such recommendation, which shall be included in the report of the review team. The review team shall attempt to prioritize each of its recommendations and provide a rationale for such prioritization.

(B) At least one draft report of the review team shall be posted on the Website for public review and comment. The review team must consider the public comments received in response to any posted draft report and shall

amend the report as the review team deems appropriate and in the public interest before submitting its final report to the Board. The final report should include an explanation of how public comments were considered as well as a summary of changes made in response to public comments.

(C) Each final report of a review team shall be published for public comment in advance of the Board's consideration. Within six months of receipt of a final report, the Board shall consider such final report and the public comments on the final report, and determine whether to approve the recommendations in the final report. If the Board does not approve any or all of the recommendations, the written rationale supporting the Board's decision shall include an explanation for the decision on each recommendation that was not approved. The Board shall promptly direct implementation of the recommendations that were approved.

(b) Accountability and Transparency Review

(i) The Board shall cause a periodic review of ICANN's execution of its commitment to maintain and improve robust mechanisms for public input, accountability, and transparency so as to ensure that the outcomes of its decision-making reflect the public interest and are accountable to the Internet community ("**Accountability and Transparency Review**").

(ii) The issues that the review team for the Accountability and Transparency Review (the "**Accountability and Transparency Review Team**") may assess include, but are not limited to, the following:

(A) assessing and improving Board governance which shall include an ongoing evaluation of Board performance, the Board selection process, the extent to which the Board's composition and allocation structure meets ICANN's present and future needs, and the appeal mechanisms for Board decisions contained in these Bylaws;

(B) assessing the role and effectiveness of the GAC's interaction with the Board and with the broader ICANN community, and making recommendations for improvement to ensure effective consideration by ICANN of GAC input on the public policy aspects of the technical coordination of the DNS;

(C) assessing and improving the processes by which ICANN receives public input (including adequate explanation of decisions taken and the rationale

thereof);

(D) assessing the extent to which ICANN's decisions are supported and accepted by the Internet community;

(E) assessing the policy development process to facilitate enhanced cross community deliberations, and effective and timely policy development; and

(F) assessing and improving the Independent Review Process.

(iii) The Accountability and Transparency Review Team shall also assess the extent to which prior Accountability and Transparency Review recommendations have been implemented and the extent to which implementation of such recommendations has resulted in the intended effect.

(iv) The Accountability and Transparency Review Team may recommend to the Board the termination or amendment of other periodic reviews required by this Section 4.6, and may recommend to the Board the creation of additional periodic reviews.

(v) The Accountability and Transparency Review Team should issue its final report within one year of convening its first meeting.

(vi) The Accountability and Transparency Review shall be conducted no less frequently than every five years measured from the date the previous Accountability and Transparency Review Team was convened.

(c) Security, Stability, and Resiliency Review

(i) The Board shall cause a periodic review of ICANN's execution of its commitment to enhance the operational stability, reliability, resiliency, security, and global interoperability of the systems and processes, both internal and external, that directly affect and/or are affected by the Internet's system of unique identifiers that ICANN coordinates ("**SSR Review**").

(ii) The issues that the review team for the SSR Review ("**SSR Review Team**") may assess are the following:

(A) security, operational stability and resiliency matters, both physical and network, relating to the coordination of the Internet's system of unique identifiers;

(B) conformance with appropriate security contingency planning framework for the Internet's system of unique identifiers; and

(C) maintaining clear and globally interoperable security processes for those portions of the Internet's system of unique identifiers that ICANN coordinates.

(iii) The SSR Review Team shall also assess the extent to which ICANN has successfully implemented its security efforts, the effectiveness of the security efforts to deal with actual and potential challenges and threats to the security and stability of the DNS, and the extent to which the security efforts are sufficiently robust to meet future challenges and threats to the security, stability and resiliency of the DNS, consistent with ICANN's Mission.

(iv) The SSR Review Team shall also assess the extent to which prior SSR Review recommendations have been implemented and the extent to which implementation of such recommendations has resulted in the intended effect.

(v) The SSR Review shall be conducted no less frequently than every five years, measured from the date the previous SSR Review Team was convened.

(d) Competition, Consumer Trust and Consumer Choice Review

(i) ICANN will ensure that it will adequately address issues of competition, consumer protection, security, stability and resiliency, malicious abuse issues, sovereignty concerns, and rights protection prior to, or concurrent with, authorizing an increase in the number of new top-level domains in the root zone of the DNS pursuant to an application process initiated on or after the date of these Bylaws ("**New gTLD Round**").

(ii) After a New gTLD Round has been in operation for one year, the Board shall cause a competition, consumer trust and consumer choice review as specified in this Section 4.6(d) ("**CCT Review**").

(iii) The review team for the CCT Review ("**CCT Review Team**") will examine (A) the extent to which the expansion of gTLDs has promoted competition, consumer trust and consumer choice and (B) the effectiveness of the New gTLD Round's application and evaluation process and

safeguards put in place to mitigate issues arising from the New gTLD Round.

(iv) For each of its recommendations, the CCT Review Team should indicate whether the recommendation, if accepted by the Board, must be implemented before opening subsequent rounds of new generic top-level domain applications periods.

(v) The CCT Review Team shall also assess the extent to which prior CCT Review recommendations have been implemented and the extent to which implementation of such recommendations has resulted in the intended effect.

(e) Registration Directory Service Review

(i) Subject to applicable laws, ICANN shall use commercially reasonable efforts to enforce its policies relating to registration directory services and shall work with Supporting Organizations and Advisory Committees to explore structural changes to improve accuracy and access to generic top-level domain registration data, as well as consider safeguards for protecting such data.

(ii) The Board shall cause a periodic review to assess the effectiveness of the then current gTLD registry directory service and whether its implementation meets the legitimate needs of law enforcement, promoting consumer trust and safeguarding registrant data ("**Directory Service Review**").

(iii) The review team for the Directory Service Review ("**Directory Service Review Team**") will consider the Organisation for Economic Co-operation and Development ("**OECD**") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data as defined by the OECD in 1980 and amended in 2013 and as may be amended from time to time.

(iv) The Directory Service Review Team shall assess the extent to which prior Directory Service Review recommendations have been implemented and the extent to which implementation of such recommendations has resulted in the intended effect.

(v) The Directory Service Review shall be conducted no less frequently than every five years, measured from the date the previous Directory Service

> Review Team was convened, except that the first Directory Service Review to be conducted after 1 October 2016 shall be deemed to be timely if the applicable Directory Service Review Team is convened on or before 31 October 2016.

Section 4.7. COMMUNITY MEDIATION

(a) If the Board refuses or fails to comply with a duly authorized and valid EC Decision under these Bylaws, the EC Administration representative of any Decisional Participant who supported the exercise by the EC of its rights in the applicable EC Decision during the applicable decision period may request that the EC initiate a mediation process pursuant to this Section 4.7. The Board shall be deemed to have refused or failed to comply with a duly authorized and valid EC Decision if the Board has not complied with the EC Decision within 30 days of being notified of the relevant EC Decision.

(b) If a Mediation Initiation Notice (as defined in Section 4.1(a) of Annex D) is delivered to the Secretary pursuant to and in compliance with Section 4.1(a) of Annex D, as soon as reasonably practicable thereafter, the EC Administration shall designate individuals to represent the EC in the mediation ("**Mediation Administration**") and the Board shall designate representatives for the mediation ("**Board Mediation Representatives**"). Members of the EC Administration and the Board can designate themselves as representatives. ICANN shall promptly post the Mediation Initiation Notice on the Website.

(c) There shall be a single mediator who shall be selected by the agreement of the Mediation Administration and Board Mediation Representatives. The Mediation Administration shall propose a slate of at least five potential mediators, and the Board Mediation Representatives shall select a mediator from the slate or request a new slate until a mutually-agreed mediator is selected. The Board Mediation Representatives may recommend potential mediators for inclusion on the slates selected by the Mediation Administration. The Mediation Administration shall not unreasonably decline to include mediators recommended by the Board Mediation Representatives on proposed slates and the Board Mediation Representatives shall not unreasonably withhold consent to the selection of a mediator on slates proposed by the Mediation Administration.

(d) The mediator shall be a licensed attorney with general knowledge of contract law and general knowledge of the DNS and ICANN. The mediator may not have any ongoing business relationship with ICANN, any Supporting Organization (or constituent thereof), any Advisory Committee (or constituent thereof), the EC Administration or the EC. The mediator must confirm in writing that he or she is

not, directly or indirectly, and will not become during the term of the mediation, an employee, partner, executive officer, director, consultant or advisor of ICANN, any Supporting Organization (or constituent thereof), any Advisory Committee (or constituent thereof), the EC Administration or the EC.

(e) The mediator shall conduct the mediation in accordance with these Bylaws, the laws of California and the rules and procedures of a well-respected international dispute resolution provider, which may be the IRP Provider. The arbitration will be conducted in the English language consistent with the provisions relevant for mediation under the IRP Rules of Procedure and will occur in Los Angeles County, California, unless another location is mutually-agreed between the Mediation Administration and Board Mediation Representatives.

(f) The Mediation Administration and the Board Mediation Representatives shall discuss the dispute in good faith and attempt, with the mediator's assistance, to reach an amicable resolution of the dispute.

(g) ICANN shall bear all costs of the mediator.

(h) If the Mediation Administration and the Board Mediation Representatives have engaged in good faith participation in the mediation but have not resolved the dispute for any reason, the Mediation Administration or the Board Mediation Representatives may terminate the mediation at any time by declaring an impasse.

(i) If a resolution to the dispute is reached by the Mediation Administration and the Board Mediation Representatives, the Mediation Administration and the Board Mediation Representatives shall document such resolution including recommendations ("**Mediation Resolution**" and the date of such resolution, the "**Mediation Resolution Date**"). ICANN shall promptly post the Mediation Resolution on the Website (in no event later than 14 days after mediation efforts are completed) and the EC Administration shall promptly notify the Decisional Participants of the Mediation Resolution.

(j) The EC shall be deemed to have accepted the Mediation Resolution if it has not delivered an EC Community IRP Initiation Notice (as defined in Section 4.2(e) of Annex D) pursuant to and in compliance with Section 4.2 of Annex D within eighty (80) days following the Mediation Resolution Date.

ARTICLE 5 OMBUDSMAN

Section 5.1. OFFICE OF OMBUDSMAN

(a) ICANN shall maintain an Office of Ombudsman ("**Office of Ombudsman**"), to

be managed by an ombudsman ("**Ombudsman**") and to include such staff support as the Board determines is appropriate and feasible. The Ombudsman shall be a full-time position, with salary and benefits appropriate to the function, as determined by the Board.

(b) The Ombudsman shall be appointed by the Board for an initial term of two years, subject to renewal by the Board.

(c) The Ombudsman shall be subject to dismissal by the Board only upon a three-fourths (3/4) vote of the entire Board.

(d) The annual budget for the Office of Ombudsman shall be established by the Board as part of the annual ICANN Budget process. The Ombudsman shall submit a proposed budget to the President, and the President shall include that budget submission in its entirety and without change in the general ICANN Budget recommended by the ICANN President to the Board. Nothing in this Section 5.1 shall prevent the President from offering separate views on the substance, size, or other features of the Ombudsman's proposed budget to the Board.

Section 5.2. CHARTER

The charter of the Ombudsman shall be to act as a neutral dispute resolution practitioner for those matters for which the provisions of the Independent Review Process set forth in Section 4.3 have not been invoked. The principal function of the Ombudsman shall be to provide an independent internal evaluation of complaints by members of the ICANN community who believe that the ICANN staff, Board or an ICANN constituent body has treated them unfairly. The Ombudsman shall serve as an objective advocate for fairness, and shall seek to evaluate and where possible resolve complaints about unfair or inappropriate treatment by ICANN staff, the Board, or ICANN constituent bodies, clarifying the issues and using conflict resolution tools such as negotiation, facilitation, and "shuttle diplomacy" to achieve these results. With respect to the Reconsideration Request Process set forth in Section 4.2 , the Ombudsman shall serve the function expressly provided for in Section 4.2 .

Section 5.3. OPERATIONS

The Office of Ombudsman shall:

(a) facilitate the fair, impartial, and timely resolution of problems and complaints that affected members of the ICANN community (excluding employees and vendors/suppliers of ICANN) may have with specific actions or failures to act by the Board or ICANN staff which have not otherwise become the subject of either a Reconsideration Request or Independent Review Process;

(b) perform the functions set forth in Section 4.2 relating to review and consideration of Reconsideration Requests;

(c) exercise discretion to accept or decline to act on a complaint or question, including by the development of procedures to dispose of complaints that are insufficiently concrete, substantive, or related to ICANN's interactions with the community so as to be inappropriate subject matters for the Ombudsman to act on. In addition, and without limiting the foregoing, the Ombudsman shall have no authority to act in any way with respect to internal administrative matters, personnel matters, issues relating to membership on the Board, or issues related to vendor/supplier relations;

(d) have the right to have access to (but not to publish if otherwise confidential) all necessary information and records from ICANN staff and constituent bodies to enable an informed evaluation of the complaint and to assist in dispute resolution where feasible (subject only to such confidentiality obligations as are imposed by the complainant or any generally applicable confidentiality policies adopted by ICANN);

(e) heighten awareness of the Ombudsman program and functions through routine interaction with the ICANN community and online availability;

(f) maintain neutrality and independence, and have no bias or personal stake in an outcome; and

(g) comply with all ICANN conflicts of interest and confidentiality policies.

Section 5.4. INTERACTION WITH ICANN AND OUTSIDE ENTITIES

(a) No ICANN employee, Board member, or other participant in Supporting Organizations or Advisory Committees shall prevent or impede the Ombudsman's contact with the ICANN community (including employees of ICANN). ICANN employees and Board members shall direct members of the ICANN community who voice problems, concerns, or complaints about ICANN to the Ombudsman, who shall advise complainants about the various options available for review of such problems, concerns, or complaints.

(b) ICANN staff and other ICANN participants shall observe and respect determinations made by the Office of Ombudsman concerning confidentiality of any complaints received by that Office.

(c) Contact with the Ombudsman shall not constitute notice to ICANN of any

particular action or cause of action.

(d) The Ombudsman shall be specifically authorized to make such reports to the Board as he or she deems appropriate with respect to any particular matter and its resolution or the inability to resolve it. Absent a determination by the Ombudsman, in his or her sole discretion, that it would be inappropriate, such reports shall be posted on the Website.

(e) The Ombudsman shall not take any actions not authorized in these Bylaws, and in particular shall not institute, join, or support in any way any legal actions challenging ICANN structure, procedures, processes, or any conduct by the ICANN Board, staff, or constituent bodies.

Section 5.5. ANNUAL REPORT

The Office of Ombudsman shall publish on an annual basis a consolidated analysis of the year's complaints and resolutions, appropriately dealing with confidentiality obligations and concerns. Such annual report should include a description of any trends or common elements of complaints received during the period in question, as well as recommendations for steps that could be taken to minimize future complaints. The annual report shall be posted on the Website.

ARTICLE 6 EMPOWERED COMMUNITY

Section 6.1. COMPOSITION AND ORGANIZATION OF THE EMPOWERED COMMUNITY

(a) The Empowered Community ("**EC**") shall be a nonprofit association formed under the laws of the State of California consisting of the ASO, the ccNSO (as defined in Section 10.1), the GNSO (as defined in Section 11.1), the ALAC (as defined in Section 12.2(d)(i)) and the GAC (each a "**Decisional Participant**" or "associate," and collectively, the "**Decisional Participants**").

(b) This Article 6 shall constitute the articles of association of the EC and shall be considered the formational "governing document" (as defined in Section 18008 of the CCC) of the EC, and the terms contained herein and in these Bylaws relating to the EC shall be the EC's "governing principles" (as defined in Section 18010 of the CCC), which may only be amended as set forth in Section 25.2 . Where necessary for purposes of interpretation of these Bylaws, an "associate" shall be deemed to be a "member" of the EC as defined in Section 18015 of the CCC. Any change in the number and/or identity of Decisional Participants for any reason (including the resignation of any Decisional Participant or the addition of new Decisional Participants as a result of the creation of additional Supporting Organizations or Advisory Committees), and any corresponding changes in the

voting thresholds for exercise of the EC's rights described in Annex D of these Bylaws, will only be effective following the completion of the process for amending Fundamental Bylaws described in Section 25.2 and Annex D. The EC may not be dissolved except upon the completion of the process for amending Fundamental Bylaws described in Section 25.2 and Annex D.

(c) The sole purpose of the EC is to exercise its rights and perform its obligations under ICANN's Articles of Incorporation and these Bylaws, and the EC shall have no other powers or rights except as expressly provided therein. The EC may only act as provided in these Bylaws. Any act of the EC that is not in accordance with these Bylaws shall not be effective.

(d) The EC shall not acquire, hold, manage, encumber or transfer any interest in real or personal property, nor have any directors, officers or employees. The EC shall not merge with or into another entity nor shall it dissolve, except with the approval of the Board and as part of a Fundamental Bylaw Amendment (as defined in Section 25.2(b)).

(e) Decisional Participants shall not transfer their right to be an associate of the EC. Any attempted transfer by any Decisional Participant of its right to be an associate of the EC shall be void ab initio.

(f) The location and street address of the EC shall be the principal office of ICANN.

(g) Each Decisional Participant shall, except as otherwise provided in Annex D, adopt procedures for exercising the rights of such Decisional Participant pursuant to the procedures set forth in Annex D, including (i) who can submit a petition to such Decisional Participant, (ii) the process for an individual to submit a petition to such Decisional Participant, including whether a petition must be accompanied by a rationale, (iii) how the Decisional Participant determines whether to accept or reject a petition, (iv) how the Decisional Participant determines whether an issue subject to a petition has been resolved, (v) how the Decisional Participant determines whether to support or object to actions supported by another Decisional Participant, and (vi) the process for the Decisional Participant to notify its constituents of relevant matters.

Section 6.2. POWERS AND ACKNOWLEDGMENTS

(a) Pursuant to and in compliance with the terms and conditions of these Bylaws, the EC shall have the powers and rights, as set forth more fully elsewhere in these Bylaws, to:

(i) Appoint and remove individual Directors (other than the President);

(ii) Recall the entire Board;

(iii) Reject ICANN Budgets, IANA Budgets, Operating Plans (as defined in Section 22.5(a)(i)) and Strategic Plans (as defined in Section 22.5(b)(i));

(iv) Reject Standard Bylaw Amendments (as defined in Section 25.1(a));

(v) Approve Fundamental Bylaw Amendments, Articles Amendments (as defined in Section 25.2(b)), and Asset Sales (as defined in Article 26(a));

(vi) Reject PTI Governance Actions (as defined in Section 16.2(d));,

(vii) Require the ICANN Board to re-review its rejection of IFR Recommendation Decisions (as defined in Section 18.6(d)), Special IFR Recommendation Decisions (as defined in Section 18.12(e)), SCWG Creation Decisions (as defined in Section 19.1(d)) and SCWG Recommendation Decisions (as defined in Section 19.4(d));

(viii) Initiate a Community Reconsideration Request, mediation or a Community IRP; and

(ix) Take necessary and appropriate action to enforce its powers and rights, including through the community mechanism contained in Annex D or an action filed in a court of competent jurisdiction.

(b) The EC may pursue an action in any court with jurisdiction over ICANN to enforce the EC's rights under these Bylaws. ICANN acknowledges the EC's legal personhood and shall not raise the EC's legal personhood as a defense in any proceeding between ICANN and the EC. ICANN shall not assert as a defense that prior filing or completion of a Reconsideration Request or an IRP Claim was a prerequisite to an action in court regarding the EC's power to appoint or remove an individual Director or recall the Board (except to the extent an IRP Panel award is applicable pursuant to Section 3.6(e)).

(c) By nominating a Director for designation by the EC or exercising the community mechanism contained in Annex D with respect to any rights granted to the EC pursuant to these Bylaws, the EC and each of its Decisional Participants agrees and consents to the terms of these Bylaws and intends to be legally bound hereby.

Section 6.3. EC ADMINISTRATION

(a) The Decisional Participants shall act through their respective chairs or such other persons as may be designated by the Decisional Participants (collectively, such persons are the "**EC Administration**"). Each Decisional Participant shall deliver annually a written certification from its chair or co-chairs to the Secretary designating the individual who shall represent the Decisional Participant on the EC Administration.

(b) In representing a Decisional Participant on the EC Administration, the representative individual shall act solely as directed by the represented Decisional Participant and in accordance with processes developed by such Decisional Participant in accordance with Section 6.1(g).

(c) In representing the EC Administration, the individuals serving thereon shall act as required for the EC to follow the applicable procedures in Annex D, and to implement EC decisions made in accordance with such procedures.

(d) All communications and notices required or permitted to be given under these Bylaws by a Decisional Participant shall be provided by the Decisional Participant's representative on the EC Administration. All communications and notices required or permitted to be given under these Bylaws by the EC shall be provided by any member of the EC Administration. Where a particular Bylaws notice provision does not require notice to the Secretary, the EC and the Decisional Participants shall provide a copy of the notice to the Secretary in accordance with Section 21.5, and ICANN shall post it on the Website.

(e) ICANN shall be entitled to rely on notices from a Decisional Participant's representative or an individual serving on the EC Administration delivered in accordance with Section 21.5 as evidence that the actions set forth therein have been approved by or are the actions of the Decisional Participant, the EC or the EC Administration, as applicable, pursuant to and in compliance with the requirements of these Bylaws (including Annex D) .

(f) No person participating in the EC, the EC Administration or a Decisional Participant shall be liable for any debt, obligation or liability of ICANN or the EC, other than in the case of a fraudulent act committed by such person.

Section 6.4. CONSENT TO BOARD-INITIATED REMOVAL OF DIRECTOR WITHOUT CAUSE

In the event the EC Administration receives from the Secretary a valid notice as described in Section 7.11(a)(i)(B), indicating that the Board has voted to remove a Director without cause pursuant to Section 7.11(a)(i)(B), the EC shall without

deliberation consent to such removal, and the EC Administration shall provide notice to the Secretary of such consent.

ARTICLE 7 BOARD OF DIRECTORS

Section 7.1. COMPOSITION OF THE BOARD

The ICANN Board of Directors ("**Board**") shall consist of sixteen voting directors ("**Directors**"). In addition, four non-voting liaisons ("**Liaisons**") shall be appointed for the purposes set forth in Section 7.9. Only Directors shall be included in determining the existence of quorums, and in establishing the validity of votes taken by the Board.

Section 7.2. DIRECTORS AND THEIR SELECTION; ELECTION OF CHAIR AND VICE-CHAIR

(a) As of the effective date of the amendment and restatement of these Bylaws on 1 October 2016, the EC shall be the sole designator of ICANN and shall designate, within the meaning of Section 5220 of the CCC, all Directors except for the President ex officio. The EC shall notify promptly the Secretary in writing of the following designations:

> (i) Eight Directors nominated by the Nominating Committee to be designated as Directors by the EC. These seats on the Board are referred to in these Bylaws as Seats 1 through 8.
>
> (ii) Two Directors nominated by the ASO to be designated as Directors by the EC. These seats on the Board are referred to in these Bylaws as Seat 9 and Seat 10.
>
> (iii) Two Directors nominated by the ccNSO to be designated as Directors by the EC. These seats on the Board are referred to in these Bylaws as Seat 11 and Seat 12.
>
> (iv) Two Directors nominated by the GNSO to be designated as Directors by the EC. These seats on the Board are referred to in these Bylaws as Seat 13 and Seat 14.
>
> (v) One Director nominated by the At-Large Community to be designated as Directors by the EC. This seat on the Board is referred to in these Bylaws as Seat 15.

In addition to the Directors designated by the EC, the President shall serve ex officio as a Director. The seat held by the President on the Board is referred to in these Bylaws as Seat 16.

(b) In carrying out its responsibilities to nominate the Directors for Seats 1 through 8 for designation by the EC, the Nominating Committee shall ensure that the Board is composed of Directors who, in the aggregate, display diversity in geography, culture, skills, experience, and perspective, by applying the criteria set forth in Section 7.3, Section 7.4 and Section 7.5. At no time when it makes its nomination shall the Nominating Committee nominate a Director to fill any vacancy or expired term whose designation would cause the total number of Directors (not including the President) from countries in any one Geographic Region to exceed five; and the Nominating Committee shall ensure when it makes its nominations that the Board includes at least one Director who is from a country in each ICANN Geographic Region ("**Diversity Calculation**"). For purposes of this Section 7.2(b), if any candidate for director maintains citizenship of more than one country, or has been domiciled for more than five years in a country of which the candidate does not maintain citizenship ("**Domicile**"), that candidate may be deemed to be from either country and must select in his or her Statement of Interest the country of citizenship or Domicile that he or she wants the Nominating Committee to use for Diversity Calculation purposes. For purposes of this Section 7.2(b), a person can only have one Domicile, which shall be determined by where the candidate has a permanent residence and place of habitation.

(c) In carrying out their responsibilities to nominate Directors for Seats 9 through 15 for designation by the EC, the Supporting Organizations and the At-Large Community shall seek to ensure that the Board is composed of Directors who, in the aggregate, display diversity in geography, culture, skills, experience, and perspective, by applying the criteria set forth in Section 7.3, Section 7.4 and Section 7.5. The Supporting Organizations shall ensure that, at any given time, no two Directors nominated by a Supporting Organization are citizens from the same country or of countries located in the same Geographic Region. For purposes of this Section 7.2(c), if any candidate for Director maintains citizenship or Domicile of more than one country, that candidate may be deemed to be from either country and must select in his or her Statement of Interest the country of citizenship or Domicile that he or she wants the Supporting Organization or the At-Large Community, as applicable, to use for nomination purposes. For purposes of this Section 7.2(c), a person can only have one Domicile, which shall be determined by where the candidate has a permanent residence and place of habitation.

(d) The Board shall annually elect a Chair and a Vice-Chair from among the Directors, not to include the President.

(e) The EC shall designate each person nominated as a Director by the Nominating Committee, the ASO, the ccNSO, the GNSO and the At-Large Community in accordance with this Section 7.2.

(f) As a condition to sitting on the Board, each Director other than the President ex officio shall sign a pre-service letter pursuant to which such Director:

> (i) acknowledges and agrees to the EC's right to remove the Director at any time and for any reason following the processes set forth in these Bylaws;
>
> (ii) acknowledges and agrees that serving as a Director shall not establish any employment or other relationship (whether to ICANN, the EC, any body entitled to nominate a Director, or any of their agents) that provides any due process rights related to termination of service as a Director; and
>
> (iii) conditionally and irrevocably resigns as a Director automatically effective upon communication to the Director or, in the case of Board recall, communication to the Board of a final determination of removal following the processes set forth in these Bylaws.

Section 7.3.CRITERIA FOR NOMINATION OF DIRECTORS

Directors shall be:

(a) Accomplished persons of integrity, objectivity, and intelligence, with reputations for sound judgment and open minds, and a demonstrated capacity for thoughtful group decision-making;

(b) Persons with an understanding of ICANN's Mission and the potential impact of ICANN decisions on the global Internet community, and committed to the success of ICANN;

(c) Persons who will produce the broadest cultural and geographic diversity on the Board consistent with meeting the other criteria set forth in this Section 7.3;

(d) Persons who, in the aggregate, have personal familiarity with the operation of gTLD registries and registrars; with ccTLD registries; with IP address registries; with Internet technical standards and protocols; with policy-development procedures, legal traditions, and the public interest; and with the broad range of business, individual, academic, and non-commercial users of the Internet; and

(e) Persons who are able to work and communicate in written and spoken English.

Section 7.4. ADDITIONAL QUALIFICATIONS

(a) Notwithstanding anything herein to the contrary, no official of a national government or a multinational entity established by treaty or other agreement between national governments may serve as a Director. As used herein, the term "official" means a person (i) who holds an elective governmental office or (ii) who is employed by such government or multinational entity and whose primary function with such government or entity is to develop or influence governmental or public policies.

(b) No person who serves in any capacity (including as a liaison) on any Supporting Organization Council shall simultaneously serve as a Director or Liaison to the Board. If such a person is identified by, or presents themselves to, the Supporting Organization Council or the At-Large Community for consideration for nomination to serve as a Director, the person shall not thereafter participate in any discussion of, or vote by, the Supporting Organization Council or the committee designated by the At-Large Community relating to the nomination of Directors by the Council or At-Large Community, until the Council or committee(s) specified by the At-Large Community has nominated the full complement of Directors it is responsible for nominating. In the event that a person serving in any capacity on a Supporting Organization Council is considered for nomination to serve as a Director, the constituency group or other group or entity that selected the person may select a replacement for purposes of the Council's nomination process. In the event that a person serving in any capacity on the At-Large Advisory Committee is identified as or accepts a nomination to be considered for nomination by the At-Large Community as a Director, the Regional At-Large Organization or other group or entity that selected the person may select a replacement for purposes of the At-Large Community's nomination process.

(c) Persons serving in any capacity on the Nominating Committee shall be ineligible for nomination or designation to positions on the Board as provided by Section 8.8.

(d) No person who serves on the EC Administration while serving in that capacity shall be considered for nomination or designated to the Board, nor serve simultaneously on the EC Administration and as a Director or Liaison to the Board.

Section 7.5. INTERNATIONAL REPRESENTATION

In order to ensure broad international representation on the Board, the nomination of Directors by the Nominating Committee, each Supporting Organization and the At-Large Community shall comply with all applicable diversity provisions of these

Bylaws or of any memorandum of understanding referred to in these Bylaws concerning the Supporting Organization. One intent of these diversity provisions is to ensure that at all times each Geographic Region shall have at least one Director, and at all times no Geographic Region shall have more than five Directors on the Board (not including the President). As used in these Bylaws, each of the following is considered to be a "**Geographic Region**": (a) Europe; (b) Asia/Australia/Pacific; (c) Latin America/Caribbean islands; (d) Africa; and (e) North America. The specific countries included in each Geographic Region shall be determined by the Board, and this Section 7.5 shall be reviewed by the Board from time to time (and in any event at least once every three years) to determine whether any change is appropriate, taking account of the evolution of the Internet.

Section 7.6. DIRECTORS' CONFLICTS OF INTEREST

The Board, through the Board Governance Committee, shall require a statement from each Director not less frequently than once a year setting forth all business and other affiliations that relate in any way to the business and other affiliations of ICANN. Each Director shall be responsible for disclosing to ICANN any matter that could reasonably be considered to make such Director an "interested director" within the meaning of Section 5233 of the CCC. In addition, each Director shall disclose to ICANN any relationship or other factor that could reasonably be considered to cause the Director to be considered to be an "interested person" within the meaning of Section 5227 of the CCC. The Board shall adopt policies specifically addressing Director, Officer, EC and Supporting Organization conflicts of interest. No Director shall vote on any matter in which he or she has a material and direct financial interest that would be affected by the outcome of the vote.

Section 7.7. DUTIES OF DIRECTORS

Directors shall serve as individuals who have the duty to act in what they reasonably believe are the best interests of ICANN and not as representatives of the EC, the Nominating Committee, Supporting Organization or Advisory Committee that nominated them, as applicable, their employers, or any other organizations or constituencies.

Section 7.8. TERMS OF DIRECTORS

(a) The regular term of office of Director Seats 1 through 15 shall begin as follows:

> (i) The regular terms of Seats 1 through 3 shall begin at the conclusion of each ICANN annual meeting every third year after 2003;

(ii) The regular terms of Seats 4 through 6 shall begin at the conclusion of each ICANN annual meeting every third year after 2004;

(iii) The regular terms of Seats 7 and 8 shall begin at the conclusion of each ICANN annual meeting every third year after 2005;

(iv) The terms of Seats 9 and 12 shall begin at the conclusion of each ICANN annual meeting every third year after 2015;

(v) The terms of Seats 10 and 13 shall begin at the conclusion of each ICANN annual meeting every third year after 2013; and

(vi) The terms of Seats 11, 14 and 15 shall begin at the conclusion of each ICANN annual meeting every third year after 2014.

(b) Each Director holding any of Seats 1 through 15, including a Director nominated and designated to fill a vacancy, shall hold office for a term that lasts until the next term for that Seat commences and until a successor has been designated and qualified or until that Director resigns or is removed in accordance with these Bylaws. For the avoidance of doubt, the new governance provisions effective as of the amendment and restatement of these Bylaws on 1 October 2016 shall not have the effect of shortening or terminating the terms of any Directors serving at the time of the amendment and restatement.

(c) At least two months before the commencement of each annual meeting, the Nominating Committee shall give the EC Administration (with a copy to the Decisional Participants and Secretary) written notice of its nomination of Directors for seats with terms beginning at the conclusion of the annual meeting, and the EC Administration shall promptly provide the Secretary (with a copy to the Decisional Participants) with written notice of the designation of those Directors. All such notices shall be posted promptly to the Website.

(d) At least six months before the date specified for the commencement of the term as specified in Section 7.8(a)(iv) through Section 7.8(a)(vi) above, any Supporting Organization or the At-Large Community entitled to nominate a Director for a Seat with a term beginning that year shall give the EC Administration (with a copy to the Secretary and the Decisional Participants) written notice of its nomination of Directors for seats with terms beginning at the conclusion of the annual meeting, and the EC Administration shall promptly provide the Secretary (with a copy to the Decisional Participants) with written notice of the designation of those Directors. All such notices shall be posted promptly to the Website.

(e) No Director may serve more than three consecutive terms. For these

purposes, a person designated to fill a vacancy in a term shall not be deemed to have served that term.

(f) The term as Director of the person holding the office of President shall be for as long as, and only for as long as, such person holds the office of President.

Section 7.9. NON-VOTING LIAISONS

(a) The non-voting Liaisons shall include:

> (i) One appointed by the Governmental Advisory Committee;
>
> (ii) One appointed by the Root Server System Advisory Committee established by Section 12.2(c);
>
> (iii) One appointed by the Security and Stability Advisory Committee established by Section 12.2(b); and
>
> (iv) One appointed by the Internet Engineering Task Force.

(b) The Liaisons shall serve terms that begin at the conclusion of each annual meeting. At least one month before the commencement of each annual meeting, each body entitled to appoint a Liaison shall give the Secretary written notice of its appointment.

(c) Each Liaison may be reappointed, and shall remain in that position until a successor has been appointed or until the Liaison resigns or is removed in accordance with these Bylaws.

(d) The Liaisons shall be entitled to attend Board meetings, participate in Board discussions and deliberations, and have access (under conditions established by the Board) to materials provided to Directors for use in Board discussions, deliberations and meetings, but shall otherwise not have any of the rights and privileges of Directors. Liaisons shall be entitled (under conditions established by the Board) to use any materials provided to them pursuant to this Section 7.9(d) for the purpose of consulting with their respective committee or organization.

Section 7.10. RESIGNATION OF A DIRECTOR OR NON-VOTING LIAISON

Subject to Section 5226 of the CCC, any Director or Liaison may resign at any

time by giving written notice thereof to the Chair of the Board, the President, the Secretary, or the Board. Such resignation shall take effect at the time specified, and, unless otherwise specified, the acceptance of such resignation shall not be necessary to make it effective.

Section 7.11. REMOVAL OF A DIRECTOR OR NON-VOTING LIAISON

(a) Directors

> (i) Any Director designated by the EC may be removed without cause:
>
> (A) by the EC pursuant to and in compliance with procedures in Section 3.1 or Section 3.2 of Annex D, as applicable, or
>
> (B) following notice to that Director, by a three-fourths (3/4) majority vote of all Directors; provided, however, that (x) each vote to remove a Director shall be a separate vote on the sole question of the removal of that particular Director; and (y) such removal shall not be effective until the Secretary has provided notice to the EC Administration of the Board's removal vote and the requirements of Section 6.4 have been met.
>
> (ii) The Board may remove any Director who has been declared of unsound mind by a final order of court, or convicted of a felony, or been found by a final order or judgment of any court to have breached any duty under Sections 5230 through 5239 of the CCC, and in the case of such removal, the Secretary shall promptly notify the EC Administration in writing, with a copy to the body that nominated such Director, and shall promptly post such notification to the Website. The vacancies created by such removal shall be filled in accordance with Section 7.12(a).
>
> (iii) All Directors (other than the President) may be removed at the same time by the EC by the EC Administration delivering an EC Board Recall Notice to the Secretary pursuant to and in compliance with Section 3.3 of Annex D. The vacancies created by such removal shall be filled by the EC in accordance with Section 7.12(b).

(b) With the exception of the Liaison appointed by the Governmental Advisory Committee, any Liaison may be removed following notice to that Liaison and to the organization which selected that Liaison, by a three-fourths (3/4) majority vote of all Directors if the selecting organization fails to promptly remove that Liaison

following such notice. The vacancies created by such removal shall be filled in accordance with Section 7.12. The Board may request the Governmental Advisory Committee to consider the replacement of the Governmental Advisory Committee Liaison if the Board, by a three-fourths (3/4) majority vote of all Directors, determines that such an action is appropriate.

Section 7.12. VACANCIES

(a) This Section 7.12(a) shall apply to Board vacancies other than those occurring by recall of all Directors (other than the President). A vacancy or vacancies in the Board shall be deemed to exist in the case of the death, resignation, or removal of any Director or Interim Director (as defined in Section 7.12(b)), or if the authorized number of Directors is increased. Vacancies occurring in Seats 1 through 15 shall be filled by the EC after nomination as provided in Section 7.2 and Articles 8 through 12. A vacancy in Seat 16 shall be filled as provided in Article 15. A Director designated by the EC to fill a vacancy on the Board shall serve for the unexpired term of his or her predecessor in office and until a successor has been designated and qualified. No reduction of the authorized number of Directors shall have the effect of removing a Director prior to the expiration of the Director's term of office.

(b) This Section 7.12(b) shall apply to Board vacancies occurring when all Directors (other than the President) are recalled as provided by Section 7.11(a)(iii). Concurrently with delivery of any EC Board Recall Notice (as defined in Section 3.3(f) of Annex D), the EC Administration shall provide written notice of the EC's designation of individuals to fill such vacancies (each such individual, an **"Interim Director"**) to the Decisional Participants and to the Secretary, who shall cause such notice to be promptly posted to the Website. An Interim Director must meet the criteria specified in Section 7.3, Section 7.4 and Section 7.5, as applicable. An Interim Director shall hold office until the EC designates the Interim Director's successor in accordance with Section 7.12(a), and the successor's designation shall occur within 120 days of the Interim Director's designation. For avoidance of doubt, persons designated as Interim Directors may be eligible for designation as Directors as well.

(c) The organizations selecting the Liaisons identified in Section 7.9 are responsible for determining the existence of, and filling, any vacancies in those positions. Such organizations shall give the Secretary written notice of their appointments to fill any such vacancies, subject to the requirements set forth in Section 7.4, as applicable.

Section 7.13. ANNUAL MEETINGS

Annual meetings of ICANN shall be held for the purpose of electing Officers and

for the transaction of such other business as may come before the meeting. Each annual meeting of ICANN shall be held at the principal office of ICANN, or any other appropriate place of the Board's time and choosing, provided such annual meeting is held within 14 months of the immediately preceding annual meeting. If the Board determines that it is practical, the annual meeting should be distributed in real-time and archived video and audio formats on the Internet.

Section 7.14. REGULAR MEETINGS

Regular meetings of the Board shall be held on dates to be determined by the Board. In the absence of other designation, regular meetings shall be held at the principal office of ICANN.

Section 7.15. SPECIAL MEETINGS

Special meetings of the Board may be called by or at the request of one-quarter (1/4) of the Directors, by the Chair of the Board or the President. A call for a special meeting shall be made by the Secretary. Special meetings shall be held at the principal office of ICANN unless otherwise specified in the notice of the meeting.

Section 7.16. NOTICE OF MEETINGS

Notice of time and place of all meetings shall be delivered personally or by telephone or by electronic mail to each Director and Liaison, or sent by first-class mail (air mail for addresses outside the United States) or facsimile, charges prepaid, addressed to each Director and Liaison at the Director's or Liaison's address as it is shown on the records of ICANN. In case the notice is mailed, it shall be deposited in the United States mail at least fourteen (14) days before the time of the holding of the meeting. In case the notice is delivered personally or by telephone or facsimile or electronic mail it shall be delivered personally or by telephone or facsimile or electronic mail at least forty-eight (48) hours before the time of the holding of the meeting. Notwithstanding anything in this Section 7.16 to the contrary, notice of a meeting need not be given to any Director or Liaison who signed a waiver of notice or a Director who signed a written consent to holding the meeting or an approval of the minutes thereof, whether before or after the meeting, or who attends the meeting without protesting, prior thereto or at its commencement, the lack of notice to such Director. All such waivers, consents and approvals shall be filed with the corporate records or made a part of the minutes of the meetings.

Section 7.17. QUORUM

At all annual, regular, and special meetings of the Board, a majority of the total number of Directors then in office shall constitute a quorum for the transaction of business, and the act of a majority of the Directors present at any meeting at which there is a quorum shall be the act of the Board, unless otherwise provided herein or by law. If a quorum shall not be present at any meeting of the Board, the Directors present thereat may adjourn the meeting from time to time to another place, time or date. If the meeting is adjourned for more than twenty-four (24) hours, notice shall be given to those Directors not at the meeting at the time of the adjournment.

Section 7.18. ACTIONS BY TELEPHONE MEETING OR BY OTHER COMMUNICATIONS EQUIPMENT

Directors and Liaisons may participate in a meeting of the Board or Board Committee (as defined in Section 14.1) through use of (a) conference telephone or similar communications equipment, provided that all Directors participating in such a meeting can speak to and hear one another or (b) electronic video screen communication or other communication equipment; provided that (i) all Directors participating in such a meeting can speak to and hear one another, (ii) all Directors are provided the means of fully participating in all matters before the Board or Board Committee, and (iii) ICANN adopts and implements means of verifying that (A) a person participating in such a meeting is a Director or other person entitled to participate in the meeting and (B) all actions of, or votes by, the Board or Board Committee are taken or cast only by Directors and not persons who are not Directors. Participation in a meeting pursuant to this Section 7.18 constitutes presence in person at such meeting. ICANN shall make available at the place of any meeting of the Board the telecommunications equipment necessary to permit Directors and Liaisons to participate by telephone.

Section 7.19. ACTION WITHOUT MEETING

Any action required or permitted to be taken by the Board or a Committee of the Board may be taken without a meeting if all of the Directors entitled to vote thereat shall individually or collectively consent in writing to such action. Such written consent shall have the same force and effect as the unanimous vote of such Directors. Such written consent or consents shall be filed with the minutes of the proceedings of the Board.

Section 7.20. ELECTRONIC MAIL

If permitted by applicable law, communication by electronic mail shall be considered equivalent to any communication otherwise required to be in writing. ICANN shall take such steps as it deems appropriate under the circumstances to

assure itself that communications by electronic mail are authentic.

Section 7.21. BOARD RIGHTS OF INSPECTION

(a) Every Director shall have the right at any reasonable time to inspect and copy all books, records and documents of every kind, and to inspect the physical properties of ICANN.

(b) ICANN shall establish reasonable procedures to protect against the inappropriate disclosure of confidential information.

Section 7.22. COMPENSATION

(a) Except for the President of ICANN, who serves ex officio as a Director, each of the Directors shall be entitled to receive compensation for his or her services as a Director. The President shall receive only his or her compensation for service as President and shall not receive additional compensation for service as a Director.

(b) If the Board determines to offer a compensation arrangement to one or more Directors (other than the President) for services to ICANN as Directors, the Board shall follow the process that is calculated to pay an amount for service as a Director that is not an excess benefit under the standards set forth in Section 4958 of the Internal Revenue Code of 1986, as amended (the "**Code**").

(c) As part of the process, the Board shall retain an Independent Valuation Expert (as defined in Section 7.22(g)(i)) to consult with and to advise the Board regarding Director compensation arrangements and to issue to the Board a Reasoned Written Opinion (as defined in Section 7.22(g)(ii)) from such expert regarding the ranges of Reasonable Compensation (as defined in Section 7.22(g)(iii)) for any such services by a Director. The expert's opinion shall address all relevant factors affecting the level of compensation to be paid a Director, including offices held on the Board, attendance at Board and Board Committee meetings, the nature of service on the Board and on Board Committees, and appropriate data as to comparability regarding director compensation arrangements for U.S.-based, nonprofit, tax-exempt organizations possessing a global employee base.

(d) After having reviewed the Independent Valuation Expert's Reasoned Written Opinion, the Board shall meet with the expert to discuss the expert's opinion and to ask questions of the expert regarding the expert's opinion, the comparability data obtained and relied upon, and the conclusions reached by the expert.

(e) The Board shall adequately document the basis for any determination the Board makes regarding a Director compensation arrangement concurrently with making that determination.

(f) In addition to authorizing payment of compensation for services as Directors as set forth in this Section 7.22, the Board may also authorize the reimbursement of actual and necessary reasonable expenses incurred by any Director and by Liaisons performing their duties as Directors or Liaisons.

(g) As used in this Section 7.22, the following terms shall have the following meanings:

> (i) An "**Independent Valuation Expert**" means a person retained by ICANN to value compensation arrangements that: (A) holds itself out to the public as a compensation consultant; (B) performs valuations regarding compensation arrangements on a regular basis, with a majority of its compensation consulting services performed for persons other than ICANN; (C) is qualified to make valuations of the type of services involved in any engagement by and for ICANN; (D) issues to ICANN a Reasoned Written Opinion regarding a particular compensation arrangement; and (E) includes in its Reasoned Written Opinion a certification that it meets the requirements set forth in (A) through (D) of this definition.
>
> (ii) A "**Reasoned Written Opinion**" means a written opinion of a valuation expert who meets the requirements of Section 7.22(g)(i)(A) through (D). To be reasoned, the opinion must be based upon a full disclosure by ICANN to the valuation expert of the factual situation regarding the compensation arrangement that is the subject of the opinion, the opinion must articulate the applicable valuation standards relevant in valuing such compensation arrangement, the opinion must apply those standards to such compensation arrangement, and the opinion must arrive at a conclusion regarding whether the compensation arrangement is within the range of Reasonable Compensation for the services covered by the arrangement. A written opinion is reasoned even though it reaches a conclusion that is subsequently determined to be incorrect so long as the opinion addresses itself to the facts and the applicable standards. However, a written opinion is not reasoned if it does nothing more than recite the facts and express a conclusion.
>
> (iii) "**Reasonable Compensation**" shall have the meaning set forth in §53.4958-4(b)(1)(ii) of the Regulations issued under §4958 of the Code.

(h) Each of the Liaisons, with the exception of the Governmental Advisory Committee Liaison, shall be entitled to receive compensation for his or her

services as a Liaison. If the Board determines to offer a compensation arrangement to one or more Liaisons, the Board shall approve that arrangement by a required three-fourths (3/4) vote.

Section 7.23. PRESUMPTION OF ASSENT

A Director present at a Board meeting at which action on any corporate matter is taken shall be presumed to have assented to the action taken unless his or her dissent or abstention is entered in the minutes of the meeting, or unless such Director files a written dissent or abstention to such action with the person acting as the secretary of the meeting before the adjournment thereof, or forwards such dissent or abstention by registered mail to the Secretary immediately after the adjournment of the meeting. Such right to dissent or abstain shall not apply to a Director who voted in favor of such action.

Section 7.24 INTERIM BOARD

Except in circumstances in which urgent decisions are needed to protect the security, stability or resilience of the DNS or to the extent necessary to comply with its fiduciary obligations under applicable law, a Board that consists of a majority or more of Interim Directors (an "**Interim Board**") shall (a) consult with the chairs of the Supporting Organizations and Advisory Committees before making major decisions and (b) consult through a community forum (in a manner consistent with the process for a Rejection Action Community Forum pursuant to Section 2.3 of Annex D) prior to taking any action that would, if implemented, materially change ICANN's strategy, policies or management, including replacement of the then-serving President. Interim Directors shall be entitled to compensation as provided in this Article 7.

Section 7.25 COMMUNICATION OF DESIGNATION

Upon its receipt of nominations as provided in Articles 7 through 12, the EC Administration, on behalf of the EC, shall promptly notify the Secretary of the EC's designation of individuals to fill seats on the Board. ICANN shall post all such designations promptly to the Website.

ARTICLE 8 NOMINATING COMMITTEE

Section 8.1. DESCRIPTION

There shall be a Nominating Committee of ICANN ("**Nominating Committee**"), responsible for nominating all Directors except the President and those Directors nominated by Decisional Participants; for nominating two directors of PTI (in

accordance with the articles of incorporation and bylaws of PTI); and for such other selections as are set forth in these Bylaws. Notification of the Nominating Committee's Director nominations shall be given by the Nominating Committee Chair in writing to the EC Administration, with a copy to the Secretary, and the EC shall promptly act on it as provided in Section 7.25. Notification of the Nominating Committee's PTI director nomination shall be given to the Secretary.

Section 8.2. COMPOSITION

The Nominating Committee shall be composed of the following persons:

(a) A non-voting Chair, appointed by the Board;

(b) A non-voting Chair-Elect, appointed by the Board as a non-voting advisor;

(c) A non-voting liaison appointed by the Root Server System Advisory Committee established by Section 12.2(c);

(d) A non-voting liaison appointed by the Security and Stability Advisory Committee established by Section 12.2(b);

(e) A non-voting liaison appointed by the Governmental Advisory Committee;

(f) Five voting delegates selected by the At-Large Advisory Committee established by Section 12.2(d);

(g) Voting delegates to the Nominating Committee shall be selected from the Generic Names Supporting Organization established by Article 11, as follows:

> (i) One delegate from the Registries Stakeholder Group;
>
> (ii) One delegate from the Registrars Stakeholder Group;
>
> (iii) Two delegates from the Business Constituency, one representing small business users and one representing large business users;
>
> (iv) One delegate from the Internet Service Providers and Connectivity Providers Constituency (as defined in Section 11.5(a)(iii));
>
> (v) One delegate from the Intellectual Property Constituency; and
>
> (vi) One delegate from consumer and civil society groups, selected by the Non-Commercial Users Constituency.

(h) One voting delegate each selected by the following entities:

> (i) The Council of the Country Code Names Supporting Organization established by Section 10.3;
>
> (ii) The Council of the Address Supporting Organization established by Section 9.2; and
>
> (iii) The Internet Engineering Task Force.

(i) A non-voting Associate Chair, who may be appointed by the Chair, at his or her sole discretion, to serve during all or part of the term of the Chair. The Associate Chair may not be a person who is otherwise a member of the same Nominating Committee. The Associate Chair shall assist the Chair in carrying out the duties of the Chair, but shall not serve, temporarily or otherwise, in the place of the Chair.

Section 8.3. TERMS

(a) Each voting delegate shall serve a one-year term. A delegate may serve at most two successive one-year terms, after which at least two years must elapse before the individual is eligible to serve another term.

(b) The regular term of each voting delegate shall begin at the conclusion of an ICANN annual meeting and shall end at the conclusion of the immediately following ICANN annual meeting.

(c) Non-voting liaisons shall serve during the term designated by the entity that appoints them. The Chair, the Chair-Elect, and any Associate Chair shall serve as such until the conclusion of the next ICANN annual meeting.

(d) It is anticipated that upon the conclusion of the term of the Chair-Elect, the Chair-Elect will be appointed by the Board to the position of Chair. However, the Board retains the discretion to appoint any other person to the position of Chair. At the time of appointing a Chair-Elect, if the Board determines that the person identified to serve as Chair shall be appointed as Chair for a successive term, the Chair-Elect position shall remain vacant for the term designated by the Board.

(e) Vacancies in the positions of delegate, non-voting liaison, Chair or Chair-Elect shall be filled by the entity entitled to select the delegate, non-voting liaison, Chair or Chair-Elect involved. For any term that the Chair-Elect position is vacant

pursuant to Section 8.3(d), or until any other vacancy in the position of Chair-Elect can be filled, a non-voting advisor to the Chair may be appointed by the Board from among persons with prior service on the Board or a Nominating Committee, including the immediately previous Chair of the Nominating Committee. A vacancy in the position of Associate Chair may be filled by the Chair in accordance with the criteria established by Section 8.2(i).

(f) The existence of any vacancies shall not affect the obligation of the Nominating Committee to carry out the responsibilities assigned to it in these Bylaws.

Section 8.4. CRITERIA FOR SELECTION OF NOMINATING COMMITTEE DELEGATES

Delegates to the ICANN Nominating Committee shall be:

(a) Accomplished persons of integrity, objectivity, and intelligence, with reputations for sound judgment and open minds, and with experience and competence with collegial large group decision-making;

(b) Persons with wide contacts, broad experience in the Internet community, and a commitment to the success of ICANN;

(c) Persons whom the selecting body is confident will consult widely and accept input in carrying out their responsibilities;

(d) Persons who are neutral and objective, without any fixed personal commitments to particular individuals, organizations, or commercial objectives in carrying out their Nominating Committee responsibilities;

(e) Persons with an understanding of ICANN's mission and the potential impact of ICANN's activities on the broader Internet community who are willing to serve as volunteers, without compensation other than the reimbursement of certain expenses; and

(f) Persons who are able to work and communicate in written and spoken English.

Section 8.5. DIVERSITY

In carrying out its responsibilities to nominate Directors to fill Seats 1 through 8 (and selections to any other ICANN bodies as the Nominating Committee is responsible for under these Bylaws), the Nominating Committee shall take into account the continuing membership of the Board (and such other bodies), and seek to ensure that the persons it nominates to serve as Director and selects shall, to the extent feasible and consistent with the other criteria required to be

applied by Section 8.4, be guided by Section 1.2(b)(ii).

Section 8.6. ADMINISTRATIVE AND OPERATIONAL SUPPORT

ICANN shall provide administrative and operational support necessary for the Nominating Committee to carry out its responsibilities.

Section 8.7. PROCEDURES

The Nominating Committee shall adopt such operating procedures as it deems necessary, which shall be published on the Website.

Section 8.8. INELIGIBILITY FOR SELECTION BY NOMINATING COMMITTEE

No person who serves on the Nominating Committee in any capacity shall be eligible for nomination by any means to any position on the Board or any other ICANN body having one or more membership positions that the Nominating Committee is responsible for filling, until the conclusion of an ICANN annual meeting that coincides with, or is after, the conclusion of that person's service on the Nominating Committee.

Section 8.9. INELIGIBILITY FOR SERVICE ON NOMINATING COMMITTEE

No person who is an employee of or paid consultant to ICANN (including the Ombudsman) shall simultaneously serve in any of the Nominating Committee positions described in Section 8.2.

ARTICLE 9 ADDRESS SUPPORTING ORGANIZATION

Section 9.1. DESCRIPTION

(a) The Address Supporting Organization ("**Address Supporting Organization**" or "**ASO**") shall advise the Board with respect to policy issues relating to the operation, assignment, and management of Internet addresses.

(b) The ASO shall be the entity established by the Memorandum of Understanding entered on 21 October 2004 between ICANN and the Number Resource Organization ("**NRO**"), an organization of the existing RIRs.

Section 9.2. ADDRESS COUNCIL

(a) The ASO shall have an Address Council, consisting of the members of the NRO Number Council.

(b) The Address Council shall nominate individuals to fill Seats 9 and 10 on the Board. Notification of the Address Council's nominations shall be given by the Address Council in writing to the EC Administration, with a copy to the Secretary, and the EC shall promptly act on it as provided in Section 7.25.

ARTICLE 10 COUNTRY-CODE NAMES SUPPORTING ORGANIZATION

Section 10.1. DESCRIPTION

There shall be a policy-development body known as the Country-Code Names Supporting Organization ("**ccNSO**"), which shall be responsible for:

(a) developing and recommending to the Board global policies relating to country-code top-level domains;

(b) Nurturing consensus across the ccNSO's community, including the name-related activities of ccTLDs;

(c) Coordinating with other ICANN Supporting Organizations, committees, and constituencies under ICANN;

(d) Nominating individuals to fill Seats 11 and 12 on the Board; and

(e) Other responsibilities of the ccNSO as set forth in these Bylaws.

Policies that apply to ccNSO members by virtue of their membership are only those policies developed according to Section 10.4(j) and Section 10.4(k). However, the ccNSO may also engage in other activities authorized by its members. Adherence to the results of these activities will be voluntary and such activities may include: seeking to develop voluntary best practices for ccTLD managers, assisting in skills building within the global community of ccTLD managers, and enhancing operational and technical cooperation among ccTLD managers.

Section 10.2. ORGANIZATION

The ccNSO shall consist of (a) ccTLD managers that have agreed in writing to be members of the ccNSO (see Section 10.4(b)) and (b) a ccNSO Council responsible for managing the policy-development process of the ccNSO.

Section 10.3. ccNSO COUNCIL

(a) The ccNSO Council shall consist of three ccNSO Council members selected by the ccNSO members within each of ICANN's Geographic Regions in the manner described in Section 10.4(g) through Section 10.4(i); (ii) three ccNSO Council members selected by the ICANN Nominating Committee; (iii) liaisons as described in Section 10.3(b); and (iv) observers as described in Section 10.3(c).

(b) There shall also be one liaison to the ccNSO Council from each of the following organizations, to the extent they choose to appoint such a liaison: (i) the Governmental Advisory Committee; (ii) the At-Large Advisory Committee; and (iii) each of the Regional Organizations described in Section 10.5. These liaisons shall not be members of or entitled to vote on the ccNSO Council, but otherwise shall be entitled to participate on equal footing with members of the ccNSO Council. Appointments of liaisons shall be made by providing written notice to the ICANN Secretary, with a notification copy to the ccNSO Council Chair, and shall be for the term designated by the appointing organization as stated in the written notice. The appointing organization may recall from office or replace its liaison at any time by providing written notice of the recall or replacement to the ICANN Secretary, with a notification copy to the ccNSO Council Chair.

(c) The ccNSO Council may agree with the Council of any other ICANN Supporting Organization to exchange observers. Such observers shall not be members of or entitled to vote on the ccNSO Council, but otherwise shall be entitled to participate on equal footing with members of the ccNSO Council. The appointing Council may designate its observer (or revoke or change the designation of its observer) on the ccNSO Council at any time by providing written notice to the ICANN Secretary, with a notification copy to the ccNSO Council Chair.

(d) (i) the regular term of each ccNSO Council member shall begin at the conclusion of an ICANN annual meeting and shall end at the conclusion of the third ICANN annual meeting thereafter; (ii) the regular terms of the three ccNSO Council members selected by the ccNSO members within each ICANN Geographic Region shall be staggered so that one member's term begins in a year divisible by three, a second member's term begins in the first year following a year divisible by three, and the third member's term begins in the second year following a year divisible by three; and (iii) the regular terms of the three ccNSO Council members selected by the Nominating Committee shall be staggered in the same manner. Each ccNSO Council member shall hold office during his or her regular term and until a successor has been selected and qualified or until that member resigns or is removed in accordance with these Bylaws.

(e) A ccNSO Council member may resign at any time by giving written notice to the ICANN Secretary, with a notification copy to the ccNSO Council Chair.

(f) ccNSO Council members may be removed for not attending three consecutive meetings of the ccNSO Council without sufficient cause or for grossly inappropriate behavior, both as determined by at least a 66% vote of all of the members of the ccNSO Council.

(g) A vacancy on the ccNSO Council shall be deemed to exist in the case of the death, resignation, or removal of any ccNSO Council member. Vacancies in the positions of the three members selected by the Nominating Committee shall be filled for the unexpired term involved by the Nominating Committee giving the ICANN Secretary written notice of its selection, with a notification copy to the ccNSO Council Chair. Vacancies in the positions of the ccNSO Council members selected by ccNSO members shall be filled for the unexpired term by the procedure described in Section 10.4(g) through (i).

(h) The role of the ccNSO Council is to administer and coordinate the affairs of the ccNSO (including coordinating meetings, including an annual meeting, of ccNSO members as described in Section 10.4(f)) and to manage the development of policy recommendations in accordance with Section 10.6(a). The ccNSO Council shall also undertake such other roles as the members of the ccNSO shall decide from time to time.

(i) The ccNSO Council shall nominate individuals to fill Seats 11 and 12 on the Board by written ballot or by action at a meeting; any such nomination must have affirmative votes of a majority of all the members of the ccNSO Council then in office. Notification of the ccNSO Council's nominations shall be given by the ccNSO Council Chair in writing to the EC Administration, with a copy to the Secretary, and the EC shall promptly act on it as provided in Section 7.25.

(j) The ccNSO Council shall select from among its members the ccNSO Council Chair and such Vice Chair(s) as it deems appropriate. Selections of the ccNSO Council Chair and Vice Chair(s) shall be by written ballot or by action at a meeting; any such selection must have affirmative votes of a majority of all the members of the ccNSO Council then in office. The term of office of the ccNSO Council Chair and any Vice Chair(s) shall be as specified by the ccNSO Council at or before the time the selection is made. The ccNSO Council Chair or any Vice Chair(s) may be recalled from office by the same procedure as used for selection.

(k) The ccNSO Council, subject to direction by the ccNSO members, shall adopt such rules and procedures for the ccNSO as it deems necessary, provided they are consistent with these Bylaws. Rules for ccNSO membership and operating procedures adopted by the ccNSO Council shall be published on the Website.

(l) Except as provided by Section 10.3(i) and Section 10.3(j), the ccNSO Council shall act at meetings. The ccNSO Council shall meet regularly on a schedule it determines, but not fewer than four times each calendar year. At the discretion of the ccNSO Council, meetings may be held in person or by other means, provided that all ccNSO Council members are permitted to participate by at least one means described in Section 10.3(n). Except where determined by a majority vote of the members of the ccNSO Council present that a closed session is appropriate, physical meetings shall be open to attendance by all interested persons. To the extent practicable, ccNSO Council meetings should be held in conjunction with meetings of the Board, or of one or more of ICANN's other Supporting Organizations.

(m) Notice of time and place (and information about means of participation other than personal attendance) of all meetings of the ccNSO Council shall be provided to each ccNSO Council member, liaison, and observer by e-mail, telephone, facsimile, or a paper notice delivered personally or by postal mail. In case the notice is sent by postal mail, it shall be sent at least 21 days before the day of the meeting. In case the notice is delivered personally or by telephone, facsimile, or e-mail it shall be provided at least seven days before the day of the meeting. At least seven days in advance of each ccNSO Council meeting (or if not practicable, as far in advance as is practicable), a notice of such meeting and, to the extent known, an agenda for the meeting shall be posted.

(n) Members of the ccNSO Council may participate in a meeting of the ccNSO Council through personal attendance or use of electronic communication (such as telephone or video conference), provided that (i) all ccNSO Council members participating in the meeting can speak to and hear one another, (ii) all ccNSO Council members participating in the meeting are provided the means of fully participating in all matters before the ccNSO Council, and (iii)there is a reasonable means of verifying the identity of ccNSO Council members participating in the meeting and their votes. A majority of the ccNSO Council members (i.e. those entitled to vote) then in office shall constitute a quorum for the transaction of business, and actions by a majority vote of the ccNSO Council members present at any meeting at which there is a quorum shall be actions of the ccNSO Council, unless otherwise provided in these Bylaws. The ccNSO Council shall transmit minutes of its meetings to the ICANN Secretary, who shall cause those minutes to be posted to the Website as soon as practicable following the meeting, and no later than 21 days following the meeting.

Section 10.4. MEMBERSHIP

(a) The ccNSO shall have a membership consisting of ccTLD managers. Any ccTLD manager that meets the membership qualifications stated in Section

10.4(b) shall be entitled to be members of the ccNSO. For purposes of this Article 10, a ccTLD manager is the organization or entity responsible for managing an ISO 3166 country-code top-level domain, or under any later variant, for that country-code top-level domain.

(b) Any ccTLD manager may become a ccNSO member by submitting an application to a person designated by the ccNSO Council to receive applications. The application shall be in writing in a form designated by the ccNSO Council. The application shall include the ccTLD manager's recognition of the role of the ccNSO within the ICANN structure as well as the ccTLD manager's agreement, for the duration of its membership in the ccNSO, (i) to adhere to rules of the ccNSO, including membership rules, (ii) to abide by policies developed and recommended by the ccNSO and adopted by the Board in the manner described by Section 10.4(j) and Section 10.4(k), and (ii) to pay ccNSO membership fees established by the ccNSO Council under Section 10.7(c). A ccNSO member may resign from membership at any time by giving written notice to a person designated by the ccNSO Council to receive notices of resignation. Upon resignation the ccTLD manager ceases to agree to (A)adhere to rules of the ccNSO, including membership rules, (B) to abide by policies developed and recommended by the ccNSO and adopted by the Board in the manner described by Section 10.4(j) and Section 10.4(k), and (C) to pay ccNSO membership fees established by the ccNSO Council under Section 10.7(c). In the absence of designation by the ccNSO Council of a person to receive applications and notices of resignation, they shall be sent to the ICANN Secretary, who shall notify the ccNSO Council of receipt of any such applications and notices.

(c) Neither membership in the ccNSO nor membership in any Regional Organization described in Section 10.5 shall be a condition for access to or registration in the IANA database. Any individual relationship a ccTLD manager has with ICANN or the ccTLD manager's receipt of IANA services is not in any way contingent upon membership in the ccNSO.

(d) The Geographic Regions of ccTLDs shall be as described in Section 7.5. For purposes of this Article 10, managers of ccTLDs within a Geographic Region that are members of the ccNSO are referred to as ccNSO members "within" the Geographic Region, regardless of the physical location of the ccTLD manager. In cases where the Geographic Region of a ccNSO member is unclear, the ccTLD member should self-select according to procedures adopted by the ccNSO Council.

(e) Each ccTLD manager may designate in writing a person, organization, or entity to represent the ccTLD manager. In the absence of such a designation, the ccTLD manager shall be represented by the person, organization, or entity listed as the administrative contact in the IANA database.

(f) There shall be an annual meeting of ccNSO members, which shall be coordinated by the ccNSO Council. Annual meetings should be open for all to attend, and a reasonable opportunity shall be provided for ccTLD managers that are not members of the ccNSO as well as other non-members of the ccNSO to address the meeting. To the extent practicable, annual meetings of the ccNSO members shall be held in person and should be held in conjunction with meetings of the Board, or of one or more of ICANN's other Supporting Organizations.

(g) The ccNSO Council members selected by the ccNSO members from each Geographic Region (see Section 10.3(a)(i)) shall be selected through nomination, and if necessary election, by the ccNSO members within that Geographic Region. At least 90 days before the end of the regular term of any ccNSO-member-selected member of the ccNSO Council, or upon the occurrence of a vacancy in the seat of such a ccNSO Council member, the ccNSO Council shall establish a nomination and election schedule, which shall be sent to all ccNSO members within the Geographic Region and posted on the Website.

(h) Any ccNSO member may nominate an individual to serve as a ccNSO Council member representing the ccNSO member's Geographic Region. Nominations must be seconded by another ccNSO member from the same Geographic Region. By accepting their nomination, individuals nominated to the ccNSO Council agree to support the policies committed to by ccNSO members.

(i) If at the close of nominations there are no more candidates nominated (with seconds and acceptances) in a particular Geographic Region than there are seats on the ccNSO Council available for that Geographic Region, then the nominated candidates shall be selected to serve on the ccNSO Council. Otherwise, an election by written ballot (which may be by e-mail) shall be held to select the ccNSO Council members from among those nominated (with seconds and acceptances), with ccNSO members from the Geographic Region being entitled to vote in the election through their designated representatives. In such an election, a majority of all ccNSO members in the Geographic Region entitled to vote shall constitute a quorum, and the selected candidate must receive the votes of a majority of those cast by ccNSO members within the Geographic Region. The ccNSO Council Chair shall provide the ICANN Secretary prompt written notice of the selection of ccNSO Council members under this paragraph.

(j) Subject to Section 10.4(k), ICANN policies shall apply to ccNSO members by virtue of their membership to the extent, and only to the extent, that the policies (i) only address issues that are within scope of the ccNSO according to Section 10.6(a) and Annex C; (ii) have been developed through the ccPDP as described in Section 10.6, and (iii) have been recommended as such by the ccNSO to the Board, and (iv) are adopted by the Board as policies, provided that such policies

do not conflict with the law applicable to the ccTLD manager which shall, at all times, remain paramount. In addition, such policies shall apply to ICANN in its activities concerning ccTLDs.

(k) A ccNSO member shall not be bound if it provides a declaration to the ccNSO Council stating that (i) implementation of the policy would require the member to breach custom, religion, or public policy (not embodied in the applicable law described in Section 10.4(j)), and (ii) failure to implement the policy would not impair DNS operations or interoperability, giving detailed reasons supporting its statements. After investigation, the ccNSO Council will provide a response to the ccNSO member's declaration. If there is a ccNSO Council consensus disagreeing with the declaration, which may be demonstrated by a vote of 14 or more members of the ccNSO Council, the response shall state the ccNSO Council's disagreement with the declaration and the reasons for disagreement. Otherwise, the response shall state the ccNSO Council's agreement with the declaration. If the ccNSO Council disagrees, the ccNSO Council shall review the situation after a six-month period. At the end of that period, the ccNSO Council shall make findings as to (A) whether the ccNSO members' implementation of the policy would require the member to breach custom, religion, or public policy (not embodied in the applicable law described in Section 10.4(j)) and (B) whether failure to implement the policy would impair DNS operations or interoperability. In making any findings disagreeing with the declaration, the ccNSO Council shall proceed by consensus, which may be demonstrated by a vote of 14 or more members of the ccNSO Council.

Section 10.5. REGIONAL ORGANIZATIONS

The ccNSO Council may designate a Regional Organization for each ICANN Geographic Region, provided that the Regional Organization is open to full membership by all ccNSO members within the Geographic Region. Decisions to designate or de-designate a Regional Organization shall require a 66% vote of all of the members of the ccNSO Council and shall be subject to review according to procedures established by the Board.

Section 10.6. ccNSO POLICY-DEVELOPMENT PROCESS AND SCOPE

(a) The scope of the ccNSO's policy-development role shall be as stated in Annex C to these Bylaws; any modifications to the scope shall be recommended to the Board by the ccNSO by use of the procedures of the ccPDP, and shall be subject to approval by the Board.

(b) In developing global policies within the scope of the ccNSO and

recommending them to the Board, the ccNSO shall follow the ccNSO Policy-Development Process ("**ccPDP**"). The ccPDP shall be as stated in Annex B to these Bylaws; modifications shall be recommended to the Board by the ccNSO by use of the procedures of the ccPDP, and shall be subject to approval by the Board.

Section 10.7. STAFF SUPPORT AND FUNDING

(a) Upon request of the ccNSO Council, a member of the ICANN staff may be assigned to support the ccNSO and shall be designated as the ccNSO Staff Manager. Alternatively, the ccNSO Council may designate, at ccNSO expense, another person to serve as ccNSO Staff Manager. The work of the ccNSO Staff Manager on substantive matters shall be assigned by the Chair of the ccNSO Council, and may include the duties of ccPDP Issue Manager.

(b) Upon request of the ccNSO Council, ICANN shall provide administrative and operational support necessary for the ccNSO to carry out its responsibilities. Such support shall not include an obligation for ICANN to fund travel expenses incurred by ccNSO participants for travel to any meeting of the ccNSO or for any other purpose. The ccNSO Council may make provision, at ccNSO expense, for administrative and operational support in addition or as an alternative to support provided by ICANN.

(c) The ccNSO Council shall establish fees to be paid by ccNSO members to defray ccNSO expenses as described in Section 10.7(a) and Section 10.7(b), as approved by the ccNSO members.

(d) Written notices given to the Secretary under this Article 10 shall be permanently retained, and shall be made available for review by the ccNSO Council on request. The Secretary shall also maintain the roll of members of the ccNSO, which shall include the name of each ccTLD manager's designated representative, and which shall be posted on the Website.

ARTICLE 11 GENERIC NAMES SUPPORTING ORGANIZATION

Section 11.1. DESCRIPTION

There shall be a policy-development body known as the Generic Names Supporting Organization (the "**Generic Names Supporting Organization**" or "**GNSO**", and collectively with the ASO and ccNSO, the "**Supporting Organizations**")), which shall be responsible for developing and recommending to the Board substantive policies relating to generic top-level domains and other responsibilities of the GNSO as set forth in these Bylaws.

Section 11.2. ORGANIZATION

The GNSO shall consist of:

(a) A number of Constituencies, where applicable, organized within the Stakeholder Groups as described in Section 11.5;

(b) Four Stakeholder Groups organized within Houses as described in Section 11.5;

(c) Two Houses within the GNSO Council as described in Section 11.3(h);

(d) A GNSO Council responsible for managing the policy development process of the GNSO, as described in Section 11.3; and

(e) Except as otherwise defined in these Bylaws, the four Stakeholder Groups and the Constituencies will be responsible for defining their own charters with the approval of their members and of the Board.

Section 11.3. GNSO COUNCIL

(a) Subject to Section 11.5, the GNSO Council shall consist of:

> (i) three representatives selected from the Registries Stakeholder Group;
>
> (ii) three representatives selected from the Registrars Stakeholder Group;
>
> (iii) six representatives selected from the Commercial Stakeholder Group;
>
> (iv) six representatives selected from the Non-Commercial Stakeholder Group; and
>
> (v) three representatives selected by the ICANN Nominating Committee, one of which shall be non-voting, but otherwise entitled to participate on equal footing with other members of the GNSO Council including, e.g. the making and seconding of motions and of serving as Chair if elected. One Nominating Committee appointee voting representative shall be assigned to each House (as described in Section 11.3(h)) by the Nominating Committee.

No individual representative may hold more than one seat on the GNSO Council

at the same time.

Stakeholder Groups should, in their charters, ensure their representation on the GNSO Council is as diverse as possible and practicable, including considerations of geography, GNSO Constituency, sector, ability and gender.

There may also be liaisons to the GNSO Council from other ICANN Supporting Organizations and/or Advisory Committees, from time to time. The appointing organization shall designate, revoke, or change its liaison on the GNSO Council by providing written notice to the Chair of the GNSO Council and to the ICANN Secretary. Liaisons shall not be members of or entitled to vote, to make or second motions, or to serve as an officer on the GNSO Council, but otherwise liaisons shall be entitled to participate on equal footing with members of the GNSO Council.

(b) The regular term of each GNSO Council member shall begin at the conclusion of an ICANN annual meeting and shall end at the conclusion of the second ICANN annual meeting thereafter. The regular term of two representatives selected from Stakeholder Groups with three Council seats shall begin in even-numbered years and the regular term of the other representative selected from that Stakeholder Group shall begin in odd-numbered years. The regular term of three representatives selected from Stakeholder Groups with six Council seats shall begin in even-numbered years and the regular term of the other three representatives selected from that Stakeholder Group shall begin in odd-numbered years. The regular term of one of the three members selected by the Nominating Committee shall begin in even-numbered years and the regular term of the other two of the three members selected by the Nominating Committee shall begin in odd-numbered years. Each GNSO Council member shall hold office during his or her regular term and until a successor has been selected and qualified or until that member resigns or is removed in accordance with these Bylaws.

Except in a "special circumstance," such as, but not limited to, meeting geographic or other diversity requirements defined in the Stakeholder Group charters, where no alternative representative is available to serve, no Council member may be selected to serve more than two consecutive terms, in such a special circumstance a Council member may serve one additional term. For these purposes, a person selected to fill a vacancy in a term shall not be deemed to have served that term. A former Council member who has served two consecutive terms must remain out of office for one full term prior to serving any subsequent term as Council member. A "special circumstance" is defined in the GNSO Operating Procedures.

(c) A vacancy on the GNSO Council shall be deemed to exist in the case of the

death, resignation, or removal of any member. Vacancies shall be filled for the unexpired term by the appropriate Nominating Committee or Stakeholder Group that selected the member holding the position before the vacancy occurred by giving the GNSO Secretariat written notice of its selection. Procedures for handling Stakeholder Group-appointed GNSO Council member vacancies, resignations, and removals are prescribed in the applicable Stakeholder Group Charter.

A GNSO Council member selected by the Nominating Committee may be removed for cause: (i) stated by a three-fourths (3/4) vote of all members of the applicable House to which the Nominating Committee appointee is assigned; or (ii) stated by a three-fourths (3/4) vote of all members of each House in the case of the non-voting Nominating Committee appointee (see Section 11.3(h)). Such removal shall be subject to reversal by the ICANN Board on appeal by the affected GNSO Council member.

(d) The GNSO Council is responsible for managing the policy development process of the GNSO. It shall adopt such procedures (the "**GNSO Operating Procedures**") as it sees fit to carry out that responsibility, provided that such procedures are approved by a majority vote of each House. The GNSO Operating Procedures shall be effective upon the expiration of a twenty-one (21) day public comment period, and shall be subject to Board oversight and review. Until any modifications are recommended by the GNSO Council, the applicable procedures shall be as set forth in Section 11.6.

(e) No more than one officer, director or employee of any particular corporation or other organization (including its subsidiaries and affiliates) shall serve on the GNSO Council at any given time.

(f) The GNSO shall nominate by written ballot or by action at a meeting individuals to fill Seats 13 and 14 on the Board. Each of the two voting Houses of the GNSO, as described in Section 11.3(h), shall make a nomination to fill one of two Board seats, as outlined below; any such nomination must have affirmative votes compromising sixty percent (60%) of all the respective voting House members:

> (i) the Contracted Parties House (as described in Section 11.3(h)(i)) shall select a representative to fill Seat 13; and
>
> (ii) the Non-Contracted Parties House (as described in Section 11.3(h)(ii)) shall select a representative to fill Seat 14.

Election procedures are defined in the GNSO Operating Procedures.

Notification of the Board seat nominations shall be given by the GNSO Chair in writing to the EC Administration, with a copy to the Secretary, and the EC shall promptly act on it as provided in Section 7.25.

(g) The GNSO Council shall select the GNSO Chair for a term the GNSO Council specifies, but not longer than one year. Each House (as described in Section 11.3(h)) shall select a Vice-Chair, who will be a Vice-Chair of the whole of the GNSO Council, for a term the GNSO Council specifies, but not longer than one year. The procedures for selecting the Chair and any other officers are contained in the GNSO Operating Procedures. In the event that the GNSO Council has not elected a GNSO Chair by the end of the previous Chair's term, the Vice-Chairs will serve as Interim GNSO Co-Chairs until a successful election can be held.

(h) Except as otherwise required in these Bylaws, for voting purposes, the GNSO Council (see Section 11.3(a)) shall be organized into a bicameral House structure as described below:

> (i) the Contracted Parties House includes the Registries Stakeholder Group (three members), the Registrars Stakeholder Group (three members), and one voting member appointed by the ICANN Nominating Committee for a total of seven voting members; and
>
> (ii) the Non Contracted Parties House includes the Commercial Stakeholder Group (six members), the Non-Commercial Stakeholder Group (six members), and one voting member appointed by the ICANN Nominating Committee to that House for a total of thirteen voting members.

Except as otherwise specified in these Bylaws, each member of a voting House is entitled to cast one vote in each separate matter before the GNSO Council.

(i) Except as otherwise specified in these Bylaws, Annex A, Annex A-1 or Annex A-2 hereto, or the GNSO Operating Procedures, the default threshold to pass a GNSO Council motion or other voting action requires a simple majority vote of each House. The voting thresholds described below shall apply to the following GNSO actions:

> (i) Create an Issues Report: requires an affirmative vote of more than one-fourth (1/4) vote of each House or majority of one House.

(ii) Initiate a Policy Development Process ("**PDP**") Within Scope (as described in Annex A): requires an affirmative vote of more than one-third (1/3) of each House or more than two-thirds (2/3) of one House.

(iii) Initiate a PDP Not Within Scope: requires an affirmative vote of GNSO Supermajority (as defined in Section 11.3(i)(xix)).

(iv) Approve a PDP Team Charter for a PDP Within Scope: requires an affirmative vote of more than one-third (1/3) of each House or more than two-thirds (2/3) of one House.

(v) Approve a PDP Team Charter for a PDP Not Within Scope: requires an affirmative vote of a GNSO Supermajority.

(vi) Changes to an Approved PDP Team Charter: For any PDP Team Charter approved under (iv) or (v) above, the GNSO Council may approve an amendment to the Charter through a simple majority vote of each House.

(vii) Terminate a PDP: Once initiated, and prior to the publication of a Final Report, the GNSO Council may terminate a PDP only for significant cause, upon a motion that passes with a GNSO Supermajority Vote in favor of termination.

(viii) Approve a PDP Recommendation Without a GNSO Supermajority: requires an affirmative vote of a majority of each House and further requires that one GNSO Council member representative of at least 3 of the 4 Stakeholder Groups supports the Recommendation.

(ix) Approve a PDP Recommendation With a GNSO Supermajority: requires an affirmative vote of a GNSO Supermajority,

(x) Approve a PDP Recommendation Imposing New Obligations on Certain Contracting Parties: where an ICANN contract provision specifies that "a two-thirds vote of the council" demonstrates the presence of a consensus, the GNSO Supermajority vote threshold will have to be met or exceeded.

(xi) Modification of Approved PDP Recommendation: Prior to Final Approval by the Board, an Approved PDP Recommendation may be modified or amended by the GNSO Council with a GNSO Supermajority vote.

(xii) Initiation of an Expedited Policy Development Process ("**EPDP**"): requires an affirmative vote of a GNSO Supermajority.

(xiii) Approve an EPDP Team Charter: requires an affirmative vote of a

GNSO Supermajority.

(xiv) Approval of EPDP Recommendations: requires an affirmative vote of a GNSO Supermajority.

(xv) Approve an EPDP Recommendation Imposing New Obligations on Certain Contracting Parties: where an ICANN contract provision specifies that "a two-thirds vote of the council" demonstrates the presence of a consensus, the GNSO Supermajority vote threshold will have to be met or exceeded.

(xvi) Initiation of a GNSO Guidance Process ("**GGP**"): requires an affirmative vote of more than one-third (1/3) of each House or more than two-thirds (2/3) of one House.

(xvii) Rejection of Initiation of a GGP Requested by the Board: requires an affirmative vote of a GNSO Supermajority.

(xviii) Approval of GGP Recommendations: requires an affirmative vote of a GNSO Supermajority.

(xix) A "**GNSO Supermajority**" shall mean: (A) two-thirds (2/3) of the Council members of each House, or (B) three-fourths (3/4) of the Council members of one House and a majority of the Council members of the other House.

(j) The voting thresholds described below shall apply to the following GNSO actions as a Decisional Participant in the Empowered Community. For any action not listed, the default threshold for the GNSO to act as a Decisional Participant in the Empowered community requires a simple majority vote of each House:

(i) Amendment of PTI Articles of Incorporation as contemplated in Section 16.2: requires an affirmative vote of a GNSO Supermajority.

(ii) GNSO Council Inspection Request as contemplated in Section 22.7: requires an affirmative vote of more than one-fourth (1/4) vote of each House or majority of one House.

(iii) GNSO Council Inspection Remedy, as contemplated in Section 22.7 - e, and Stakeholder Group / Constituency Inspection Remedy, as contemplated in Section 22.7 – e(ii) and e(iii), for an inspection requested by the GNSO as a Decisional Participant in the Empowered Community: requires an

affirmative vote of more than one-fourth (1/4) vote of each House or majority of one House.

(iv) Amendments to Fundamental Bylaws and Article Amendments as contemplated by Section 25.2 of the Bylaws, Asset Sales, as contemplated by Article 26 of the Bylaws, amendments to ICANN Articles of Incorporation: requires an affirmative vote of a GNSO Supermajority.

(v) Approval of a Nominating Committee Director Removal Petition as contemplated in Annex D, Article 3, Section 3.1(b) and support for a petition submitted by a Petitioning Decisional Participant as contemplated in Section 3.2(d): requires an affirmative vote of a GNSO Supermajority.

(vi) Approval of a Nominating Committee Director Removal Supported Petition as contemplated in Annex D, Article 3, Section 3.1(f): requires an affirmative vote of a GNSO Supermajority.

(vii) Approval of a petition to remove a director holding seat 13 or 14 as contemplated in Annex D, Article 3, Section 3.2(a): requires an affirmative vote of at least three-fourths (3/4) of the House that appointed that Director.

(viii) Approval of a petition notice to remove a director holding seat 13 or 14 as contemplated in Annex D, Article 3, Section 3.2(f): requires an affirmative vote of at least three-fourths (3/4) of the GNSO Council and at least three-fourths (3/4) of the House that appointed that Director.

(ix) Approval of a Board Recall Petition as contemplated in Annex D, Article 3, Section 3.3(b) and support for another Petitioning Decisional Participant: requires an affirmative vote of a GNSO Supermajority.

(x) Approval of a Board Recall Supported Petition as contemplated in Annex D, Article 3, Section 3.3(e): requires an affirmative vote of a GNSO Supermajority.

Section 11.4. STAFF SUPPORT AND FUNDING

(a) A member of the ICANN staff shall be assigned to support the GNSO, whose work on substantive matters shall be assigned by the Chair of the GNSO Council, and shall be designated as the GNSO Staff Manager ("**Staff Manager**").

(b) ICANN shall provide administrative and operational support necessary for the GNSO to carry out its responsibilities. Such support shall not include an obligation for ICANN to fund travel expenses incurred by GNSO participants for travel to any

meeting of the GNSO or for any other purpose. ICANN may, at its discretion, fund travel expenses for GNSO participants under any travel support procedures or guidelines that it may adopt from time to time.

Section 11.5. STAKEHOLDER GROUPS

(a) The following "**Stakeholder Groups**" are hereby recognized as representative of a specific group of one or more "**Constituencies**" or interest groups:

> (i) Registries Stakeholder Group representing all gTLD registries under contract to ICANN;
>
> (ii) Registrars Stakeholder Group representing all registrars accredited by and under contract to ICANN;
>
> (iii) Commercial Stakeholder Group representing the full range of large and small commercial entities of the Internet ("**Commercial Stakeholder Group**"), which includes the Business Constituency ("**Business Constituency**"), Intellectual Property Constituency ("**Intellectual Property Constituency**") and the Internet Service Providers and Connectivity Providers Constituency ("**Internet Service Providers and Connectivity Providers Constituency**"); and
>
> (iv) Non-Commercial Stakeholder Group representing the full range of non-commercial entities of the Internet.

(b) Each Stakeholder Group is assigned a specific number of GNSO Council seats in accordance with Section 11.3(a).

(c) Each Stakeholder Group identified in Section 11.3(a) and each of its associated Constituencies, where applicable, shall maintain recognition with the ICANN Board. Recognition is granted by the Board based upon the extent to which, in fact, the entity represents the global interests of the stakeholder communities it purports to represent and operates to the maximum extent feasible in an open and transparent manner consistent with procedures designed to ensure fairness. Stakeholder Group and Constituency Charters may be reviewed periodically as prescribed by the Board.

(d) Any group of individuals or entities may petition the Board for recognition as a new or separate Constituency in the Non-Contracted Parties House. Any such petition shall contain:

(i) A detailed explanation of why the addition of such a Constituency will improve the ability of the GNSO to carry out its policy-development responsibilities;

(ii) A detailed explanation of why the proposed new Constituency adequately represents, on a global basis, the stakeholders it seeks to represent;

(iii) A recommendation for organizational placement within a particular Stakeholder Group; and

(iv) A proposed charter that adheres to the principles and procedures contained in these Bylaws.

Any petition for the recognition of a new Constituency and the associated charter shall be posted for public comment.

(e) The Board may create new Constituencies as described in Section 11.5(c) in response to such a petition, or on its own motion, if the Board determines that such action would serve the purposes of ICANN. In the event the Board is considering acting on its own motion it shall post a detailed explanation of why such action is necessary or desirable, set a reasonable time for public comment, and not make a final decision on whether to create such new Constituency until after reviewing all comments received. Whenever the Board posts a petition or recommendation for a new Constituency for public comment, the Board shall notify the GNSO Council and the appropriate Stakeholder Group affected and shall consider any response to that notification prior to taking action.

Section 11.6. POLICY DEVELOPMENT PROCESS

The policy-development procedures to be followed by the GNSO shall be as stated in Annex A to these Bylaws. These procedures may be supplemented or revised in the manner stated in Section 11.3(d).

ARTICLE 12 ADVISORY COMMITTEES

Section 12.1. GENERAL

The Board may create one or more "**Advisory Committees**" in addition to those set forth in this Article 12. Advisory Committee membership may consist of Directors only, Directors and non-directors, or non-directors only, and may also

include non-voting or alternate members. Advisory Committees shall have no legal authority to act for ICANN, but shall report their findings and recommendations to the Board.

Section 12.2. SPECIFIC ADVISORY COMMITTEES

There shall be at least the following Advisory Committees:

(a) Governmental Advisory Committee

(i) The Governmental Advisory Committee should consider and provide advice on the activities of ICANN as they relate to concerns of governments, particularly matters where there may be an interaction between ICANN's policies and various laws and international agreements or where they may affect public policy issues.

(ii) Membership in the Governmental Advisory Committee shall be open to all national governments. Membership shall also be open to Distinct Economies as recognized in international fora, and multinational governmental organizations and treaty organizations, on the invitation of the Governmental Advisory Committee through its Chair.

(iii) The Governmental Advisory Committee may adopt its own charter and internal operating principles or procedures to guide its operations, to be published on the Website.

(iv) The chair of the Governmental Advisory Committee shall be elected by the members of the Governmental Advisory Committee pursuant to procedures adopted by such members.

(v) Each member of the Governmental Advisory Committee shall appoint one accredited representative to the Governmental Advisory Committee. The accredited representative of a member must hold a formal official position with the member's public administration. The term "official" includes a holder of an elected governmental office, or a person who is employed by such government, public authority, or multinational governmental or treaty organization and whose primary function with such government, public authority, or organization is to develop or influence governmental or public policies.

(vi) The Governmental Advisory Committee shall annually appoint one Liaison to the Board, without limitation on reappointment, and shall annually appoint one non-voting liaison to the ICANN Nominating Committee.

(vii) The Governmental Advisory Committee may designate a non-voting liaison to each of the Supporting Organization Councils and Advisory Committees, to the extent the Governmental Advisory Committee deems it appropriate and useful to do so.

(viii) The Board shall notify the Chair of the Governmental Advisory Committee in a timely manner of any proposal raising public policy issues on which it or any of the Supporting Organizations or Advisory Committees seeks public comment, and shall take duly into account any timely response to that notification prior to taking action.

(ix) The Governmental Advisory Committee may put issues to the Board directly, either by way of comment or prior advice, or by way of specifically recommending action or new policy development or revision to existing policies.

(x) The advice of the Governmental Advisory Committee on public policy matters shall be duly taken into account, both in the formulation and adoption of policies. In the event that the Board determines to take an action that is not consistent with Governmental Advisory Committee advice, it shall so inform the Governmental Advisory Committee and state the reasons why it decided not to follow that advice. Any Governmental Advisory Committee advice approved by a full Governmental Advisory Committee consensus, understood to mean the practice of adopting decisions by general agreement in the absence of any formal objection ("**GAC Consensus Advice**"), may only be rejected by a vote of no less than 60% of the Board, and the Governmental Advisory Committee and the Board will then try, in good faith and in a timely and efficient manner, to find a mutually acceptable solution. The Governmental Advisory Committee will state whether any advice it gives to the Board is GAC Consensus Advice.

(xi) If GAC Consensus Advice is rejected by the Board pursuant to Section 12.2(a)(x) and if no such mutually acceptable solution can be found, the Board will state in its final decision the reasons why the Governmental Advisory Committee advice was not followed, and such statement will be without prejudice to the rights or obligations of Governmental Advisory Committee members with regard to public policy issues falling within their responsibilities.

(b) Security and Stability Advisory Committee

(i) The role of the Security and Stability Advisory Committee ("**Security and Stability Advisory Committee**" or "**SSAC**") is to advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. It shall have the following responsibilities:

(A) To communicate on security matters with the Internet technical community and the operators and managers of critical DNS infrastructure services, to include the root name server operator community, the top-level domain registries and registrars, the operators of the reverse delegation trees such as in-addr.arpa and ip6.arpa, and others as events and developments dictate. The SSAC shall gather and articulate requirements to offer to those engaged in technical revision of the protocols related to DNS and address allocation and those engaged in operations planning.

(B) To engage in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and to advise the ICANN community accordingly. The SSAC shall recommend any necessary audit activity to assess the current status of DNS and address allocation security in relation to identified risks and threats.

(C) To communicate with those who have direct responsibility for Internet naming and address allocation security matters (IETF, RSSAC (as defined in Section 12.2(c)(i)), RIRs, name registries, etc.), to ensure that its advice on security risks, issues, and priorities is properly synchronized with existing standardization, deployment, operational, and coordination activities. The SSAC shall monitor these activities and inform the ICANN community and Board on their progress, as appropriate.

(D) To report periodically to the Board on its activities.

(E) To make policy recommendations to the ICANN community and Board.

(ii) The SSAC's chair and members shall be appointed by the Board. SSAC membership appointment shall be for a three-year term, commencing on 1 January and ending the second year thereafter on 31 December. The chair and members may be re-appointed, and there are no limits to the number of terms the chair or members may serve. The SSAC chair may provide recommendations to the Board regarding appointments to the SSAC. The SSAC chair shall stagger appointment recommendations so that approximately one-third (1/3) of the membership of the SSAC is considered for appointment or re-appointment each year. The Board shall also have the power to remove SSAC appointees as recommended by or in consultation

with the SSAC.

(iii) The SSAC shall annually appoint a Liaison to the Board according to Section 7.9.

(c) Root Server System Advisory Committee

(i) The role of the Root Server System Advisory Committee ("**Root Server System Advisory Committee**" or "**RSSAC**") is to advise the ICANN community and Board on matters relating to the operation, administration, security, and integrity of the Internet's Root Server System. It shall have the following responsibilities:

(A) Communicate on matters relating to the operation of the Root Servers and their multiple instances with the Internet technical community and the ICANN community. The RSSAC shall gather and articulate requirements to offer to those engaged in technical revision of the protocols and best common practices related to the operation of DNS servers.

(B) Communicate on matters relating to the administration of the Root Zone with those who have direct responsibility for that administration. These matters include the processes and procedures for the production of the Root Zone File.

(C) Engage in ongoing threat assessment and risk analysis of the Root Server System and recommend any necessary audit activity to assess the current status of root servers and the root zone.

(D) Respond to requests for information or opinions from the Board.

(E) Report periodically to the Board on its activities.

(F) Make policy recommendations to the ICANN community and Board.

(ii) The RSSAC shall be led by two co-chairs. The RSSAC's chairs and members shall be appointed by the Board.

(A) RSSAC membership appointment shall be for a three-year term, commencing on 1 January and ending the second year thereafter on 31 December. Members may be re-appointed, and there are no limits to the number of terms the members may serve. The RSSAC chairs shall provide recommendations to the Board regarding appointments to the RSSAC. If

the Board declines to appoint a person nominated by the RSSAC, then it will provide the rationale for its decision. The RSSAC chairs shall stagger appointment recommendations so that approximately one-third (1/3) of the membership of the RSSAC is considered for appointment or re-appointment each year. The Board shall also have the power to remove RSSAC appointees as recommended by or in consultation with the RSSAC.

(B) The RSSAC shall recommend the appointment of the chairs to the Board following a nomination process that it devises and documents.

(iii) The RSSAC shall annually appoint a Liaison to the Board according to Section 7.9.

(d) At-Large Advisory Committee

(i) The At-Large Advisory Committee ("**At-Large Advisory Committee**" or "**ALAC**") is the primary organizational home within ICANN for individual Internet users. The role of the ALAC shall be to consider and provide advice on the activities of ICANN, insofar as they relate to the interests of individual Internet users. This includes policies created through ICANN's Supporting Organizations, as well as the many other issues for which community input and advice is appropriate. The ALAC, which plays an important role in ICANN's accountability mechanisms, also coordinates some of ICANN's outreach to individual Internet users.

(ii) The ALAC shall consist of (A) two members selected by each of the Regional At-Large Organizations ("**RALOs**") established according to Section 12.2(d)(vii), and (B) five members selected by the Nominating Committee. The five members selected by the Nominating Committee shall include one citizen of a country within each of the five Geographic Regions established according to Section 7.5.

(iii) The regular terms of members of the ALAC shall be as follows:

(A) The term of one member selected by each RALO shall begin at the conclusion of an ICANN annual meeting in an even-numbered year.

(B) The term of the other member selected by each RALO shall begin at the conclusion of an ICANN annual meeting in an odd-numbered year.

(C) The terms of three of the members selected by the Nominating

Committee shall begin at the conclusion of an annual meeting in an odd-numbered year and the terms of the other two members selected by the Nominating Committee shall begin at the conclusion of an annual meeting in an even-numbered year.

(D) The regular term of each member shall end at the conclusion of the second ICANN annual meeting after the term began.

(iv) The Chair of the ALAC shall be elected by the members of the ALAC pursuant to procedures adopted by the ALAC.

(v) The ALAC shall, after consultation with each RALO, annually appoint five voting delegates (no two of whom shall be citizens of countries in the same Geographic Region) to the Nominating Committee.

(vi) The At-Large Advisory Committee may designate non-voting liaisons to each of the ccNSO Council and the GNSO Council.

(vii) There shall be one RALO for each Geographic Region established according to Section 7.5. Each RALO shall serve as the main forum and coordination point for public input to ICANN in its Geographic Region and shall be a non-profit organization certified by ICANN according to criteria and standards established by the Board based on recommendations of the At-Large Advisory Committee. An organization shall become the recognized RALO for its Geographic Region upon entering a Memorandum of Understanding with ICANN addressing the respective roles and responsibilities of ICANN and the RALO regarding the process for selecting ALAC members and requirements of openness, participatory opportunities, transparency, accountability, and diversity in the RALO's structure and procedures, as well as criteria and standards for the RALO's constituent At-Large Structures ("**At-Large Structures**").

(viii) Each RALO shall be comprised of self-supporting At-Large Structures within its Geographic Region that have been certified to meet the requirements of the RALO's Memorandum of Understanding with ICANN according to Section 12.2(d)(ix). If so provided by its Memorandum of Understanding with ICANN, a RALO may also include individual Internet users who are citizens or residents of countries within the RALO's Geographic Region.

(ix) Membership in the At-Large Community

(A) The criteria and standards for the certification of At-Large Structures within each Geographic Region shall be established by the Board based on

recommendations from the ALAC and shall be stated in the Memorandum of Understanding between ICANN and the RALO for each Geographic Region.

(B) The criteria and standards for the certification of At-Large Structures shall be established in such a way that participation by individual Internet users who are citizens or residents of countries within the Geographic Region of the RALO will predominate in the operation of each At-Large Structure within the RALO, while not necessarily excluding additional participation, compatible with the interests of the individual Internet users within the region, by others.

(C) Each RALO's Memorandum of Understanding shall also include provisions designed to allow, to the greatest extent possible, every individual Internet user who is a citizen of a country within the RALO's Geographic Region to participate in at least one of the RALO's At-Large Structures.

(D) To the extent compatible with these objectives, the criteria and standards should also afford to each RALO the type of structure that best fits the customs and character of its Geographic Region.

(E) Once the criteria and standards have been established as provided in this Section 12.2(d)(ix), the ALAC, with the advice and participation of the RALO where the applicant is based, shall be responsible for certifying organizations as meeting the criteria and standards for At-Large Structure accreditation.

(F) Decisions to certify or decertify an At-Large Structure shall be made as decided by the ALAC in its rules of procedure, save always that any changes made to the rules of procedure in respect of an At-Large Structure applications shall be subject to review by the RALOs and by the Board.

(G) Decisions as to whether to accredit, not to accredit, or disaccredit an At-Large Structure shall be subject to review according to procedures established by the Board.

(H) On an ongoing basis, the ALAC may also give advice as to whether a prospective At-Large Structure meets the applicable criteria and standards.

(x) The ALAC is also responsible, working in conjunction with the RALOs, for coordinating the following activities:

(A) Nominating individuals to fill Seat 15 on the Board. Notification of the At-

Large Community's nomination shall be given by the ALAC Chair in writing to the EC Administration, with a copy to the Secretary, and the EC shall promptly act on it as provided in Section 7.25.

(B) Keeping the community of individual Internet users informed about the significant news from ICANN;

(C) Distributing (through posting or otherwise) an updated agenda, news about ICANN, and information about items in the ICANN policy-development process;

(D) Promoting outreach activities in the community of individual Internet users;

(E) Developing and maintaining on-going information and education programs, regarding ICANN and its work;

(F) Establishing an outreach strategy about ICANN issues in each RALO's Geographic Region;

(G) Participating in the ICANN policy development processes and providing input and advice that accurately reflects the views of individual Internet users;

(H) Making public, and analyzing, ICANN's proposed policies and its decisions and their (potential) regional impact and (potential) effect on individuals in the region;

(I) Offering Internet-based mechanisms that enable discussions among members of At-Large Structures; and

(xi) Establishing mechanisms and processes that enable two-way communication between members of At-Large Structures and those involved in ICANN decision-making, so interested individuals can share their views on pending ICANN issues.

Section 12.3. PROCEDURES

Each Advisory Committee shall determine its own rules of procedure and quorum requirements; provided that each Advisory Committee shall ensure that the advice provided to the Board by such Advisory Committee is communicated in a clear and unambiguous written statement, including the rationale for such advice. The Board will respond in a timely manner to formal advice from all Advisory

Committees explaining what action it took and the rationale for doing so.

Section 12.4. TERM OF OFFICE

The chair and each member of an Advisory Committee shall serve until his or her successor is appointed, or until such Advisory Committee is sooner terminated, or until he or she is removed, resigns, or otherwise ceases to qualify as a member of the Advisory Committee.

Section 12.5. VACANCIES

Vacancies on any Advisory Committee shall be filled in the same manner as provided in the case of original appointments.

Section 12.6. COMPENSATION

Advisory Committee members shall receive no compensation for their services as a member of such Advisory Committee. The Board may, however, authorize the reimbursement of actual and necessary expenses incurred by Advisory Committee members, including Directors, performing their duties as Advisory Committee members.

ARTICLE 13 OTHER ADVISORY MECHANISMS

Section 13.1. EXTERNAL EXPERT ADVICE

(a) Purpose. The purpose of seeking external expert advice is to allow the policy-development process within ICANN to take advantage of existing expertise that resides in the public or private sector but outside of ICANN. In those cases where there are relevant public bodies with expertise, or where access to private expertise could be helpful, the Board and constituent bodies should be encouraged to seek advice from such expert bodies or individuals.

(b) Types of Expert Advisory Panels

> (i) On its own initiative or at the suggestion of any ICANN body, the Board may appoint, or authorize the President to appoint, Expert Advisory Panels consisting of public or private sector individuals or entities. If the advice sought from such Panels concerns issues of public policy, the provisions of Section 13.1(c) shall apply.
>
> (ii) In addition, in accordance with Section 13.1(c), the Board may refer

> issues of public policy pertinent to matters within ICANN's Mission to a multinational governmental or treaty organization.

(c) Process for Seeking Advice: Public Policy Matters

> (i) The Governmental Advisory Committee may at any time recommend that the Board seek advice concerning one or more issues of public policy from an external source, as set out above.
>
> (ii) In the event that the Board determines, upon such a recommendation or otherwise, that external advice should be sought concerning one or more issues of public policy, the Board shall, as appropriate, consult with the Governmental Advisory Committee regarding the appropriate source from which to seek the advice and the arrangements, including definition of scope and process, for requesting and obtaining that advice.
>
> (iii) The Board shall, as appropriate, transmit any request for advice from a multinational governmental or treaty organization, including specific terms of reference, to the Governmental Advisory Committee, with the suggestion that the request be transmitted by the Governmental Advisory Committee to the multinational governmental or treaty organization.

(d) Process for Seeking and Advice: Other Matters. Any reference of issues not concerning public policy to an Expert Advisory Panel by the Board or President in accordance with Section 13.1(b)(i) shall be made pursuant to terms of reference describing the issues on which input and advice is sought and the procedures and schedule to be followed.

(e) Receipt of Expert Advice and its Effect. External advice pursuant to this Section 13.1 shall be provided in written form. Such advice is advisory and not binding, and is intended to augment the information available to the Board or other ICANN body in carrying out its responsibilities.

(f) Opportunity to Comment. The Governmental Advisory Committee, in addition to the Supporting Organizations and other Advisory Committees, shall have an opportunity to comment upon any external advice received prior to any decision by the Board.

Section 13.2. TECHNICAL LIAISON GROUP

(a) Purpose. The quality of ICANN's work depends on access to complete and authoritative information concerning the technical standards that underlie ICANN's activities. ICANN's relationship to the organizations that produce these standards is therefore particularly important. The Technical Liaison Group ("**TLG**") shall connect the Board with appropriate sources of technical advice on specific matters pertinent to ICANN's activities.

(b) TLG Organizations. The TLG shall consist of four organizations: the European Telecommunications Standards Institute (ETSI), the International Telecommunications Union's Telecommunication Standardization Sector (ITU-T), the World Wide Web Consortium (W3C), and the Internet Architecture Board ("**IAB**").

(c) Role. The role of the TLG organizations shall be to channel technical information and guidance to the Board and to other ICANN entities. This role has both a responsive component and an active "watchdog" component, which involve the following responsibilities:

> (i) In response to a request for information, to connect the Board or other ICANN body with appropriate sources of technical expertise. This component of the TLG role covers circumstances in which ICANN seeks an authoritative answer to a specific technical question. Where information is requested regarding a particular technical standard for which a TLG organization is responsible, that request shall be directed to that TLG organization.
>
> (ii) As an ongoing "watchdog" activity, to advise the Board of the relevance and progress of technical developments in the areas covered by each organization's scope that could affect Board decisions or other ICANN actions, and to draw attention to global technical standards issues that affect policy development within the scope of ICANN's Mission. This component of the TLG role covers circumstances in which ICANN is unaware of a new development, and would therefore otherwise not realize that a question should be asked.

(d) TLG Procedures. The TLG shall not have officers or hold meetings, nor shall it provide policy advice to the Board as a committee (although TLG organizations may individually be asked by the Board to do so as the need arises in areas relevant to their individual charters). Neither shall the TLG debate or otherwise coordinate technical issues across the TLG organizations; establish or attempt to establish unified positions; or create or attempt to create additional layers or

structures within the TLG for the development of technical standards or for any other purpose.

(e) Technical Work with the IETF. The TLG shall have no involvement with ICANN's work for the Internet Engineering Task Force (IETF), Internet Research Task Force, or the Internet Architecture Board (IAB), as described in the IETF-ICANN Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority ratified by the Board on 10 March 2000 and any supplemental agreements thereto.

(f) Individual Technical Experts. Each TLG organization shall designate two individual technical experts who are familiar with the technical standards issues that are relevant to ICANN's activities. These 8 experts shall be available as necessary to determine, through an exchange of e-mail messages, where to direct a technical question from ICANN when ICANN does not ask a specific TLG organization directly.

ARTICLE 14 BOARD AND TEMPORARY COMMITTEES

Section 14.1. BOARD COMMITTEES

The Board may establish one or more committees of the Board (each, a "**Board Committee**"), which shall continue to exist until otherwise determined by the Board. Only Directors may be appointed to a Committee of the Board; provided, that a Liaison may be appointed as a liaison to a Committee of the Board consistent with their non-voting capacity. If a person appointed to a Committee of the Board ceases to be a Director, such person shall also cease to be a member of any Committee of the Board. Each Committee of the Board shall consist of two or more Directors. The Board may designate one or more Directors as alternate members of any such committee, who may replace any absent member at any meeting of the committee. Committee members may be removed from a committee at any time by a two-thirds (2/3) majority vote of all Directors; provided, however, that in no event shall a Director be removed from a committee unless such removal is approved by not less than a majority of all Directors.

Section 14.2. POWERS OF BOARD COMMITTEES

(a) The Board may delegate to Committees of the Board all legal authority of the Board except with respect to:

> (i) The filling of vacancies on the Board or on any committee;

(ii) The amendment or repeal of Bylaws or the Articles of Incorporation or the adoption of new Bylaws or Articles of Incorporation;

(iii) The amendment or repeal of any resolution of the Board which by its express terms is not so amendable or repealable;

(iv) The appointment of committees of the Board or the members thereof;

(v) The approval of any self-dealing transaction, as such transactions are defined in Section 5233(a) of the CCC;

(vi) The approval of the ICANN Budget or IANA Budget required by Section 22.4 or the Operating Plan or Strategic Plan required by Section 22.5; or

(vii) The compensation of any Officer described in Article 15.

(b) The Board shall have the power to prescribe the manner in which proceedings of any Committee of the Board shall be conducted. In the absence of any such prescription, such committee shall have the power to prescribe the manner in which its proceedings shall be conducted. Unless these Bylaws, the Board or such committee shall otherwise provide, the regular and special meetings of committees shall be governed by the provisions of Article 7 applicable to meetings and actions of the Board. Each committee shall keep regular minutes of its proceedings and shall report the same to the Board from time to time, as the Board may require.

Section 14.3. TEMPORARY COMMITTEES

The Board may establish such temporary committees as it sees fit, with membership, duties, and responsibilities as set forth in the resolutions or charters adopted by the Board in establishing such committees.

ARTICLE 15 OFFICERS

Section 15.1. OFFICERS

The officers of ICANN (each, an "**Officer**") shall be a President (who shall serve as Chief Executive Officer), a Secretary, and a Chief Financial Officer. ICANN may also have, at the discretion of the Board, any additional officers that it deems appropriate. Any person, other than the President, may hold more than one office, except that no member of the Board (other than the President) shall simultaneously serve as an officer of ICANN.

Section 15.2. ELECTION OF OFFICERS

The officers of ICANN shall be elected annually by the Board, pursuant to the recommendation of the President or, in the case of the President, of the Chair of the Board. Each such officer shall hold his or her office until he or she resigns, is removed, is otherwise disqualified to serve, or his or her successor is elected.

Section 15.3. REMOVAL OF OFFICERS

Any Officer may be removed, either with or without cause, by a two-thirds (2/3) majority vote of all Directors. Should any vacancy occur in any office as a result of death, resignation, removal, disqualification, or any other cause, the Board may delegate the powers and duties of such office to any Officer or to any Director until such time as a successor for the office has been elected.

Section 15.4. PRESIDENT

The President shall be the Chief Executive Officer (CEO) of ICANN in charge of all of its activities and business. All other officers and staff shall report to the President or his or her delegate, unless stated otherwise in these Bylaws. The President shall serve as an ex officio Director, and shall have all the same rights and privileges of any Director. The President shall be empowered to call special meetings of the Board as set forth herein, and shall discharge all other duties as may be required by these Bylaws and from time to time may be assigned by the Board.

Section 15.5. SECRETARY

The Secretary shall keep or cause to be kept the minutes of the Board in one or more books provided for that purpose, shall see that all notices are duly given in accordance with the provisions of these Bylaws or as required by law, and in general shall perform all duties as from time to time may be prescribed by the President or the Board.

Section 15.6. CHIEF FINANCIAL OFFICER

The Chief Financial Officer ("**CFO**") shall be the chief financial officer of ICANN. If required by the Board, the CFO shall give a bond for the faithful discharge of his or her duties in such form and with such surety or sureties as the Board shall determine. The CFO shall have charge and custody of all the funds of ICANN and shall keep or cause to be kept, in books belonging to ICANN, full and accurate amounts of all receipts and disbursements, and shall deposit all money and other valuable effects in the name of ICANN in such depositories as may be designated

for that purpose by the Board. The CFO shall disburse the funds of ICANN as may be ordered by the Board or the President and, whenever requested by them, shall deliver to the Board and the President an account of all his or her transactions as CFO and of the financial condition of ICANN. The CFO shall be responsible for ICANN's financial planning and forecasting and shall assist the President in the preparation of the ICANN Budget, the IANA Budget and Operating Plan. The CFO shall coordinate and oversee ICANN's funding, including any audits or other reviews of ICANN or its Supporting Organizations. The CFO shall be responsible for all other matters relating to the financial operation of ICANN.

Section 15.7. ADDITIONAL OFFICERS

In addition to the officers described above, any additional or assistant officers who are elected or appointed by the Board shall perform such duties as may be assigned to them by the President or the Board.

Section 15.8. COMPENSATION AND EXPENSES

The compensation of any Officer of ICANN shall be approved by the Board. Expenses incurred in connection with performance of their officer duties may be reimbursed to Officers upon approval of the President (in the case of Officers other than the President), by another Officer designated by the Board (in the case of the President), or the Board.

Section 15.9. CONFLICTS OF INTEREST

The Board, through the Board Governance Committee, shall establish a policy requiring a statement from each Officer not less frequently than once a year setting forth all business and other affiliations that relate in any way to the business and other affiliations of ICANN.

ARTICLE 16 POST-TRANSITION IANA ENTITY

Section 16.1. DESCRIPTION

ICANN shall maintain as a separate legal entity a California nonprofit public benefit corporation (["**PTI**"]) for the purpose of providing IANA services, including providing IANA naming function services pursuant to the IANA Naming Function Contract, as well as other services as determined by ICANN in coordination with the direct and indirect customers of the IANA functions. ICANN shall at all times be the sole member of PTI as that term is defined in Section 5056 of the CCC ("**Member**"). For the purposes of these Bylaws, the "IANA naming function" does not include the Internet Protocol numbers and Autonomous System numbers

services (as contemplated by Section 1.1(a)(iii)), the protocol ports and parameters services and the root zone maintainer function.

Section 16.2. PTI Governance

(a) ICANN, in its capacity as the sole Member of PTI, shall elect the directors of PTI in accordance with the articles of incorporation and bylaws of PTI and have all other powers of a sole Member under the CCC except as otherwise provided in these Bylaws.

(b) No amendment or modification of the articles of incorporation of PTI shall be effective unless approved by the EC (pursuant to the procedures applicable to Articles Amendments described in Section 25.2, as if such Article Amendment referenced therein refers to an amendment of PTI's articles of incorporation).

(c) ICANN shall not amend or modify the bylaws of PTI in a manner that would effect any of the matters set forth in clauses (i) through (xiv) below (a "**PTI Bylaw Amendment**") if such PTI Bylaw Amendment has been rejected by the EC pursuant to the procedures described in Section 16.2(e):

> (i) any change to the corporate form of PTI to an entity that is not a California nonprofit public benefit corporation organized under the CCC or any successor statute;
>
> (ii) any change in the corporate mission of PTI that is materially inconsistent with ICANN's Mission as set forth in these Bylaws;
>
> (iii) any change to the status of PTI as a corporation with members;
>
> (iv) any change in the rights of ICANN as the sole Member of PTI, including voting, classes of membership, rights, privileges, preferences, restrictions and conditions;
>
> (v) any change that would grant rights to any person or entity (other than ICANN) with respect to PTI as designators or otherwise to: (A) elect or designate directors of PTI; or (B) approve any amendments to the articles of incorporation or bylaws of PTI;
>
> (vi) any change in the number of directors of the board of directors of PTI (the "**PTI Board**");
>
> (vii) any changes in the allocation of directors on the PTI Board between independent directors and employees of ICANN or employees of PTI or to

the definition of "independent" (as used in PTI's bylaws) for purposes of determining whether a director of PTI is independent;

(viii) the creation of any committee of the PTI Board with the power to exercise the authority of the PTI Board;

(ix) any change in the procedures for nominating independent PTI directors;

(x) the creation of classes of PTI directors or PTI directors with different terms or voting rights;

(xi) any change in PTI Board quorum requirements or voting requirements;

(xii) any change to the powers and responsibilities of the PTI Board or the PTI officers;

(xiii) any change to the rights to exculpation and indemnification that is adverse to the exculpated or indemnified party, including with respect to advancement of expenses and insurance, provided to directors, officers, employees or other agents of PTI; or

(xiv) any change to the requirements to amend the articles of incorporation or bylaws of PTI.

(d) ICANN shall not take any of the following actions (together with the PTI Bylaw Amendments, "**PTI Governance Actions**") if such PTI Governance Action has been rejected by the EC pursuant to the procedures described in Section 16.2(e).

(i) Any resignation by ICANN as sole Member of PTI or any transfer, disposition, cession, expulsion, suspension or termination by ICANN of its membership in PTI or any transfer, disposition, cession, expulsion, suspension or termination by ICANN of any right arising from its membership in PTI.

(ii) Any sale, transfer or other disposition of PTI's assets, other than (A) in the ordinary course of PTI's business, (B) in connection with an IANA Naming Function Separation Process (as defined in Section 19.1(a)) that has been approved in accordance with Article 19 or (C) the disposition of obsolete, damaged, redundant or unused assets.

(iii) Any merger, consolidation, sale or reorganization of PTI.

(iv) Any dissolution, liquidation or winding-up of the business and affairs of PTI or the commencement of any other voluntary bankruptcy proceeding of PTI.

(e) Promptly after the Board approves a PTI Governance Action (a "**PTI Governance Action Approval**"), the Secretary shall provide a notice of the Board's decision to the EC Administration and the Decisional Participants ("**Board Notice**"), which Board Notice shall enclose a copy of the PTI Governance Action that is the subject of the PTI Governance Action Approval. ICANN shall post the Board Notice, along with a copy of the notification(s) sent to the EC Administration and the Decisional Participants, on the Website promptly following the delivery of the Board Notice to the EC Administration and the Decisional Participants. The EC Administration shall promptly commence and comply with the procedures and requirements specified in Article 2 of Annex D.

(i) A PTI Governance Action shall become effective upon the earliest to occur of the following:

(A)(1) A Rejection Action Petition Notice (as defined in Section 2.2(c)(i) of Annex D) is not timely delivered by the Rejection Action Petitioning Decisional Participant (as defined in Section 2.2(c)(i) of Annex D) to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D or (2) a Rejection Process Termination Notice (as defined in Section 2.2(c)(ii) of Annex D) is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D, in which case the PTI Governance Action that is the subject of the PTI Governance Action Approval shall be in full force and effect as of the date immediately following the expiration of the Rejection Action Petition Period (as defined in Section 2.2(b) of Annex D) relating to such PTI Governance Action Approval and the effectiveness of such PTI Governance Action shall not be subject to further challenge by the EC pursuant to the EC's rejection right as described in Article 2 of Annex D;

(B)(1) A Rejection Action Supported Petition (as defined in Section 2.2(d)(i) of Annex D) is not timely delivered by the Rejection Action Petitioning Decisional Participant to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D, in which case the PTI Governance Action that is the subject of the PTI Governance Action Approval shall be in full force and effect as of the date immediately following

the expiration of the Rejection Action Petition Support Period (as defined in Section 2.2(d)(i) of Annex D) relating to such PTI Governance Action Approval and the effectiveness of such PTI Governance Action shall not be subject to further challenge by the EC pursuant to the EC's rejection right as described in Article 2 of Annex D; and

(C)(1) An EC Rejection Notice (as defined in Section 2.4(b) of Annex D) is not timely delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4 of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4(c) of Annex D, in which case the PTI Governance Action that is the subject of the PTI Governance Action Approval shall be in full force and effect as of the date immediately following the expiration of the Rejection Action Decision Period (as defined in Section 2.4(a) of Annex D) relating to such PTI Governance Action Approval and the effectiveness of such PTI Governance Action shall not be subject to further challenge by the EC pursuant to the EC's rejection right as described in Article 2 of Annex D.

(ii) A PTI Governance Action that has been rejected by the EC pursuant to and in compliance with Article 2 of Annex D shall have no force and effect, and shall be void ab initio.

(iii) Following receipt of an EC Rejection Notice relating to a PTI Governance Action, ICANN staff and the Board shall consider the explanation provided by the EC Administration as to why the EC has chosen to reject the PTI Governance Action in determining whether or not to develop a new PTI Governance Action and the substance of such new PTI Governance Action, which shall be subject to the procedures of this Section 16.2.

Section 16.3. IANA NAMING FUNCTION CONTRACT

(a) On or prior to 1 October 2016, ICANN shall enter into a contract with PTI for the performance of the IANA naming function (as it may be amended or modified, the "**IANA Naming Function Contract**") and a related statement of work (the "**IANA Naming Function SOW**"). Except as to implement any modification, waiver or amendment to the IANA Naming Function Contract or IANA Naming Function SOW related to an IFR Recommendation or Special IFR Recommendation approved pursuant to Section 18.6 or an SCWG Recommendation approved pursuant to Section 19.4 (which, for the avoidance of doubt, shall not be subject to this Section 16.3(a)), ICANN shall not agree to modify, amend or waive any

Material Terms (as defined below) of the IANA Naming Function Contract or the IANA Naming Function SOW if a majority of each of the ccNSO and GNSO Councils reject the proposed modification, amendment or waiver. The following are the "**Material Terms**" of the IANA Naming Function Contract and IANA Naming Function SOW:

> (i) The parties to the IANA Naming Function Contract and IANA Naming Function SOW;
>
> (ii) The initial term and renewal provisions of the IANA Naming Function Contract and IANA Naming Function SOW;
>
> (iii) The manner in which the IANA Naming Function Contract or IANA Naming Function SOW may be terminated;
>
> (iv) The mechanisms that are available to enforce the IANA Naming Function Contract or IANA Naming Function SOW;
>
> (v) The role and responsibilities of the CSC (as defined in Section 17.1), escalation mechanisms and/or the IFR (as defined in Section 18.1);
>
> (vi) The IANA Naming Function Contract's provisions requiring that fees charged by PTI be based on direct costs and resources incurred by PTI;
>
> (vii) The IANA Naming Function Contract's prohibition against subcontracting;
>
> (viii)The availability of the IRP as a point of escalation for claims of PTI's failure to meet defined service level expectations;
>
> (ix) The IANA Naming Function Contract's audit requirements; and
>
> (x) The requirements related to ICANN funding of PTI.

(b) ICANN shall enforce its rights under the IANA Naming Function Contract and the IANA Naming Function SOW.

ARTICLE 17 CUSTOMER STANDING COMMITTEE

Section 17.1. DESCRIPTION

ICANN shall establish a Customer Standing Committee ("**CSC**") to monitor PTI's

performance under the IANA Naming Function Contract and IANA Naming Function SOW.

The mission of the CSC is to ensure continued satisfactory performance of the IANA naming function for the direct customers of the naming services. The direct customers of the naming services are top-level domain registry operators as well as root server operators and other non-root zone functions.

The CSC will achieve this mission through regular monitoring of the performance of the IANA naming function against the IANA Naming Function Contract and IANA Naming Function SOW and through mechanisms to engage with PTI to remedy identified areas of concern.

The CSC is not authorized to initiate a change in PTI through a Special IFR (as defined in Section 18.1), but may escalate a failure to correct an identified deficiency to the ccNSO and GNSO, which might then decide to take further action using consultation and escalation processes, which may include a Special IFR. The ccNSO and GNSO may address matters escalated by the CSC, pursuant to their operating rules and procedures.

Section 17.2. COMPOSITION, APPOINTMENT, TERM AND REMOVAL

(a) The CSC shall consist of:

> (i) Two individuals representing gTLD registry operators appointed by the Registries Stakeholder Group;
>
> (ii) Two individuals representing ccTLD registry operators appointed by the ccNSO; and
>
> (iii) One individual liaison appointed by PTI,
>
> each appointed in accordance with the rules and procedures of the appointing organization; provided that such individuals should have direct experience and knowledge of the IANA naming function.

(b) If so determined by the ccNSO and GNSO, the CSC may, but is not required to, include one additional member: an individual representing top-level domain registry operators that are not considered a ccTLD or gTLD, who shall be appointed by the ccNSO and the GNSO. Such representative shall be required to

submit a letter of support from the registry operator it represents.

(c) Each of the following organizations may also appoint one liaison to the CSC in accordance with the rules and procedures of the appointing organization: (i) GNSO (from the Registrars Stakeholder Group or the Non-Contracted Parties House), (ii) ALAC, (iii) either the NRO or ASO (as determined by the ASO), (iv) GAC, (v) RSSAC, (vi) SSAC and (vii) any other Supporting Organization or Advisory Committee established under these Bylaws.

(d) The GNSO and ccNSO shall approve the initial proposed members and liaisons of the CSC, and thereafter, the ccNSO and GNSO shall approve each annual slate of members and liaisons being recommended for a new term.

(e) The CSC members and liaisons shall select from among the CSC members who will serve as the CSC's liaison to the IFRT (as defined in Section 18.1) and any Separation Cross-Community Working Group ("**SCWG**").

(f) Any CSC member or liaison may be removed and replaced at any time and for any reason or no reason by the organization that appointed such member or liaison.

(g) In addition, the Chair of the CSC may recommend that a CSC member or liaison be removed by the organization that appointed such member or liaison, upon any of the following: (i) (A) for not attending without sufficient cause a minimum of nine CSC meetings in a one-year period (or at least 75% of all CSC meetings in a one-year period if less than nine meetings were held in such one-year period) or (B) if such member or liaison has been absent for more than two consecutive meetings without sufficient cause; or (ii) for grossly inappropriate behavior.

(h) A vacancy on the CSC shall be deemed to exist in the event of the death, resignation or removal of any CSC member or liaison. Vacancies shall be filled by the organization(s) that appointed such CSC member or liaison. The appointing organization(s) shall provide written notice to the Secretary of its appointment to fill a vacancy, with a notification copy to the Chair of the CSC. The organization(s) responsible for filling such vacancy shall use its reasonable efforts to fill such vacancy within one month after the occurrence of such vacancy.

Section 17.3.CSC CHARTER; PERIODIC REVIEW

(a) The CSC shall act in accordance with its charter (the "**CSC Charter**").

(b) The effectiveness of the CSC shall be reviewed two years after the first meeting of the CSC; and then every three years thereafter. The method of review

will be determined by the ccNSO and GNSO and the findings of the review will be published on the Website.

(c) The CSC Charter shall be reviewed by a committee of representatives from the ccNSO and the Registries Stakeholder Group selected by such organizations. This review shall commence one year after the first meeting of the CSC. Thereafter, the CSC Charter shall be reviewed by such committee of representatives from the ccNSO and the Registries Stakeholder Group selected by such organizations at the request of the CSC, ccNSO, GNSO, the Board and/or the PTI Board and/or by an IFRT in connection with an IFR.

(d) Amendments to the CSC Charter shall not be effective unless ratified by the vote of a simple majority of each of the ccNSO and GNSO Councils pursuant to each such organizations' procedures. Prior to any action by the ccNSO and GNSO, any recommended changes to the CSC Charter shall be subject to a public comment period that complies with the designated practice for public comment periods within ICANN. Notwithstanding the foregoing, to the extent any provision of an amendment to the CSC Charter conflicts with the terms of the Bylaws, the terms of the Bylaws shall control.

Section 17.4. ADMINISTRATIVE AND OPERATIONAL SUPPORT

ICANN shall provide administrative and operational support necessary for the CSC to carry out its responsibilities, including providing and facilitating remote participation in all meetings of the CSC.

ARTICLE 18 IANA NAMING FUNCTION REVIEWS

Section 18.1. IANA NAMING FUNCTION REVIEW

The Board, or an appropriate committee thereof, shall cause periodic and/or special reviews (each such review, an "**IFR**") of PTI's performance of the IANA naming function against the contractual requirements set forth in the IANA Naming Function Contract and the IANA Naming Function SOW to be carried out by an IANA Function Review Team ("**IFRT**") established in accordance with Article 18, as follows:

(a) Regularly scheduled periodic IFRs, to be conducted pursuant to Section 18.2 below ("**Periodic IFRs**"); and

(b) IFRs that are not Periodic IFRs, to be conducted pursuant to Section 18.12 below ("**Special IFRs**").

Section 18.2. FREQUENCY OF PERIODIC IFRS

(a) The first Periodic IFR shall be convened no later than [1 October 2018].

(b) Periodic IFRs after the first Periodic IFR shall be convened no less frequently than every five years, measured from the date the previous IFRT for a Periodic IFR was convened.

(c) In the event a Special IFR is ongoing at the time a Periodic IFR is required to be convened under this Section 18.2, the Board shall cause the convening of the Periodic IFR to be delayed if such delay is approved by the vote of (i) a supermajority of the ccNSO Council (pursuant to the ccNSO's procedures or, if such procedures do not define a supermajority, two-thirds (2/3) of the ccNSO Council's members) and (ii) a GNSO Supermajority. Any decision by the ccNSO and GNSO to delay a Periodic IFR must identify the period of delay, which should generally not exceed 12 months after the completion of the Special IFR.

Section 18.3. IFR RESPONSIBILITIES

For each Periodic IFR, the IFRT shall:

(a) Review and evaluate the performance of PTI against the requirements set forth in the IANA Naming Function Contract in relation to the needs of its direct customers and the expectations of the broader ICANN community, and determine whether to make any recommendations with respect to PTI's performance;

(b) Review and evaluate the performance of PTI against the requirements set forth in the IANA Naming Function Contract and IANA Naming Function SOW;

(c) Review the IANA Naming Function SOW and determine whether to recommend any amendments to the IANA Naming Function Contract and IANA Naming Function SOW to account for the needs of the direct customers of the naming services and/or the community at large;

(d) Review and evaluate the openness and transparency procedures of PTI and any oversight structures for PTI's performance, including reporting requirements and budget transparency;

(e) Review and evaluate the performance and effectiveness of the EC with respect to actions taken by the EC, if any, pursuant to Section 16.2, Section 18.6, Section 18.12, Section 19.1, Section 19.4, Section 22.4(b) and Annex D;

(f) Review and evaluate the performance of the IANA naming function according to established service level expectations during the IFR period being reviewed and

compared to the immediately preceding Periodic IFR period;

(g) Review and evaluate whether there are any systemic issues that are impacting PTI's performance under the IANA Naming Function Contract and IANA Naming Function SOW;

(h) Initiate public comment periods and other processes for community input on PTI's performance under the IANA Naming Function Contract and IANA Naming Function SOW (such public comment periods shall comply with the designated practice for public comment periods within ICANN);

(i) Consider input from the CSC and the community on PTI's performance under the IANA Naming Function Contract and IANA Naming Function SOW;

(j) Identify process or other areas for improvement in the performance of the IANA naming function under the IANA Naming Function Contract and IANA Naming Function SOW and the performance of the CSC and the EC as it relates to oversight of PTI; and

(k) Consider and assess any changes implemented since the immediately preceding IFR and their implications for the performance of PTI under the IANA Naming Function Contract and IANA Naming Function SOW.

Section 18.4. IFR REQUIRED INPUTS

In conducting an IFR, the IFRT shall review and analyze the following information:

(a) Reports provided by PTI pursuant to the IANA Naming Function Contract and/or IANA Naming Function SOW during the IFR period being reviewed, any portion of which may be redacted pursuant to the Confidential Disclosure Framework set forth in the Operating Standards in accordance with Section 4.6(a)(vi);

(b) Reports provided by the CSC in accordance with the CSC Charter during the IFR period being reviewed;

(c) Community inputs through public consultation procedures as reasonably determined by the IFRT, including, among other things, public comment periods, input provided at in-person sessions during ICANN meetings, responses to public surveys related to PTI's performance under the IANA Naming Function Contract and IANA Naming Function SOW, and public inputs during meetings of the IFRT;

(d) Recommendations for technical, process and/or other improvements relating to the mandate of the IFR provided by the CSC or the community; and

(e) Results of any site visit conducted by the IFRT, which shall be conducted in consultation with ICANN (i) upon reasonable notice, (ii) in a manner so as to not affect PTI's performance under the IANA Naming Function Contract or the IANA Naming Function SOW and (iii) pursuant to procedures and requirements reasonably developed by ICANN and reasonably acceptable to the IFRT. Any such site visit shall be limited to matters reasonably related to the IFRT's responsibilities pursuant to Section 18.3.

Section 18.5. IFR RESULTS AND RECOMMENDATIONS

(a) The results of the IFR are not limited and could include a variety of recommendations or no recommendation; provided, however, that any recommendations must directly relate to the matters discussed in Section 18.3 and comply with this Section 18.5.

(b) Any IFRT recommendations should identify improvements that are supported by data and associated analysis about existing deficiencies and how they could be addressed. Each recommendation of the IFRT shall include proposed remedial procedures and describe how those procedures are expected to address such issues. The IFRT's report shall also propose timelines for implementing the IFRT's recommendations. The IFRT shall attempt to prioritize each of its recommendations and provide a rationale for such prioritization.

(c) In any case where a recommendation of an IFRT focuses on a service specific to gTLD registry operators, no such recommendation shall be made by the IFRT in any report to the community (including any report to the Board) if opposition to such recommendation is expressed by any IFRT member appointed by the Registries Stakeholder Group. In any case where a recommendation of an IFRT focuses on a service specific to ccTLD registry operators, no such recommendation shall be made by the IFRT in any report to the community (including any report to the Board) if opposition to such recommendation is expressed by any IFRT member appointed by the ccNSO.

(d) Notwithstanding anything herein to the contrary, the IFRT shall not have the authority to review or make recommendations relating to policy or contracting issues that are not included in the IANA Naming Function Contract or the IANA Naming Function SOW, including, without limitation, policy development, adoption processes or contract enforcement measures between contracted registries and ICANN.

Section 18.6.Recommendations to Amend the IANA Naming Function contract, iana naming function SOW or CSC charter

(a) The IFRT may recommend, among other things to the extent reasonably related to the IFR responsibilities set forth in Section 18.3, amendments to the IANA Naming Function Contract, IANA Naming Function SOW and/or the CSC Charter. The IFRT shall, at a minimum, take the following steps before an amendment to either the IANA Naming Function Contract, IANA Naming Function SOW or CSC Charter is proposed:

> (i) Consult with the Board (such consultation to be conducted in parallel with other processes set forth in this Section 18.6(a)) and PTI;
>
> (ii) Consult with the CSC;
>
> (iii) Conduct a public input session for ccTLD and gTLD registry operators; and
>
> (iv) Seek public comment on the amendments that are under consideration by the IFRT through a public comment period that complies with the designated practice for public comment periods within ICANN.

(b) A recommendation of an IFRT for a Periodic IFR that would amend the IANA Naming Function Contract or IANA Naming Function SOW shall only become effective if, with respect to each such recommendation (each, an "**IFR Recommendation**"), each of the following occurs:

> (i) The IFR Recommendation has been approved by the vote of (A) a supermajority of the ccNSO Council (pursuant to the ccNSO's procedures or, if such procedures do not define a supermajority, two-thirds (2/3) of the ccNSO Council's members) and (B) a GNSO Supermajority;
>
> (ii) After a public comment period that complies with the designated practice for public comment periods within ICANN, the Board has approved the IFR Recommendation; and
>
> (iii) The EC has not rejected the Board's approval of the IFR Recommendation pursuant to and in compliance with Section 18.6(d).

(c) If the Board (x) rejects an IFR Recommendation that was approved by the ccNSO Council and GNSO Council pursuant to Section 18.6(b)(i) or (y) does not resolve to either accept or reject an IFR Recommendation within 45 days of the

later of (1) the date that the condition in Section 18.6(b)(i) is satisfied or (2) the expiration of the public comment period contemplated by Section 18.6(b)(ii), the Secretary shall provide a Board Notice to the EC Administration and the Decisional Participants, which Board Notice shall enclose a copy of the applicable IFR Recommendation. ICANN shall post the Board Notice, along with a copy of the notification(s) sent to the EC Administration and the Decisional Participants, on the Website promptly following the delivery of the Board Notice to the EC Administration and the Decisional Participants.

> (i) ICANN shall, at the direction of the EC Administration, convene a Rejection Action Community Forum (as defined in Section 2.3(a) of Annex D), which Rejection Action Community Forum shall be conducted in accordance with Section 2.3 of Annex D, to discuss the Board Notice; provided, that, for purposes of Section 2.3 of Annex D, (A) the Board Notice shall be treated as the Rejection Action Supported Petition, (B) the EC Administration shall be treated as the Rejection Action Petitioning Decisional Participant (and there shall be no Rejection Action Supporting Decisional Participants (as defined in Section 2.2(d)(i) of Annex D) and (C) the Rejection Action Community Forum Period shall expire on the 21st day after the date the Secretary provides the Board Notice to the EC Administration and the Decisional Participants.
>
> (ii) No later than 45 days after the conclusion of such Rejection Action Community Forum Period, the Board shall resolve to either uphold its rejection of the IFR Recommendation or approve the IFR Recommendation (either, a "**Post-Forum IFR Recommendation Decision**").
>
> (A)If the Board resolves to approve the IFR Recommendation, such IFR Recommendation will be subject to Section 18.6(d).
>
> (B)For the avoidance of doubt, the Board shall not be obligated to change its decision on the IFR Recommendation as a result of the Rejection Action Community Forum.
>
> (C)The Board's Post-Forum IFR Recommendation Decision shall be posted on the Website in accordance with the Board's posting obligations as set forth in Article 3.

(d) Promptly after the Board approves an IFR Recommendation (an "**IFR Recommendation Decision**"), the Secretary shall provide a Board Notice to the EC Administration and the Decisional Participants, which Board Notice shall

enclose a copy of the IFR Recommendation that is the subject of the IFR Recommendation Decision. ICANN shall post the Board Notice, along with a copy of the notification(s) sent to the EC Administration and the Decisional Participants, on the Website promptly following the delivery of the Board Notice to the EC Administration and the Decisional Participants. The EC Administration shall promptly commence and comply with the procedures and requirements specified in Article 2 of Annex D.

(i) An IFR Recommendation Decision shall become final upon the earliest to occur of the following:

(A)(1) A Rejection Action Petition Notice is not timely delivered by the Rejection Action Petitioning Decisional Participant to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D, in which case the IFR Recommendation Decision shall be final as of the date immediately following the expiration of the Rejection Action Petition Period relating to such IFR Recommendation Decision;

(B)(1) A Rejection Action Supported Petition is not timely delivered by the Rejection Action Petitioning Decisional Participant to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D, in which case the IFR Recommendation Decision shall be final as of the date immediately following the expiration of the Rejection Action Petition Support Period relating to such IFR Recommendation Decision; and

(C)(1) An EC Rejection Notice is not timely delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4 of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4(c) of Annex D, in which case the IFR Recommendation Decision shall be final as of the date immediately following the expiration of the Rejection Action Decision Period relating to such IFR Recommendation Decision.

(ii) An IFR Recommendation Decision that has been rejected by the EC pursuant to and in compliance with Article 2 of Annex D shall have no force and effect, and shall be void ab initio.

(e) For the avoidance of doubt, Section 18.6(d) shall not apply when the Board acts in a manner that is consistent with an IFR Recommendation unless such IFR Recommendation relates to an IANA Naming Function Separation Process as described in Article 19.

(f) Timelines for implementing any amendments to the IANA Naming Function Contract or IANA Naming Function SOW shall be reasonably agreed between the IFRT, ICANN and PTI.

(g) A recommendation of an IFRT that would amend the CSC Charter shall only become effective if approved pursuant to Section 17.3(d).

Section 18.7. COMPOSITION OF IFR TEAMS

Each IFRT shall consist of the following members and liaisons to be appointed in accordance with the rules and procedures of the appointing organization:

(a) Two representatives appointed by the ccNSO from its ccTLD registry operator representatives;

(b) One non-ccNSO ccTLD representative who is associated with a ccTLD registry operator that is not a representative of the ccNSO, appointed by the ccNSO; it is strongly recommended that the ccNSO consult with the regional ccTLD organizations (i.e., AfTLD, APTLD, LACTLD, and CENTR) in making its appointment;

(c) Two representatives appointed by the Registries Stakeholder Group;

(d) One representative appointed by the Registrars Stakeholder Group;

(e) One representative appointed by the Commercial Stakeholder Group;

(f) One representative appointed by the Non-Commercial Stakeholder Group;

(g) One representative appointed by the GAC;

(h) One representative appointed by the SSAC;

(i) One representative appointed by the RSSAC;

(j) One representative appointed by the ALAC;

(k) One liaison appointed by the CSC;

(l) One liaison who may be appointed by the ASO; and

(m) One liaison who may be appointed by the IAB.

(n) The IFRT shall also include an unlimited number of non-member, non-liaison participants.

(o) The IFRT shall not be a standing body. A new IFRT shall be constituted for each IFR and the IFRT shall automatically dissolve following the end of the process for approving such IFRT's IFR Recommendations pursuant to Section 18.6.

Section 18.8. MEMBERSHIP; ELECTION OF CO-CHAIRS, AND LIAISONS

(a) All candidates for appointment to the IFRT as a member or liaison shall submit an expression of interest to the organization that would appoint such candidate as a member or liaison to the IFRT, which shall state: (i) why the candidate is interested in becoming involved in the IFRT, (ii) what particular skills the candidate would bring to the IFRT, (iii) the candidate's knowledge of the IANA functions, (iv) the candidate's understanding of the purpose of the IFRT, and (v) that the candidate understands the time necessary to participate in the IFR process and can commit to the role.

(b) Members, liaisons and participants of the IFRT shall disclose to ICANN and the IFRT any conflicts of interest with a specific complaint or issue under review. The IFRT may exclude from the discussion of a specific complaint or issue any member deemed by the majority of IFRT members to have a conflict of interest. The co-chairs of the IFRT shall record any such conflict of interest in the minutes of the IFRT.

(c) To the extent reasonably possible, the appointing organizations for the IFRT members and liaisons shall work together to achieve an IFRT that is balanced for diversity (including functional, geographic and cultural) and skill, and should seek to broaden the number of individuals participating across the various reviews; provided, that the IFRT should include members from each ICANN Geographic Region, and the ccNSO and Registries Stakeholder Group shall not appoint multiple members who are citizens of countries from the same ICANN Geographic Region.

(d) The IFRT shall be led by two co-chairs: one appointed by the GNSO from one of the members appointed pursuant to clauses (c)-(f) of Section 18.7 and one appointed by the ccNSO from one of the members appointed pursuant to clauses (a)-(b) of Section 18.7.

(e) The PTI Board shall select a PTI staff member to serve as a point of contact to facilitate formal lines of communication between the IFRT and PTI. The Board shall select an ICANN staff member to serve as a point of contact to facilitate formal lines of communication between the IFRT and ICANN.

(f) Liaisons to the IFRT are not members of or entitled to vote on any matters before the IFRT, but otherwise are entitled to participate on equal footing with members of the IFRT.

(g) Other participants are entitled to participate in the IFRT, but are not entitled to vote.

(h) Removal and Replacement of IFRT Members and Liaisons

> (i) The IFRT members and liaisons may be removed from the IFRT by their respective appointing organization at any time upon such organization providing written notice to the Secretary and the co-chairs of the IFRT.
>
> (ii) A vacancy on the IFRT shall be deemed to exist in the event of the death, resignation or removal of any IFRT member or liaison. Vacancies shall be filled by the organization that appointed such IFRT member or liaison. The appointing organization shall provide written notice to the Secretary of its appointment to fill a vacancy, with a notification copy to the IFRT co-chairs. The organization responsible for filling such vacancy shall use its reasonable efforts to fill such vacancy within one month after the occurrence of such vacancy.

Section 18.9. MEETINGS

(a) All actions of the IFRT shall be taken by consensus of the IFRT, which is where a small minority may disagree, but most agree. If consensus cannot be reached with respect to a particular issue, actions by the majority of all of the members of the IFRT shall be the action of the IFRT.

(b) Any members of the IFRT not in favor of an action (whether as a result of voting against a matter or objecting to the consensus position) may record a minority dissent to such action, which shall be included in the IFRT minutes and/or report, as applicable.

(c) IFRT meetings, deliberations and other working procedures shall be open to the public and conducted in a transparent manner to the fullest extent possible.

(d) The IFRT shall transmit minutes of its meetings to the Secretary, who shall cause those minutes to be posted to the Website as soon as practicable following each IFRT meeting. Recordings and transcripts of meetings, as well as mailing lists, shall also be posted to the Website.

Section 18.10. COMMUNITY REVIEWS AND REPORTS

(a) The IFRT shall seek community input as to the issues relevant to the IFR through one or more public comment periods that shall comply with the designated practice for public comment periods within ICANN and through discussions during ICANN's public meetings in developing and finalizing its recommendations and any report.

(b) The IFRT shall provide a draft report of its findings and recommendations to the community for public comment. The public comment period is required to comply with the designated practice for public comment periods within ICANN.

(c) After completion of the IFR, the IFRT shall submit its final report containing its findings and recommendations to the Board. ICANN shall thereafter promptly post the IFRT's final report on the Website.

Section 18.11. ADMINISTRATIVE AND OPERATIONAL SUPPORT

ICANN shall provide administrative and operational support necessary for each IFRT to carry out its responsibilities, including providing and facilitating remote participation in all meetings of the IFRT.

Section 18.12. SPECIAL IFRS

(a) A Special IFR may be initiated outside of the cycle for the Periodic IFRs to address any deficiency, problem or other issue that has adversely affected PTI's performance under the IANA Naming Function Contract and IANA Naming Function SOW (a "**PTI Performance Issue**"), following the satisfaction of each of the following conditions:

> (i) The Remedial Action Procedures of the CSC set forth in the IANA Naming Function Contract shall have been followed and failed to correct the PTI Performance Issue and the outcome of such procedures shall have been reviewed by the ccNSO and GNSO according to each organization's respective operating procedures;

(ii) The IANA Problem Resolution Process set forth in the IANA Naming Function Contract shall have been followed and failed to correct the PTI Performance Issue and the outcome of such process shall have been reviewed by the ccNSO and GNSO according to each organization's respective operating procedures;

(iii) The ccNSO and GNSO shall have considered the outcomes of the processes set forth in the preceding clauses (i) and (ii) and shall have conducted meaningful consultation with the other Supporting Organizations and Advisory Committees with respect to the PTI Performance Issue and whether or not to initiate a Special IFR; and

(iv) After a public comment period that complies with the designated practice for public comment periods within ICANN, if a public comment period is requested by the ccNSO and the GNSO, a Special IFR shall have been approved by the vote of (A) a supermajority of the ccNSO Council (pursuant to the ccNSO's procedures or if such procedures do not define a supermajority, two-thirds (2/3) of the Council members) and (B) a GNSO Supermajority.

(b) Each Special IFR shall be conducted by an IFRT and shall follow the same procedures and requirements applicable to Periodic IFRs as set forth in this Section 18, except that:

(i) The scope of the Special IFR and the related inputs that are required to be reviewed by the IFRT shall be focused primarily on the PTI Performance Issue, its implications for overall IANA naming function performance by PTI and how to resolve the PTI Performance Issue;

(ii) The IFRT shall review and analyze the information that is relevant to the scope of the Special IFR; and

(iii) Each recommendation of the IFRT relating to the Special IFR, including but not limited to any recommendation to initiate an IANA Naming Function Separation Process, must be related to remediating the PTI Performance Issue or other issue with PTI's performance that is related to the IFRT responsibilities set forth in Section 18.3, shall include proposed remedial procedures and describe how those procedures are expected to address the PTI Performance Issue or other relevant issue with PTI's performance.

(c) A recommendation of an IFRT for a Special IFR shall only become effective if, with respect to each such recommendation (each, a "**Special IFR Recommendation**"), each of the following occurs:

> (i) The Special IFR Recommendation has been approved by the vote of (A) a supermajority of the ccNSO Council (pursuant to the ccNSO's procedures or, if such procedures do not define a supermajority, two-thirds (2/3) of the ccNSO Council's members) and (B) a GNSO Supermajority;
>
> (ii) After a public comment period that complies with the designated practice for public comment periods within ICANN, the Board has approved the Special IFR Recommendation; and
>
> (iii) The EC has not rejected the Board's approval of the Special IFR Recommendation pursuant to and in compliance with Section 18.12(e).

(d) If the Board (x) rejects a Special IFR Recommendation that was approved by the ccNSO Council and GNSO Council pursuant to Section 18.12(c)(i) or (y) does not resolve to either accept or reject a Special IFR Recommendation within 45 days of the later of (1) the date that the condition in Section 18.12(c)(i) is satisfied or (2) the expiration of the public comment period contemplated by Section 18.12(c)(ii), the Secretary shall provide a Board Notice to the EC Administration and the Decisional Participants, which Board Notice shall enclose a copy of the applicable Special IFR Recommendation. ICANN shall post the Board Notice, along with a copy of the notification(s) sent to the EC Administration and the Decisional Participants, on the Website promptly following the delivery of the Board Notice to the EC Administration and the Decisional Participants.

> (i) ICANN shall, at the direction of the EC Administration, convene a Rejection Action Community Forum, which Rejection Action Community Forum shall be conducted in accordance with Section 2.3 of Annex D, to discuss the Board Notice; provided, that, for purposes of Section 2.3 of Annex D, (A) the Board Notice shall be treated as the Rejection Action Supported Petition, (B) the EC Administration shall be treated as the Rejection Action Petitioning Decisional Participant (and there shall be no Rejection Action Supporting Decisional Participants) and (C) the Rejection Action Community Forum Period shall expire on the 21st day after the date the Secretary provides the Board Notice to the EC Administration and the Decisional Participants.

(ii) No later than 45 days after the conclusion of such Rejection Action Community Forum Period, the Board shall resolve to either uphold its rejection of the Special IFR Recommendation or approve the Special IFR Recommendation (either, a "**Post-Forum Special IFR Recommendation Decision**").

(A)If the Board resolves to approve the Special IFR Recommendation, such Special IFR Recommendation will be subject to Section 18.6(d).

(B)For the avoidance of doubt, the Board shall not be obligated to change its decision on the Special IFR Recommendation as a result of the Rejection Action Community Forum.

(C)The Board's Post-Forum Special IFR Recommendation Decision shall be posted on the Website in accordance with the Board's posting obligations as set forth in Article 3.

(e) Promptly after the Board approves a Special IFR Recommendation (a "**Special IFR Recommendation Decision**"), the Secretary shall provide a Board Notice to the EC Administration and the Decisional Participants, which Board Notice shall enclose a copy of the Special IFR Recommendation that is the subject of the Special IFR Recommendation Decision. ICANN shall post the Board Notice, along with a copy of the notification(s) sent to the EC Administration and the Decisional Participants, on the Website promptly following the delivery of the Board Notice to the EC Administration and the Decisional Participants. The EC Administration shall promptly commence and comply with the procedures and requirements specified in Article 2 of Annex D.

(i) A Special IFR Recommendation Decision shall become final upon the earliest to occur of the following:

(A)(1) A Rejection Action Petition Notice is not timely delivered by the Rejection Action Petitioning Decisional Participant to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D, in which case the Special IFR Recommendation Decision shall be final as of the date immediately following the expiration of the Rejection Action Petition Period relating to such Special IFR Recommendation Decision;

(B)(1) A Rejection Action Supported Petition is not timely delivered by the

> Rejection Action Petitioning Decisional Participant to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D, in which case the Special IFR Recommendation Decision shall be final as of the date immediately following the expiration of the Rejection Action Petition Support Period relating to such Special IFR Recommendation Decision; and
>
> (C)(1) An EC Rejection Notice is not timely delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4 of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4(c) of Annex D, in which case the Special IFR Recommendation Decision shall be final as of the date immediately following the expiration of the Rejection Action Decision Period relating to such Special IFR Recommendation Decision.
>
> (ii) A Special IFR Recommendation Decision that has been rejected by the EC pursuant to and in compliance with Article 2 of Annex D shall have no force and effect, and shall be void ab initio.

(f) For the avoidance of doubt, Section 18.12(e) shall not apply when the Board acts in a manner that is consistent with a Special IFR Recommendation unless such Special IFR Recommendation relates to an IANA Naming Function Separation Process as described in Article 19.

Section 18.13. PROPOSED SEPARATION PROCESS

The IFRT conducting either a Special IFR or Periodic IFR may, upon conclusion of a Special IFR or Periodic IFR, as applicable, determine that an IANA Naming Function Separation Process is necessary and, if so, it shall recommend the creation of an SCWG pursuant to Article 19.

ARTICLE 19IANA NAMING FUNCTION SEPARATION PROCESS

Section 19.1. ESTABLISHING AN SCWG

(a) An "**IANA Naming Function Separation Process**" is the process initiated in accordance with this Article 19 pursuant to which PTI may cease to perform the IANA naming function including, without limitation, the initiation of a request for proposal to select an operator to perform the IANA naming function instead of PTI

("**IANA Naming Function RFP**"), the selection of an IANA naming function operator other than PTI, termination or non-renewal of the IANA Naming Function Contract, and/or divestiture, or other reorganization of PTI by ICANN.

(b) The Board shall establish an SCWG if each of the following occurs:

> (i) The IFRT conducting either a Special IFR or Periodic IFR, upon conclusion of a Special IFR or Periodic IFR, as applicable, has recommended that an IANA Naming Function Separation Process is necessary and has recommended the creation of an SCWG (an "**SCWG Creation Recommendation**");
>
> (ii) The SCWG Creation Recommendation has been approved by the vote of (A) a supermajority of the ccNSO Council (pursuant to the ccNSO's procedures or, if such procedures do not define a supermajority, two-thirds (2/3) of the ccNSO Council's members) and (B) a GNSO Supermajority;
>
> (iii) After a public comment period that complies with the designated practice for public comment periods within ICANN, the Board has approved the SCWG Creation Recommendation. A determination by the Board to not approve an SCWG Creation Recommendation, where such creation has been approved by the ccNSO and GNSO Councils pursuant to Section 19.1(b)(ii), shall require a vote of at least two-thirds (2/3) of the Board and the Board shall follow the same consultation procedures set forth in Section 9 of Annex A of these Bylaws that relate to Board rejection of a PDP recommendation that is supported by a GNSO Supermajority; and
>
> (iv) The EC has not rejected the Board's approval of the SCWG Creation Recommendation pursuant to and in compliance with Section 19.1(d).

(c) If the Board (x) rejects an SCWG Creation Recommendation that was approved by the ccNSO Council and GNSO Council pursuant to Section 19.1(b)(ii) or (y) does not resolve to either accept or reject an SCWG Creation Recommendation within 45 days of the later of (1) the date that the condition in Section 19.1(b)(ii) is satisfied or (2) the expiration of the public comment period contemplated by Section 19.1(b)(iii), the Secretary shall provide a Board Notice to the EC Administration and the Decisional Participants, which Board Notice shall enclose a copy of the applicable SCWG Creation Recommendation. ICANN shall post the Board Notice, along with a copy of the notification(s) sent to the EC Administration and the Decisional Participants, on the Website promptly following the delivery of the Board Notice to the EC Administration and the Decisional

Participants.

(i) ICANN shall, at the direction of the EC Administration, convene a Rejection Action Community Forum, which Rejection Action Community Forum shall be conducted in accordance with Section 2.3 of Annex D, to discuss the Board Notice; provided, that, for purposes of Section 2.3 of Annex D, (A) the Board Notice shall be treated as the Rejection Action Supported Petition, (B) the EC Administration shall be treated as the Rejection Action Petitioning Decisional Participant (and there shall be no Rejection Action Supporting Decisional Participants) and (C) the Rejection Action Community Forum Period shall expire on the 21st day after the date the Secretary provides the Board Notice to the EC Administration and the Decisional Participants.

(ii) No later than 45 days after the conclusion of such Rejection Action Community Forum Period, the Board shall resolve to either uphold its rejection of the SCWG Creation Recommendation or approve the SCWG Creation Recommendation (either, a "**Post-Forum SCWG Creation Recommendation Decision**").

(A)If the Board resolves to approve the SCWG Creation Recommendation, such SCWG Creation Recommendation will be subject to Section 19.1(d).

(B)For the avoidance of doubt, the Board shall not be obligated to change its decision on the SCWG Creation Recommendation as a result of the Rejection Action Community Forum.

(C)The Board's Post-Forum SCWG Creation Recommendation Decision shall be posted on the Website in accordance with the Board's posting obligations as set forth in Article 3.

(d) Promptly after the Board approves an SCWG Creation Recommendation (an "**SCWG Creation Decision**"), the Secretary shall provide a Board Notice to the EC Administration and the Decisional Participants, which Board Notice shall enclose a copy of the SCWG Creation Decision. ICANN shall post the Board Notice, along with a copy of the notification(s) sent to the EC Administration and the Decisional Participants, on the Website promptly following the delivery of the Board Notice to the EC Administration and the Decisional Participants. The EC Administration shall promptly commence and comply with the procedures and requirements specified in Article 2 of Annex D.

(i) An SCWG Creation Decision shall become final upon the earliest to occur of the following:

(A)(1) A Rejection Action Petition Notice is not timely delivered by the Rejection Action Petitioning Decisional Participant to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D, in which case the SCWG Creation Decision shall be final as of the date immediately following the expiration of the Rejection Action Petition Period relating to such SCWG Creation Decision;

(B)(1) A Rejection Action Supported Petition is not timely delivered by the Rejection Action Petitioning Decisional Participant to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D, in which case the SCWG Creation Decision shall be final as of the date immediately following the expiration of the Rejection Action Petition Support Period relating to such SCWG Creation Decision; and

(C)(1) An EC Rejection Notice is not timely delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4 of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4(c) of Annex D, in which case the SCWG Creation Decision shall be final as of the date immediately following the expiration of the Rejection Action Decision Period relating to such SCWG Creation Decision.

(ii) An SCWG Creation Decision that has been rejected by the EC pursuant to and in compliance with Article 2 of Annex D shall have no force and effect, and shall be void ab initio.

Section 19.2. SCWG RESPONSIBILITIES

The responsibilities of the SCWG shall be as follows:

(a) The SCWG shall determine how to resolve the PTI Performance Issue(s) which the IFRT that conducted the Special IFR or Periodic IFR, as applicable, identified as triggering formation of this SCWG.

(b) If the SCWG recommends the issuance of an IANA Naming Function RFP, the

SCWG shall:

> (i) Develop IANA Naming Function RFP guidelines and requirements for the performance of the IANA naming function, in a manner consistent with ICANN's publicly available procurement guidelines (as in effect immediately prior to the formation of the SCWG); and
>
> (ii) Solicit input from ICANN as well as the global Internet community (through community consultation, including public comment opportunities as necessary that comply with the designated practice for public comment periods within ICANN) on requirements to plan and participate in the IANA Naming Function RFP process.

(c) If an SCWG Recommendation (as defined in Section 19.4(b)) to issue the IANA Naming Function RFP is approved pursuant to Section 19.4(b) and the EC does not reject the relevant SCWG Recommendation Decision pursuant to Section 19.4(d), the SCWG, in consultation with ICANN, shall:

> (i) Issue the IANA Naming Function RFP;
>
> (ii) Review responses from interested candidates to the IANA Naming Function RFP, which may be received from PTI and/or any other entity or person; and
>
> (iii) Recommend the entity that ICANN should contract with to perform the IANA naming function.

(d) If the SCWG recommends an IANA Naming Function Separation Process other than the issuance of an IANA Naming Function RFP, the SCWG shall develop recommendations to be followed with respect to that process and its implementation consistent with the terms of this Article 19. The SCWG shall monitor and manage the implementation of such IANA Naming Function Separation Process.

Section 19.3. COMMUNITY REVIEWS AND REPORTS

(a) The SCWG shall seek community input through one or more public comment periods (such public comment period shall comply with the designated practice for public comment periods within ICANN) and may recommend discussions during

ICANN's public meetings in developing and finalizing its recommendations and any report.

(b) The SCWG shall provide a draft report of its findings and recommendations to the community after convening of the SCWG, which such draft report will be posted for public comment on the Website. The SCWG may post additional drafts of its report for public comment until it has reached its final report.

(c) After completion of its review, the SCWG shall submit its final report containing its findings and recommendations to the Board. ICANN shall promptly post the SCWG's final report on the Website.

Section 19.4. SCWG RECOMMENDATIONS

(a) The recommendations of the SCWG are not limited and could include a variety of recommendations or a recommendation that no action is required; provided, however, that any recommendations must directly relate to the matters discussed in Section 19.2 and comply with this Section 19.4.

(b) ICANN shall not implement an SCWG recommendation (including an SCWG recommendation to issue an IANA Naming Function RFP) unless, with respect to each such recommendation (each, an "**SCWG Recommendation**"), each of the following occurs:

> (i) The SCWG Recommendation has been approved by the vote of (A) a supermajority of the ccNSO Council (pursuant to the ccNSO's procedures or, if such procedures do not define a supermajority, two-thirds (2/3) of the ccNSO Council's members) and (B) a GNSO Supermajority;
>
> (ii) After a public comment period that complies with the designated practice for public comment periods within ICANN, the Board has approved the SCWG Recommendation. A determination by the Board to not approve an SCWG Recommendation, where such SCWG Recommendation has been approved by the ccNSO and GNSO Councils pursuant to Section 19.4(b)(i), shall require a vote of at least two-thirds (2/3) of the Board and the Board shall follow the same consultation procedures set forth in Section 9 of Annex A of these Bylaws that relate to Board rejection of a PDP recommendation that is supported by a GNSO Supermajority; and
>
> (iii) The EC has not rejected the Board's approval of the SCWG Recommendation pursuant to and in compliance with Section 19.4(d).

(c) If the Board (x) rejects an SCWG Recommendation that was approved by the ccNSO Council and GNSO Council pursuant to Section 19.4(b)(i) or (y) does not resolve to either accept or reject an SCWG Recommendation within 45 days of the later of (1) the date that the condition in Section 19.4(b)(i) is satisfied or (2) the expiration of the public comment period contemplated by Section 19.4(b)(ii), the Secretary shall provide a Board Notice to the EC Administration and the Decisional Participants, which Board Notice shall enclose a copy of the applicable SCWG Recommendation. ICANN shall post the Board Notice, along with a copy of the notification(s) sent to the EC Administration and the Decisional Participants, on the Website promptly following the delivery of the Board Notice to the EC Administration and the Decisional Participants.

> (i) ICANN shall, at the direction of the EC Administration, convene a Rejection Action Community Forum, which Rejection Action Community Forum shall be conducted in accordance with Section 2.3 of Annex D, to discuss the Board Notice; provided, that, for purposes of Section 2.3 of Annex D, (A) the Board Notice shall be treated as the Rejection Action Supported Petition, (B) the EC Administration shall be treated as the Rejection Action Petitioning Decisional Participant (and there shall be no Rejection Action Supporting Decisional Participants) and (C) the Rejection Action Community Forum Period shall expire on the 21st day after the date the Secretary provides the Board Notice to the EC Administration and the Decisional Participants.
>
> (ii) No later than 45 days after the conclusion of such Rejection Action Community Forum Period, the Board shall resolve to either uphold its rejection of the SCWG Recommendation or approve the SCWG Recommendation (either, a "**Post-Forum SCWG Recommendation Decision**").

(A)If the Board resolves to approve the SCWG Recommendation, such SCWG Recommendation will be subject to Section 19.4(d).

(B)For the avoidance of doubt, the Board shall not be obligated to change its decision on the SCWG Recommendation as a result of the Rejection Action Community Forum.

(C)The Board's Post-Forum SCWG Recommendation Decision shall be posted on the Website in accordance with the Board's posting obligations as set forth in Article 3.

(d) Promptly after the Board approves an SCWG Recommendation (an "**SCWG Recommendation Decision**"), the Secretary shall provide a Board Notice to the EC Administration and the Decisional Participants, which Board Notice shall enclose a copy of the SCWG Recommendation that is the subject of the SCWG Recommendation Decision. ICANN shall post the Board Notice, along with a copy of the notification(s) sent to the EC Administration and the Decisional Participants, on the Website promptly following the delivery of the Board Notice to the EC Administration and the Decisional Participants. The EC Administration shall promptly commence and comply with the procedures and requirements specified in Article 2 of Annex D.

(i) An SCWG Recommendation Decision shall become final upon the earliest to occur of the following:

(A)(1) A Rejection Action Petition Notice is not timely delivered by the Rejection Action Petitioning Decisional Participant to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D, in which case the SCWG Recommendation Decision shall be final as of the date immediately following the expiration of the Rejection Action Petition Period relating to such SCWG Recommendation Decision;

(B)(1) A Rejection Action Supported Petition is not timely delivered by the Rejection Action Petitioning Decisional Participant to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D, in which case the SCWG Recommendation Decision shall be final as of the date immediately following the expiration of the Rejection Action Petition Support Period relating to such SCWG Recommendation Decision; and

(C)(1) An EC Rejection Notice is not timely delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4 of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4(c) of Annex D, in which case the SCWG Recommendation Decision shall be final as of the date immediately following the expiration of the Rejection Action Decision Period relating to such SCWG Recommendation Decision.

(ii) An SCWG Recommendation Decision that has been rejected by the EC

pursuant to and in compliance with Article 2 of Annex D shall have no force and effect, and shall be void ab initio.

(e) ICANN shall absorb the costs relating to recommendations made by the SCWG, including, without limitation, costs related to the process of selecting or potentially selecting a new operator for the IANA naming function and the operating costs of the successor operator that are necessary for the successor operator's performance of the IANA naming function as ICANN's independent contractor. ICANN shall not be authorized to raise fees from any TLD registry operators to cover the costs associated with implementation of any SCWG Recommendations that specifically relate to the transition to a successor operator. For avoidance of doubt, this restriction shall not apply to collecting appropriate fees necessary to maintain the ongoing performance of the IANA naming function, including those relating to the operating costs of the successor operator.

(f) In the event that (i) an SCWG Recommendation that selects an entity (other than PTI) as a new operator of the IANA naming function is approved pursuant to Section 19.4(b) and (ii) the EC does not reject the relevant SCWG Recommendation Decision pursuant to Section 19.4(d), ICANN shall enter into a contract with the new operator on substantially the same terms recommended by the SCWG and approved as part of such SCWG Recommendation.

(g) As promptly as practical following an SCWG Recommendation Decision becoming final in accordance with this Section 19.4, ICANN shall take all steps reasonably necessary to effect such SCWG Recommendation Decision as soon as practicable.

Section 19.5. SCWG COMPOSITION

(a) Each SCWG shall consist of the following members and liaisons to be appointed in accordance with the rules and procedures of the appointing organization:

(i) Two representatives appointed by the ccNSO from its ccTLD registry operator representatives;

(ii) One non-ccNSO ccTLD representative who is associated with a ccTLD registry operator that is not a representative of the ccNSO, appointed by the ccNSO; it is strongly recommended that the ccNSO consult with the

regional ccTLD organizations (i.e., AfTLD, APTLD, LACTLD and CENTR) in making its appointment;

(iii) Three representatives appointed by the Registries Stakeholder Group;

(iv) One representative appointed by the Registrars Stakeholder Group;

(v) One representative appointed by the Commercial Stakeholder Group;

(vi) One representative appointed by the Non-Commercial Stakeholder Group;

(vii) One representative appointed by the GAC;

(viii) One representative appointed by the SSAC;

(ix) One representative appointed by the RSSAC;

(x) One representative appointed by the ALAC;

(xi) One liaison appointed by the CSC;

(xii) One liaison appointed by the IFRT that conducted the Special IFR or Periodic IFR, as applicable, that recommended the creation of the SCWG, who shall be named in the IFRT's recommendation to convene the Special IFR;

(xiii) One liaison who may be appointed by the ASO;

(xiv) One liaison who may be appointed by the IAB; and

(xv) One liaison who may be appointed by the Board.

(xvi) The SCWG may also include an unlimited number of non-member, non-liaison participants.

(b) All candidates for appointment to the SCWG as a member or liaison shall submit an expression of interest to the organization that would appoint such candidate as a member or liaison, which shall state (i) why the candidate is interested in becoming involved in the SCWG, (ii) what particular skills the candidate would bring to the SCWG, (iii) the candidate's knowledge of the IANA naming function, (iv) the candidate's understanding of the purpose of the SCWG, and (v)that the candidate understands the time necessary to participate in the

SCWG process and can commit to the role.

(c) Members and liaisons of the SCWG shall disclose to ICANN and the SCWG any conflicts of interest with a specific complaint or issue under review. The SCWG may exclude from the discussion of a specific complaint or issue any member, liaison or participant deemed by the majority of SCWG members to have a conflict of interest. The co-chairs of the SCWG shall record any such conflict of interest in the minutes of the SCWG.

(d) To the extent reasonably possible, the appointing organizations for SCWG members and liaisons shall work together to:

> (i) achieve an SCWG that is balanced for diversity (including functional, geographic and cultural) and skill, and should seek to broaden the number of individuals participating across the various reviews; provided, that the SCWG should include members from each ICANN Geographic Region, and the ccNSO and Registries Stakeholder Group shall not appoint multiple members who are citizens of countries from the same ICANN Geographic Region;
>
> (ii) ensure that the SCWG is comprised of individuals who are different from those individuals who comprised the IFRT that conducted the Special IFR or Periodic IFR, as applicable, that recommended the creation of the SCWG, other than the liaison to the IFRT appointed by the CSC; and
>
> (iii) seek to appoint as representatives of the SCWG as many individuals as practicable with experience managing or participating in RFP processes.

(e) ICANN shall select an ICANN staff member and a PTI staff member to serve as points of contact to facilitate formal lines of communication between the SCWG and ICANN and the SCWG and PTI. Communications between the SCWG and the ICANN and PTI points of contact shall be communicated by the SCWG co-chairs.

(f) The SCWG shall not be a standing body. Each SCWG shall be constituted when and as required under these Bylaws and shall dissolve following the end of the process for approving such SCWG's SCWG Recommendations pursuant to Section 19.4(d).

Section 19.6. ELECTION OF CO-CHAIRS AND LIAISONS

(a) The SCWG shall be led by two co-chairs: one appointed by the GNSO from one of the members appointed pursuant to clauses (iii)-(vi) of Section 19.5(a) and one appointed by the ccNSO from one of the members appointed pursuant to clauses (i)-(ii) of Section 19.5(a).

(b) Liaisons to the SCWG shall not be members of or entitled to vote on any matters before the SCWG, but otherwise shall be entitled to participate on equal footing with SCWG members.

(c) Removal and Replacement of SCWG Members and Liaisons

> (i) The SCWG members and liaisons may be removed from the SCWG by their respective appointing organization at any time upon such organization providing written notice to the Secretary and the co-chairs of the SCWG.
>
> (ii) A vacancy on the SCWG shall be deemed to exist in the event of the death, resignation or removal of any SCWG member or liaison. Vacancies shall be filled by the organization that appointed such SCWG member or liaison. The appointing organization shall provide written notice to the Secretary of its appointment to fill a vacancy, with a notification copy to the SCWG co-chairs. The organization responsible for filling such vacancy shall use its reasonable efforts to fill such vacancy within one month after the occurrence of such vacancy.

Section 19.7. MEETINGS

(a) The SCWG shall act by consensus, which is where a small minority may disagree, but most agree.

(b) Any members of the SCWG not in favor of an action may record a minority dissent to such action, which shall be included in the SCWG minutes and/or report, as applicable.

(c) SCWG meetings and other working procedures shall be open to the public and conducted in a transparent manner to the fullest extent possible.

(d) The SCWG shall transmit minutes of its meetings to the Secretary, who shall cause those minutes to be posted to the Website as soon as practicable following each SCWG meeting, and no later than five business days following the meeting.

(e) Except as otherwise provided in these Bylaws, the SCWG shall follow the

guidelines and procedures applicable to ICANN Cross Community Working Groups that will be publicly available and may be amended from time to time.

Section 19.8. ADMINISTRATIVE SUPPORT

ICANN shall provide administrative and operational support necessary for the SCWG to carry out its responsibilities, including providing and facilitating remote participation in all meetings of the SCWG.

Section 19.9. CONFLICTING PROVISIONS

In the event any SCWG Recommendation that is approved in accordance with this Article 19 requires ICANN to take any action that is inconsistent with a provision of the Bylaws (including any action taken in implementing such SCWG Recommendation), the requirements of such provision of these Bylaws shall not apply to the extent of that inconsistency.

ARTICLE 20 INDEMNIFICATION OF DIRECTORS, OFFICERS, EMPLOYEES, AND OTHER AGENTS

Section 20.1. INDEMNIFICATION GENERALLY

ICANN shall, to the maximum extent permitted by the CCC, indemnify each of its agents against expenses, judgments, fines, settlements, and other amounts actually and reasonably incurred in connection with any proceeding arising by reason of the fact that any such person is or was an agent of ICANN, provided that the indemnified person's acts were done in good faith and in a manner that the indemnified person reasonably believed to be in ICANN's best interests and not criminal. For purposes of this Article 20, an "agent" of ICANN includes any person who is or was a Director, Officer, employee, or any other agent of ICANN (including a member of the EC, the EC Administration, any Supporting Organization, any Advisory Committee, the Nominating Committee, any other ICANN committee, or the Technical Liaison Group) acting within the scope of his or her responsibility; or is or was serving at the request of ICANN as a Director, Officer, employee, or agent of another corporation, partnership, joint venture, trust, or other enterprise. The Board may adopt a resolution authorizing the purchase and maintenance of insurance on behalf of any agent of ICANN against any liability asserted against or incurred by the agent in such capacity or arising out of the agent's status as such, whether or not ICANN would have the power to indemnify the agent against that liability under the provisions of this Article 20.

Section 20.2. INDEMNIFICATION WITH RESPECT TO DIRECTOR REMOVAL

If a Director initiates any proceeding in connection with his or her removal or recall pursuant to the Bylaws, to which a person who is a member of the leadership council (or equivalent body) of a Decisional Participant or representative of a Decisional Participant in the EC Administration is a party or is threatened to be made a party (as a party or witness) (a "**Director Removal Proceeding**"), ICANN shall, to the maximum extent permitted by the CCC, indemnify any such person, against expenses, judgments, fines, settlements, and other amounts actually and reasonably incurred by such person in connection with such Director Removal Proceeding, for actions taken by such person in his or her representative capacity within his or her Decisional Participant pursuant to the processes and procedures set forth in these Bylaws, provided that all such actions were taken by such person in good faith and in a manner that such person reasonably believed to be in ICANN's best interests and not criminal. The actual and reasonable legal fees of a single firm of counsel and other expenses actually and reasonably incurred by such person in defending against a Director Removal Proceeding shall be paid by ICANN in advance of the final disposition of such Director Removal Proceeding, provided, however, that such expenses shall be advanced only upon delivery to the Secretary of an undertaking (which shall be in writing and in a form provided by the Secretary) by such person to repay the amount of such expenses if it shall ultimately be determined that such person is not entitled to be indemnified by ICANN. ICANN shall not be obligated to indemnify such person against any settlement of a Director Removal Proceeding, unless such settlement is approved in advance by the Board in its reasonable discretion. Notwithstanding Section 20.1, the indemnification provided in this Section 20.2 shall be ICANN's sole indemnification obligation with respect to the subject matter set forth in this Section 20.2.

ARTICLE 21 GENERAL PROVISIONS

Section 21.1. CONTRACTS

The Board may authorize any Officer or Officers, agent or agents, to enter into any contract or execute or deliver any instrument in the name of and on behalf of ICANN, and such authority may be general or confined to specific instances. In the absence of a contrary Board authorization, contracts and instruments may only be executed by the following Officers: President, any Vice President, or the CFO. Unless authorized or ratified by the Board, no other Officer, agent, or employee shall have any power or authority to bind ICANN or to render it liable for any debts or obligations.

Section 21.2. DEPOSITS

All funds of ICANN not otherwise employed shall be deposited from time to time to

the credit of ICANN in such banks, trust companies, or other depositories as the Board, or the President under its delegation, may select.

Section 21.3. CHECKS

All checks, drafts, or other orders for the payment of money, notes, or other evidences of indebtedness issued in the name of ICANN shall be signed by such Officer or Officers, agent or agents, of ICANN and in such a manner as shall from time to time be determined by resolution of the Board.

Section 21.4. LOANS

No loans shall be made by or to ICANN and no evidences of indebtedness shall be issued in its name unless authorized by a resolution of the Board. Such authority may be general or confined to specific instances; provided, however, that no loans shall be made by ICANN to its Directors or Officers.

Section 21.5. NOTICES

All notices to be given to the EC Administration, the Decisional Participants, or the Secretary pursuant to any provision of these Bylaws shall be given either (a) in writing at the address of the appropriate party as set forth below or (b) via electronic mail as provided below, unless that party has given a notice of change of postal or email address, as provided in this Section 21.5. Any change in the contact information for notice below will be given by the party within 30 days of such change. Any notice required by these Bylaws will be deemed to have been properly given (i) if in paper form, when delivered in person or via courier service with confirmation of receipt or (ii) if via electronic mail, upon confirmation of receipt by the recipient's email server, provided that such notice via electronic mail shall be followed by a copy sent by regular postal mail service within three days. In the event other means of notice become practically achievable, such as notice via a secure website, the EC Administration, the Decisional Participants, and ICANN will work together to implement such notice means.

If to ICANN, addressed to:

Internet Corporation for Assigned Names and Numbers

12025 Waterfront Drive, Suite 300

Los Angeles, CA 90094-2536

USA

Email: [___]

Attention: Secretary

If to a Decisional Participant or the EC Administration, addressed to the contact information available at [insert Website reference].

ARTICLE 22 FISCAL AND STRATEGIC MATTERS, INSPECTION AND INDEPENDENT INVESTIGATION

Section 22.1. ACCOUNTING

The fiscal year end of ICANN shall be determined by the Board.

Section 22.2. AUDIT

At the end of the fiscal year, the books of ICANN shall be closed and audited by certified public accountants. The appointment of the fiscal auditors shall be the responsibility of the Board.

Section 22.3. ANNUAL REPORT AND ANNUAL STATEMENT

The Board shall publish, at least annually, a report describing its activities, including an audited financial statement, a description of any payments made by ICANN to Directors (including reimbursements of expenses) and a description of ICANN's progress towards the obligations imposed under the Bylaws as revised on 1 October 2016 and the Operating Plan and Strategic Plan. ICANN shall cause the annual report and the annual statement of certain transactions as required by the CCC to be prepared and sent to each member of the Board and to such other persons as the Board may designate, no later than one hundred twenty (120) days after the close of ICANN's fiscal year.

Section 22.4. BUDGETS

(a) ICANN Budget

> (i) In furtherance of its Commitment to transparent and accountable budgeting processes, at least forty-five (45) days prior to the commencement of each fiscal year, ICANN staff shall prepare and submit to the Board a proposed annual operating plan and budget of ICANN for the next fiscal year (the "**ICANN Budget**"), which shall be posted on the

Website. The ICANN Budget shall identify anticipated revenue sources and levels and shall, to the extent practical, identify anticipated material expense items by line item.

(ii) Prior to approval of the ICANN Budget by the Board, ICANN staff shall consult with the Supporting Organizations and Advisory Committees during the ICANN Budget development process, and comply with the requirements of this Section 22.4(a).

(iii) Prior to approval of the ICANN Budget by the Board, a draft of the ICANN Budget shall be posted on the Website and shall be subject to public comment.

(iv) After reviewing the comments submitted during the public comment period, the Board may direct ICANN staff to post a revised draft of the ICANN Budget and may direct ICANN Staff to conduct one or more additional public comment periods of lengths determined by the Board, in accordance with ICANN's public comment processes.

(v) Promptly after the Board approves an ICANN Budget (an "**ICANN Budget Approval**"), the Secretary shall provide a Board Notice to the EC Administration and the Decisional Participants, which Board Notice shall enclose a copy of the ICANN Budget that is the subject of the ICANN Budget Approval. ICANN shall post the Board Notice, along with a copy of the notification(s) sent to the EC Administration and the Decisional Participants, on the Website promptly following the delivery of the Board Notice to the EC Administration and the Decisional Participants. The EC Administration shall promptly commence and comply with the procedures and requirements specified in Article 2 of Annex D.

(vi) An ICANN Budget shall become effective upon the earliest to occur of the following:

(A)(1) A Rejection Action Petition Notice is not timely delivered by the Rejection Action Petitioning Decisional Participant to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D, in which case the ICANN Budget that is the subject of the ICANN Budget Approval shall be in full force and effect as of the 28th day following the Rejection Action Board Notification Date (as defined in Section 2.2(a) of Annex D) relating to such ICANN Budget Approval and the effectiveness of such ICANN Budget shall not be subject to further challenge by the EC pursuant to the EC's rejection right as described in Article 2 of Annex D;

(B)(1) A Rejection Action Supported Petition is not timely delivered by the Rejection Action Petitioning Decisional Participant to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D, in which case the ICANN Budget that is the subject of the ICANN Budget Approval shall be in full force and effect as of the date immediately following the expiration of the Rejection Action Petition Support Period relating to such ICANN Budget Approval and the effectiveness of such ICANN Budget shall not be subject to further challenge by the EC pursuant to the EC's rejection right as described in Article 2 of Annex D; and

(C)(1) An EC Rejection Notice is not timely delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4 of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4(c) of Annex D, in which case the ICANN Budget that is the subject of the ICANN Budget Approval shall be in full force and effect as of the date immediately following the expiration of the Rejection Action Decision Period relating to such ICANN Budget Approval and the effectiveness of such ICANN Budget shall not be subject to further challenge by the EC pursuant to the EC's rejection right as described in Article 2 of Annex D.

(vii) An ICANN Budget that has been rejected by the EC pursuant to and in compliance with Article 2 of Annex D shall have no force and effect, and shall be void ab initio.

(viii) Following receipt of an EC Rejection Notice relating to an ICANN Budget, ICANN staff and the Board shall consider the explanation provided by the EC Administration as to why the EC has chosen to reject the ICANN Budget in determining the substance of such new ICANN Budget, which shall be subject to the procedures of this Section 22.4(a).

(ix) If an ICANN Budget has not come into full force and effect pursuant to this Section 22.4(a) on or prior to the first date of any fiscal year of ICANN, the Board shall adopt a temporary budget in accordance with Annex E hereto ("**Caretaker ICANN Budget**"), which Caretaker ICANN Budget shall be effective until such time as an ICANN Budget has been effectively approved by the Board and not rejected by the EC pursuant to this Section 22.4(a).

(b) IANA Budget

(i) At least 45 days prior to the commencement of each fiscal year, ICANN shall prepare and submit to the Board a proposed annual operating plan and budget of PTI and the IANA department, which budget shall include itemization of the direct costs for ICANN's IANA department, all costs for PTI, direct costs for shared resources between ICANN and PTI and support functions provided by ICANN to PTI and ICANN's IANA department for the next fiscal year (the "**IANA Budget**"), which shall be posted on the Website. Separately and in addition to the general ICANN planning process, ICANN shall require PTI to prepare and submit to the PTI Board a proposed annual operating plan and budget for PTI's performance of the IANA functions for the next fiscal year ("**PTI Budget**"). ICANN shall require PTI to consult with the Supporting Organizations and Advisory Committees, as well as the Registries Stakeholder Group, the IAB and RIRs, during the PTI Budget development process, and shall seek public comment on the draft PTI Budget prior to approval of the PTI Budget by PTI. ICANN shall require PTI to submit the PTI Budget to ICANN as an input prior to and for the purpose of being included in the proposed Operating Plan (as defined in Section 22.5(a)) and ICANN Budget.

(ii) Prior to approval of the IANA Budget by the Board, ICANN staff shall consult with the Supporting Organizations and Advisory Committees, as well as the Registries Stakeholder Group, IAB and RIRs, during the IANA Budget development process, and comply with the requirements of this Section 22.4(b).

(iii) Prior to approval of the IANA Budget by the Board, a draft of the IANA Budget shall be posted on the Website and shall be subject to public comment.

(iv) After reviewing the comments submitted during the public comment period, the Board may direct ICANN staff to post a revised draft of the IANA Budget and may direct ICANN staff to conduct one or more additional public comment periods of lengths determined by the Board, in accordance with ICANN's public comment processes.

(v) Promptly after the Board approves an IANA Budget (an "**IANA Budget Approval**"), the Secretary shall provide a Board Notice to the EC Administration and the Decisional Participants, which Board Notice shall enclose a copy of the IANA Budget that is the subject of the IANA Budget Approval. ICANN shall post the Board Notice, along with a copy of the notification(s) sent to the EC Administration and the Decisional Participants,

on the Website promptly following the delivery of the Board Notice to the EC Administration and the Decisional Participants. The EC Administration shall promptly commence and comply with the procedures and requirements specified in Article 2 of Annex D.

(vi) An IANA Budget shall become effective upon the earliest to occur of the following:

(A)(1) A Rejection Action Petition Notice is not timely delivered by the Rejection Action Petitioning Decisional Participant to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D, in which case the IANA Budget that is the subject of the IANA Budget Approval shall be in full force and effect as of the 28th day following the Rejection Action Board Notification Date relating to such IANA Budget Approval and the effectiveness of such IANA Budget shall not be subject to further challenge by the EC pursuant to the EC's rejection right as described in Article 2 of Annex D;

(B)(1) A Rejection Action Supported Petition is not timely delivered by the Rejection Action Petitioning Decisional Participant to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D, in which case the IANA Budget that is the subject of the IANA Budget Approval shall be in full force and effect as of the date immediately following the expiration of the Rejection Action Petition Support Period relating to such IANA Budget Approval and the effectiveness of such IANA Budget shall not be subject to further challenge by the EC pursuant to the EC's rejection right as described in Article 2 of Annex D; and

(C)(1) An EC Rejection Notice is not timely delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4 of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4(c) of Annex D, in which case the IANA Budget that is the subject of the IANA Budget Approval shall be in full force and effect as of the date immediately following the expiration of the Rejection Action Decision Period relating to such IANA Budget Approval and the effectiveness of such IANA Budget shall not be subject to further challenge by the EC pursuant to the EC's rejection right as described in Article 2 of Annex D.

(vii) An IANA Budget that has been rejected by the EC pursuant to and in compliance with Article 2 of Annex D shall have no force and effect, and shall be void ab initio.

(viii) Following receipt of an EC Rejection Notice relating to an IANA Budget, ICANN staff and the Board shall consider the explanation provided by the EC Administration as to why the EC has chosen to reject the IANA Budget in determining the substance of such new IANA Budget, which shall be subject to the procedures of this Section 22.4(b).

(ix) If an IANA Budget has not come into full force and effect pursuant to this Section 22.4(b) on or prior to the first date of any fiscal year of ICANN, the Board shall adopt a temporary budget in accordance with Annex F hereto ("**Caretaker IANA Budget**"), which Caretaker IANA Budget shall be effective until such time as an IANA Budget has been effectively approved by the Board and not rejected by the EC pursuant to this Section 22.4(b).

(c) If an IANA Budget does not receive an EC Rejection Notice but an ICANN Budget receives an EC Rejection Notice, any subsequent revised ICANN Budget shall not alter the expenditures allocated for the IANA Budget.

(d) If an ICANN Budget does not receive an EC Rejection Notice but an IANA Budget receives an EC Rejection Notice, any subsequent revised IANA Budget shall, once approved, be deemed to automatically modify the ICANN Budget in a manner determined by the Board without any further right of the EC to reject the ICANN Budget.

(e) Under all circumstances, the Board will have the ability to make out-of-budget funding decisions for unforeseen expenses necessary to maintaining ICANN's Mission or to fulfilling ICANN's pre-existing legal obligations and protecting ICANN from harm or waste.

(f) To maintain ongoing operational excellence and financial stability of the IANA functions (so long as they are performed by ICANN or pursuant to contract with ICANN) and PTI, ICANN shall be required to plan for and allocate funds to ICANN's performance of the IANA functions and to PTI, as applicable, that are sufficient to cover future expenses and contingencies to ensure that the performance of those IANA functions and PTI in the future are not interrupted due to lack of funding.

(g) The ICANN Budget and the IANA Budget shall be published on the Website.

Section 22.5. PLANS

(a) Operating Plan

(i) At least 45 days prior to the commencement of each fiscal year, ICANN staff shall prepare and submit to the Board a proposed operating plan of ICANN for the next five fiscal years (the "**Operating Plan**"), which shall be posted on the Website.

(ii) Prior to approval of the Operating Plan by the Board, ICANN staff shall consult with the Supporting Organizations and Advisory Committees during the Operating Plan development process, and comply with the requirements of this Section 22.5(a).

(iii) Prior to approval of the Operating Plan by the Board, a draft of the Operating Plan shall be posted on the Website and shall be subject to public comment.

(iv) After reviewing the comments submitted during the public comment period, the Board may direct ICANN staff to post a revised draft of the Operating Plan and may direct ICANN staff to conduct one or more additional public comment periods of lengths determined by the Board, in accordance with ICANN's public comment processes.

(v) Promptly after the Board approves an Operating Plan (an "**Operating Plan Approval**"), the Secretary shall provide a Board Notice to the EC Administration and the Decisional Participants, which Board Notice shall enclose a copy of the Operating Plan that is the subject of the Operating Plan Approval. ICANN shall post the Board Notice, along with a copy of the notification(s) sent to the EC Administration and the Decisional Participants, on the Website promptly following the delivery of the Board Notice to the EC Administration and the Decisional Participants. The EC Administration shall promptly commence and comply with the procedures and requirements specified in Article 2 of Annex D.

(vi) An Operating Plan shall become effective upon the earliest to occur of the following:

(A)(1) A Rejection Action Petition Notice is not timely delivered by the Rejection Action Petitioning Decisional Participant to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D, in

which case the Operating Plan that is the subject of the Operating Plan Approval shall be in full force and effect as of the 28th day following the Rejection Action Board Notification Date relating to such Operating Plan Approval and the effectiveness of such Operating Plan shall not be subject to further challenge by the EC pursuant to the EC's rejection right as described in Article 2 of Annex D;

(B)(1) A Rejection Action Supported Petition is not timely delivered by the Rejection Action Petitioning Decisional Participant to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D, in which case the Operating Plan that is the subject of the Operating Plan Approval shall be in full force and effect as of the date immediately following the expiration of the Rejection Action Petition Support Period relating to such Operating Plan Approval and the effectiveness of such Operating Plan shall not be subject to further challenge by the EC pursuant to the EC's rejection right as described in Article 2 of Annex D; and

(C)(1) An EC Rejection Notice is not timely delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4 of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4(c) of Annex D, in which case the Operating Plan that is the subject of the Operating Plan Approval shall be in full force and effect as of the date immediately following the expiration of the Rejection Action Decision Period relating to such Operating Plan Approval and the effectiveness of such Operating Plan shall not be subject to further challenge by the EC pursuant to the EC's rejection right as described in Article 2 of Annex D.

(vii) An Operating Plan that has been rejected by the EC pursuant to and in compliance with Article 2 of Annex D shall have no force and effect, and shall be void ab initio.

(viii) Following receipt of an EC Rejection Notice relating to an Operating Plan, ICANN staff and the Board shall consider the explanation provided by the EC Administration as to why the EC has chosen to reject the Operating Plan in determining the substance of such new Operating Plan, which shall be subject to the procedures of this Section 22.5(a).

(b) Strategic Plan

(i) At least 45 days prior to the commencement of each five fiscal year period, with the first such period covering fiscal years 2021 through 2025, ICANN staff shall prepare and submit to the Board a proposed strategic plan of ICANN for the next five fiscal years (the "**Strategic Plan**"), which shall be posted on the Website.

(ii) Prior to approval of the Strategic Plan by the Board, ICANN staff shall consult with the Supporting Organizations and Advisory Committees during the Strategic Plan development process, and comply with the requirements of this Section 22.5(b).

(iii) Prior to approval of the Strategic Plan by the Board, a draft of the Strategic Plan shall be posted on the Website and shall be subject to public comment.

(iv) After reviewing the comments submitted during the public comment period, the Board may direct ICANN staff to submit a revised draft of the Strategic Plan and may direct ICANN staff to conduct one or more additional public comment periods of lengths determined by the Board, in accordance with ICANN's public comment processes.

(v) Promptly after the Board approves a Strategic Plan (a "**Strategic Plan Approval**"), the Secretary shall provide a Board Notice to the EC Administration and the Decisional Participants, which Board Notice shall enclose a copy of the Strategic Plan that is the subject of the Strategic Plan Approval. ICANN shall post the Board Notice, along with a copy of the notification(s) sent to the EC Administration and the Decisional Participants, on the Website promptly following the delivery of the Board Notice to the EC Administration and the Decisional Participants. The EC Administration shall promptly commence and comply with the procedures and requirements specified in Article 2 of Annex D.

(vi) A Strategic Plan shall become effective upon the earliest to occur of the following:

(A)(1) A Rejection Action Petition Notice is not timely delivered by the Rejection Action Petitioning Decisional Participant to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D, in which case the Strategic Plan that is the subject of the Strategic Plan Approval shall be in full force and effect as of the 28th day following the

Rejection Action Board Notification Date relating to such Strategic Plan Approval and the effectiveness of such Strategic Plan shall not be subject to further challenge by the EC pursuant to the EC's rejection right as described in Article 2 of Annex D;

(B)(1) A Rejection Action Supported Petition is not timely delivered by the Rejection Action Petitioning Decisional Participant to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D, in which case the Strategic Plan that is the subject of the Strategic Plan Approval shall be in full force and effect as of the date immediately following the expiration of the Rejection Action Petition Support Period relating to such Strategic Plan Approval and the effectiveness of such Strategic Plan shall not be subject to further challenge by the EC pursuant to the EC's rejection right as described in Article 2 of Annex D; and

(C)(1) An EC Rejection Notice is not timely delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4 of Annex D or (2) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4(c) of Annex D, in which case the Strategic Plan that is the subject of the Strategic Plan Approval shall be in full force and effect as of the date immediately following the expiration of the Rejection Action Decision Period relating to such Strategic Plan Approval and the effectiveness of such Strategic Plan shall not be subject to further challenge by the EC pursuant to the EC's rejection right as described in Article 2 of Annex D.

(vii) A Strategic Plan that has been rejected by the EC pursuant to and in compliance with Article 2 of Annex D shall have no force and effect, and shall be void ab initio.

(viii) Following receipt of an EC Rejection Notice relating to a Strategic Plan, ICANN staff and the Board shall consider the explanation provided by the EC Administration as to why the EC has chosen to reject the Strategic Plan in determining the substance of such new Strategic Plan, which shall be subject to the procedures of this Section 22.5(b).

Section 22.6. FEES AND CHARGES

The Board may set fees and charges for the services and benefits provided by

ICANN, with the goal of fully recovering the reasonable costs of the operation of ICANN and establishing reasonable reserves for future expenses and contingencies reasonably related to the legitimate activities of ICANN. Such fees and charges shall be fair and equitable, shall be published for public comment prior to adoption, and once adopted shall be published on the Website in a sufficiently detailed manner so as to be readily accessible.

Section 22.7. INSPECTION

(a) A Decisional Participant (the "**Inspecting Decisional Participant**") may request to inspect the accounting books and records of ICANN, as interpreted pursuant to the provisions of Section 6333 of the CCC, and the minutes of the Board or any Board Committee for a purpose reasonably related to such Inspecting Decisional Participant's interest as a Decisional Participant in the EC. The Inspecting Decisional Participant shall make such a request by providing written notice from the chair of the Inspecting Decisional Participant to the Secretary stating the nature of the documents the Inspecting Decisional Participant seeks to inspect ("**Inspection Request**"). Any Inspection Request must be limited to the accounting books and records of ICANN relevant to the operation of ICANN as a whole, and shall not extend to the underlying sources of such accounting books or records or to documents only relevant to a small or isolated aspect of ICANN's operations or that relate to the minutiae of ICANN's financial records or details of its management and administration (the "**Permitted Scope**"). Unless ICANN declines such request (as provided below), ICANN shall make the records requested under an Inspection Request available for inspection by such Inspecting Decisional Participant within 30 days of the date the Inspection Request is received by the Secretary or as soon as reasonably practicable thereafter. All materials and information made available by ICANN for inspection pursuant to an Inspection Request may only be used by the Inspecting Decisional Participant for purposes reasonably related to such Inspecting Decisional Participant's interest as a Decisional Participant in the EC. ICANN shall post all Inspection Requests to the Website.

(b) ICANN may decline an Inspection Request on the basis that such Inspection Request (i) is motivated by a Decisional Participant's financial, commercial or political interests, or those of one or more of its constituents, (ii) relates to documents that are not reasonably related to the purpose specified in the Inspection Request or the Inspecting Decisional Participant's interest as a Decisional Participant in the EC, (iii) requests identical records provided in a prior request of such Decisional Participant, (iv) is not within the Permitted Scope, (v) relates to personnel records, (vi) relates to documents or communications covered by attorney-client privilege, work product doctrine or other legal privilege or (vii) relates to documents or communications that ICANN may not make available

under applicable law because such documents or communications contain confidential information that ICANN is required to protect. If an Inspection Request is overly broad, ICANN may request a revised Inspection Request from the Inspecting Decisional Participant.

(c) Any such inspections shall be conducted at the times and locations reasonably determined by ICANN and shall not be conducted in a manner that unreasonably interferes with ICANN's operations. All such inspections shall be subject to reasonable procedures established by ICANN, including, without limitation, the number of individuals authorized to conduct any such inspection on behalf of the Inspecting Decisional Participant. ICANN may require the inspectors to sign a non-disclosure agreement. The Inspecting Decisional Participant may, at its own cost, copy or otherwise reproduce or make a record of materials inspected. ICANN may redact or determine not to provide requested materials on the same basis that such information is of a category or type described in Section 22.7(b), in which case ICANN will provide the Inspecting Decisional Participant a written rationale for such redactions or determination.

(d) The inspection rights provided to the Decisional Participants pursuant to this Section 22.7 are granted to the Decisional Participants and are not granted or available to any other person or entity. Notwithstanding the foregoing, nothing in this Section 22.7 shall be construed as limiting the accessibility of ICANN's document information disclosure policy ("**DIDP**").

(e) If the Inspecting Decisional Participant believes that ICANN has violated the provisions of this Section 22.7, the Inspecting Decisional Participant may seek one or more of the following remedies: (i) appeal such matter to the Ombudsman and/or the Board for a ruling on the matter, (ii) initiate the Reconsideration Request process in accordance with Section 4.2, (iii) initiate the Independent Review Process in accordance with Section 4.3, or (iv) petition the EC to initiate (A) a Community IRP pursuant to Section 4.2 of Annex D or (B) a Board Recall Process pursuant to Section 3.3 of Annex D. Any determination by the Ombudsman is not binding on ICANN staff, but may be submitted by the Inspecting Decisional Participant when appealing to the Board for a determination, if necessary.

Section 22.8. INDEPENDENT INVESTIGATION

If three or more Decisional Participants deliver to the Secretary a joint written certification from the respective chairs of each such Decisional Participant that the constituents of such Decisional Participants have, pursuant to the internal procedures of such Decisional Participants, determined that there is a credible allegation that ICANN has committed fraud or that there has been a gross mismanagement of ICANN's resources, ICANN shall retain a third-party,

independent firm to investigate such alleged fraudulent activity or gross mismanagement. ICANN shall post all such certifications to the Website. The independent firm shall issue a report to the Board. The Board shall consider the recommendations and findings set forth in such report. Such report shall be posted on the Website, which may be in a redacted form as determined by the Board, in order to preserve attorney-client privilege, work product doctrine or other legal privilege or where such information is confidential, in which case ICANN will provide the Decisional Participants that submitted the certification a written rationale for such redactions.

ARTICLE 23 MEMBERS

ICANN shall not have members, as contemplated by Section 5310 of the CCC, notwithstanding the use of the term "member" in these Bylaws, in any ICANN document, or in any action of the Board or staff. For the avoidance of doubt, the EC is not a member of ICANN.

ARTICLE 24 OFFICES AND SEAL

Section 24.1. OFFICES

The principal office for the transaction of the business of ICANN shall be in the County of Los Angeles, State of California, United States of America. ICANN may also have an additional office or offices within or outside the United States of America as it may from time to time establish.

Section 24.2. SEAL

The Board may adopt a corporate seal and use the same by causing it or a facsimile thereof to be impressed or affixed or reproduced or otherwise.

ARTICLE 25 AMENDMENTS

Section 25.1. AMENDMENTS TO THE STANDARD BYLAWS

(a) Except as otherwise provided in the Articles of Incorporation or these Bylaws, these Bylaws may be altered, amended, or repealed and new Bylaws adopted only upon approval by a two-thirds vote of all Directors and in compliance with the terms of this Section 25.1 (a "**Standard Bylaw Amendment**").

(b) Prior to approval of a Standard Bylaw Amendment by the Board, a draft of the Standard Bylaw Amendment shall be posted on the Website and shall be subject to public comment in accordance with ICANN's public comment processes.

(c) After reviewing the comments submitted during the public comment period, the Board may direct ICANN staff to post a revised draft of the Standard Bylaw Amendment and may conduct one or more additional public comment periods in accordance with ICANN's public comment processes.

(d) Within seven days after the Board's approval of a Standard Bylaw Amendment ("**Standard Bylaw Amendment Approval**"), the Secretary shall (i) provide a Board Notice to the EC Administration and the Decisional Participants, which Board Notice shall contain the form of the approved amendment and the Board's rationale for adopting such amendment, and (ii) post the Board Notice, along with a copy of the notification(s) sent to the EC Administration and the Decisional Participants, on the Website. The steps contemplated in Article 2 of Annex D shall then be followed.

(e) A Standard Bylaw Amendment shall become effective upon the earliest to occur of the following:

> (i) (A) A Rejection Action Petition Notice is not timely delivered by the Rejection Action Petitioning Decisional Participant to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D or (B) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(c) of Annex D, in which case the Standard Bylaw Amendment that is the subject of the Standard Bylaw Amendment Approval shall be in full force and effect as of the 30th day following the Rejection Action Board Notification Date relating to such Standard Bylaw Amendment Approval and the effectiveness of such Standard Bylaw Amendment shall not be subject to further challenge by the EC pursuant to the EC's rejection right as described in Article 2 of Annex D;
>
> (ii) (A) A Rejection Action Supported Petition is not timely delivered by the Rejection Action Petitioning Decisional Participant to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D or (B) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.2(d) of Annex D, in which case the Standard Bylaw Amendment that is the subject of the Standard Bylaw Amendment Approval shall be in full force and effect as of the date immediately following the expiration of the Rejection Action Petition Support Period relating to such Standard Bylaw Amendment and the effectiveness of such Standard Bylaw Amendment shall not be subject to further challenge by the EC pursuant to the EC's rejection right as described in Article 2 of Annex D; or

> (iii) (A) An EC Rejection Notice is not timely delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4 of Annex D or (B) a Rejection Process Termination Notice is delivered by the EC Administration to the Secretary pursuant to and in compliance with Section 2.4(c) of Annex D, in which case the Standard Bylaw Amendment that is the subject of the Standard Bylaw Amendment Approval shall be in full force and effect as of the date immediately following the expiration of the Rejection Action Decision Period relating to such Standard Bylaw Amendment and the effectiveness of such Standard Bylaw Amendment shall not be subject to further challenge by the EC pursuant to the EC's rejection right as described in Article 2 of Annex D.

(f) If an EC Rejection Notice is timely delivered by the EC Administration to the Secretary pursuant to and compliance with Section 2.4 of Annex D, the Standard Bylaw Amendment contained in the Board Notice shall be deemed to have been rejected by the EC. A Standard Bylaw Amendment that has been rejected by the EC shall be null and void and shall not become part of these Bylaws, notwithstanding its approval by the Board.

(g) The Secretary shall promptly inform the Board of the receipt and substance of any Rejection Action Petition, Rejection Action Supported Petition or EC Rejection Notice delivered by the Rejection Action Petitioning Decisional Participant or the EC Administration, as applicable, to the Secretary hereunder.

(h) Following receipt of an EC Rejection Notice pertaining to a Standard Bylaw Amendment, ICANN staff and the Board shall consider the explanation provided by the EC Administration as to why the EC has chosen to reject the Standard Bylaw Amendment in determining whether or not to develop a new Standard Bylaw Amendment and the substance of such new Standard Bylaw Amendment, which shall be subject to the procedures of this Section 25.1.

Section 25.2. AMENDMENTS TO THE FUNDAMENTAL BYLAWS AND ARTICLES OF INCORPORATION

(a) Article 1; Sections 4.2, 4.3 and 4.7; Article 6; Sections 7.1 through 7.5, inclusive, and Sections 7.8, 7.11, 7.12, 7.17, 7.24 and 7.25; those portions of Sections 8.1, 9.2(b), 10.3(i), 11.3(f) and 12.2(d)(x)(A) relating to the provision to the EC of nominations of Directors by the nominating body, Articles 16, 17, 18 and 19, Sections 22.4, 22.5, 22.7 and 22.8, Article 26, Section 27.1; Annexes D, E and F; and this Article 25 are each a "**Fundamental Bylaw**" and, collectively, are the "**Fundamental Bylaws**".

(b) Notwithstanding any other provision of these Bylaws, a Fundamental Bylaw or the Articles of Incorporation may be altered, amended, or repealed (a "**Fundamental Bylaw Amendment**" or an "**Articles Amendment**"), only upon approval by a three-fourths vote of all Directors and the approval of the EC as set forth in this Section 25.2.

(c) Prior to approval of a Fundamental Bylaw Amendment, or an Articles Amendment by the Board, a draft of the Fundamental Bylaw Amendment or Articles Amendment, as applicable, shall be posted on the Website and shall be subject to public comment in accordance with ICANN's public comment processes.

(d) After reviewing the comments submitted during the public comment period, the Board may direct ICANN staff to submit a revised draft of the Fundamental Bylaw Amendment or Articles Amendment, as applicable, and may direct ICANN staff to conduct one or more additional public comment periods in accordance with ICANN's public comment processes.

(e) Within seven days after the Board's approval of a Fundamental Bylaw Amendment or Articles Amendment, as applicable, the Secretary shall (i) provide a Board Notice to the EC Administration and the Decisional Participants, which Board Notice shall contain the form of the approved amendment and (ii) post the Board Notice, along with a copy of the notification(s) sent to the EC Administration and the Decisional Participants, on the Website. The steps contemplated in Article 1 of Annex D shall then be followed.

(f) If the EC Administration timely delivers an EC Approval Notice (as defined in Section 1.4(b) of Annex D), the Fundamental Bylaw Amendment or Articles Amendment, as applicable, set forth in the Board Notice shall be deemed approved by the EC, and, as applicable, (i) such Fundamental Bylaw Amendment shall be in full force and effect as part of these Bylaws as of the date immediately following the Secretary's receipt of the EC Approval Notice; or (ii) the Secretary shall cause such Articles Amendment promptly to be certified by the appropriate officers of ICANN and filed with the California Secretary of State. In the event of such approval, neither the Fundamental Bylaw Amendment nor the Articles Amendment shall be subject to any further review or approval of the EC. The Secretary shall promptly inform the Board of the receipt of an EC Approval Notice.

(g) If an EC Approval Notice is not timely delivered by the EC Administration to the Secretary, the Fundamental Bylaw Amendment or Articles Amendment, as applicable, set forth in the Board Notice shall be deemed not approved by the EC, shall be null and void, and, notwithstanding its approval by the Board, the Fundamental Bylaw Amendment shall not be part of these Bylaws and the Articles Amendment shall not be filed with the Secretary of State.

(h) If a Fundamental Bylaw Amendment or Articles Amendment, as applicable, is not approved by the EC, ICANN staff and the Board shall consider the concerns raised by the EC in determining whether or not to develop a new Fundamental Bylaws Amendment or Articles Amendment, as applicable, and the substance thereof, which shall be subject to the procedures of this Section 25.2.

Section 25.3. AMENDMENTS RESULTING FROM A POLICY DEVELOPMENT PROCESS

The Board shall not combine an amendment of these Bylaws that was the result of a policy development process of a Supporting Organization (a "**PDP Amendment**") with any other amendment. The Board shall indicate in the applicable Board Notice whether such amendment is a PDP Amendment.

Section 25.4. OTHER AMENDMENTS

For the avoidance of doubt, these Bylaws can only be amended as set forth in this Article 25. Neither the EC, the Decisional Participants, the Supporting Organizations, the Advisory Committees nor any other entity or person shall have the power to directly propose amendments to these Bylaws.

ARTICLE 26 SALE OR OTHER DISPOSITION OF ALL OR SUBSTANTIALLY ALL OF ICANN'S ASSETS

(a) ICANN may consummate a transaction or series of transactions that would result in the sale or disposition of all or substantially all of ICANN's assets (an "**Asset Sale**") only upon approval by a three-fourths vote of all Directors and the approval of the EC as set forth in this Article 26.

(b) Prior to approval of an Asset Sale by the Board, a draft of the definitive Asset Sale agreement (an "**Asset Sale Agreement**"), shall be posted on the Website and shall be subject to public comment in accordance with ICANN's public comment processes.

(c) After reviewing the comments submitted during the public comment period, the Board may direct ICANN staff to submit a revised draft of the Asset Sale Agreement, as applicable, and may direct ICANN staff to conduct one or more additional public comment periods in accordance with ICANN's public comment processes.

(d) Within seven days after the Board's approval of an Asset Sale the Secretary shall (i) provide a Board Notice to the EC Administration and the Decisional Participants, which Board Notice shall contain the form of the Asset Sale

Agreement and (ii) post the Board Notice on the Website. The steps contemplated in Article 1 of Annex D shall then be followed.

(e) If the EC Administration timely delivers an EC Approval Notice for the Asset Sale pursuant to and in compliance with the procedures and requirements of Section 1.4(b) of Annex D, the Asset Sale set forth in the Board Notice shall be deemed approved by the EC, and the Asset Sale may be consummated by ICANN, but only under the terms set forth in the Asset Sale Agreement. In the event of such approval, the Asset Sale shall not be subject to any further review or approval of the EC. The Secretary shall promptly inform the Board of the receipt of an EC Approval Notice.

(f) If an EC Approval Notice is not timely delivered by the EC Administration to the Secretary, the Asset Sale set forth in the Board Notice shall be deemed not approved by the EC, shall be null and void, and, notwithstanding its approval by the Board, ICANN shall not consummate the Asset Sale.

(g) If an Asset Sale is not approved by the EC, ICANN staff and the Board shall consider the concerns raised by the EC in determining whether or not to consider a new Asset Sale, and the substance thereof, which shall be subject to the procedures of this Article 26.

ARTICLE 27 TRANSITION ARTICLE

Section 27.1. WORK STREAM 2

(a) The Cross-Community Working Group on Enhancing ICANN Accountability ("**CCWG-Accountability**") was established pursuant to a charter dated 3 November 2014 ("**CCWG-Accountability Charter**"). The CCWG-Accountability Charter was subsequently adopted by the GNSO, ALAC, ccNSO, GAC, ASO and SSAC ("**CCWG Chartering Organizations**"). The CCWG-Accountability Charter as in effect on 3 November 2014 shall remain in effect throughout Work Stream 2 (as defined therein).

(b) The CCWG-Accountability recommended in its Supplemental Final Proposal on Work Stream 1 Recommendations to the Board, dated 23 February 2016 ("**CCWG-Accountability Final Report**") that the below matters be reviewed and developed following the adoption date of these Bylaws ("**Work Stream 2 Matters**"), in each case, to the extent set forth in the CCWG-Accountability Final Report:

> (i) Improvements to ICANN's standards for diversity at all levels;

(ii) ICANN staff accountability;

(iii) Supporting Organization and Advisory Committee accountability, including but not limited to improved processes for accountability, transparency, and participation that are helpful to prevent capture;

(iv) Improvements to ICANN's transparency, focusing on enhancements to ICANN's existing DIDP, transparency of ICANN's interactions with governments, improvements to ICANN's whistleblower policy and transparency of Board deliberations;

(v) Developing and clarifying the FOI-HR (as defined in Section 27.2);

(vi) Addressing jurisdiction-related questions, including how choice of jurisdiction and applicable laws for dispute settlement impact ICANN's accountability;

(vii) Considering enhancements to the Ombudsman's role and function;

(viii) Guidelines for standards of conduct presumed to be in good faith associated with exercising removal of individual Directors; and

(ix) Reviewing the CEP (as set forth in Section 4.3).

(c) As provided in the CCWG-Accountability Charter and the Board's 2014.10.16.16 resolution, the Board shall consider consensus-based recommendations from the CCWG-Accountability on Work Stream 2 Matters ("**Work Stream 2 Recommendations**") with the same process and criteria it committed to using to consider the CCWG-Accountability recommendations in the CCWG-Accountability Final Report (**"Work Stream 1 Recommendations"**). For the avoidance of doubt, that process and criteria includes:

(i) All Work Stream 2 Recommendations must further the following principles:

(A)Support and enhance the multistakeholder model;

(B)Maintain the security, stability and resiliency of the DNS;

(C)Meet the needs and expectations of the global customers and partners of the IANA services;

(D)Maintain the openness of the Internet; and

(E)Not result in ICANN becoming a government-led or an inter-governmental organization.

(ii) If the Board determines, by a vote of a two-thirds majority of the Board, that it is not in the global public interest to implement a Work Stream 2 Recommendation, it must initiate a dialogue with the CCWG-Accountability.

(iii) The Board shall provide detailed rationale to accompany the initiation of dialogue. The Board and the CCWG-Accountability shall mutually agree upon the method (e.g., by teleconference, email or otherwise) by which the dialogue will occur. Discussions shall be held in good faith and in a timely and efficient manner in an effort to find a mutually acceptable solution.

(iv) The CCWG-Accountability shall have an opportunity to address the Board's concerns and report back to the Board on further deliberations regarding the Board's concerns. The CCWG-Accountability shall discuss the Board's concerns within 30 days of the Board's initiation of the dialogue.

If a Work Stream 2 Recommendation is modified by the CCWG-Accountability, the CCWG-Accountability shall submit the modified Work Stream 2 Recommendation to the Board for further consideration along with detailed rationale on how the modification addresses the concerns raised by the Board.

(v) If, after the CCWG-Accountability modifies a Work Stream 2 Recommendation, the Board still believes it is not in the global public interest to implement the Work Stream 2 Recommendation, the Board may, by a vote of a two-thirds majority of the Board, send the matter back to the CCWG-Accountability for further consideration. The Board shall provide detailed rationale to accompany its action. If the Board determines not to accept a modified version of a Work Stream 2 Recommendation, unless required by its fiduciary obligations, the Board shall not establish an alternative solution on the issue addressed by the Work Stream 2 Recommendation until such time as the CCWG-Accountability and the Board reach agreement.

(d) ICANN shall provide adequate support for work on Work Stream 2 Matters, within budgeting processes and limitations reasonably acceptable to the CCWG-Accountability.

(e) The Work Stream 2 Matters specifically referenced in Section 27.1(b) shall be

the only matters subject to this Section 27.1 and any other accountability enhancements should be developed through ICANN's other procedures.

(f) The outcomes of each Work Stream 2 Matter are not limited and could include a variety of recommendations or no recommendation; provided, however, that any resulting recommendations must directly relate to the matters discussed in Section 27.1(b).

Section 27.2. HUMAN RIGHTS

(a) The Core Value set forth in Section 1.2(b)(viii) shall have no force or effect unless and until a framework of interpretation for human rights ("**FOI-HR**") is (i) approved for submission to the Board by the CCWG-Accountability as a consensus recommendation in Work Stream 2, with the CCWG Chartering Organizations having the role described in the CCWG-Accountability Charter, and (ii) approved by the Board, in each case, using the same process and criteria as for Work Stream 1 Recommendations.>

(b) No person or entity shall be entitled to invoke the reconsideration process provided in Section 4.2, or the independent review process provided in Section 4.3, based solely on the inclusion of the Core Value set forth in Section 1.2(b)(viii) (i) until after the FOI-HR contemplated by Section 27.2(a) is in place or (ii) for actions of ICANN or the Board that occurred prior to the effectiveness of the FOI-HR.

Section 27.3. EXISTING GROUPS AND TASK FORCES

Notwithstanding the adoption or effectiveness of these Bylaws, task forces and other groups in existence prior to the date of these Bylaws shall continue unchanged in membership, scope, and operation unless and until changes are made by ICANN in compliance with the Bylaws.

Section 27.4. CONTRACTS WITH ICANN

Notwithstanding the adoption or effectiveness of these Bylaws, all agreements, including employment and consulting agreements, entered into by ICANN shall continue in effect according to their terms.

Annex A: GNSO Policy Development Process

The following process shall govern the GNSO policy development process ("**PDP**") until such time as modifications are recommended to and approved by the Board. The role of the GNSO is outlined in Article 11 of these Bylaws. If the GNSO is conducting activities that are not intended to result in a Consensus Policy, the

Council may act through other processes.

Section 1. **Required Elements of a Policy Development Process**

The following elements are required at a minimum to form Consensus Policies as defined within ICANN contracts, and any other policies for which the GNSO Council requests application of this Annex A:

a. Final Issue Report requested by the Board, the GNSO Council ("Council") or Advisory Committee, which should include at a minimum a) the proposed issue raised for consideration, b) the identity of the party submitting the issue, and c) how that party Is affected by the issue;

b. Formal initiation of the Policy Development Process by the Council;

c. Formation of a Working Group or other designated work method;

d. Initial Report produced by a Working Group or other designated work method;

e. Final Report produced by a Working Group, or other designated work method, and forwarded to the Council for deliberation;

f. Council approval of PDP Recommendations contained in the Final Report, by the required thresholds;

g. PDP Recommendations and Final Report shall be forwarded to the Board through a Recommendations Report approved by the Council; and

h. Board approval of PDP Recommendations.

Section 2. **Policy Development Process Manual**

The GNSO shall maintain a Policy Development Process Manual ("**PDP Manual**") within the operating procedures of the GNSO maintained by the GNSO Council. The PDP Manual shall contain specific additional guidance on completion of all elements of a PDP, including those elements that are not otherwise defined in these Bylaws. The PDP Manual and any amendments thereto are subject to a twenty-one (21) day public comment period at minimum, as well as Board oversight and review, as specified at Section 11.3(d).

Section 3. **Requesting an Issue Report**

Board Request. The Board may request an Issue Report by instructing the GNSO Council ("Council") to begin the process outlined the PDP Manual. In the event the Board makes a request for an Issue Report, the Board should provide a

mechanism by which the GNSO Council can consult with the Board to provide information on the scope, timing, and priority of the request for an Issue Report.

Council Request. The GNSO Council may request an Issue Report by a vote of at least one-fourth (1/4) of the members of the Council of each House or a majority of one House.

Advisory Committee Request. An Advisory Committee may raise an issue for policy development by action of such committee to request an Issue Report, and transmission of that request to the Staff Manager and GNSO Council.

Section 4. **Creation of an Issue Report**

Within forty-five (45) calendar days after receipt of either (i) an instruction from the Board; (ii) a properly supported motion from the GNSO Council; or (iii) a properly supported motion from an Advisory Committee, the Staff Manager will create a report (a "**Preliminary Issue Report**"). In the event the Staff Manager determines that more time is necessary to create the Preliminary Issue Report, the Staff Manager may request an extension of time for completion of the Preliminary Issue Report.

The following elements should be considered in the Issue Report:

a. The proposed issue raised for consideration;

b. The identity of the party submitting the request for the Issue Report;

c. How that party is affected by the issue, if known;

d. Support for the issue to initiate the PDP, if known;

e. The opinion of the ICANN General Counsel regarding whether the issue proposed for consideration within the Policy Development Process is properly within the scope of the Mission, policy process and more specifically the role of the GNSO as set forth in the Bylaws.

f. The opinion of ICANN Staff as to whether the Council should initiate the PDP on the issue.

Upon completion of the Preliminary Issue Report, the Preliminary Issue Report shall be posted on the Website for a public comment period that complies with the designated practice for public comment periods within ICANN.

The Staff Manager is responsible for drafting a summary and analysis of the public comments received on the Preliminary Issue Report and producing a Final Issue Report based upon the comments received. The Staff Manager should forward the

Final Issue Report, along with any summary and analysis of the public comments received, to the Chair of the GNSO Council for consideration for initiation of a PDP.

Section 5. **Initiation of the PDP**

The Council may initiate the PDP as follows:

Board Request: If the Board requested an Issue Report, the Council, within the timeframe set forth in the PDP Manual, shall initiate a PDP. No vote is required for such action.

GNSO Council or Advisory Committee Requests: The Council may only initiate the PDP by a vote of the Council. Initiation of a PDP requires a vote as set forth in Section 11.3(i)(ii) and Section 11.3(i)(iii) in favor of initiating the PDP.

Section 6. **Reports**

An Initial Report should be delivered to the GNSO Council and posted for a public comment period that complies with the designated practice for public comment periods within ICANN, which time may be extended in accordance with the PDP Manual. Following the review of the comments received and, if required, additional deliberations, a Final Report shall be produced for transmission to the Council.

Section 7. **Council Deliberation**

Upon receipt of a Final Report, whether as the result of a working group or otherwise, the Council chair will (i) distribute the Final Report to all Council members; and (ii) call for Council deliberation on the matter in accordance with the PDP Manual.

The Council approval process is set forth in Section 11.3(i)(iv) through Section 11.3(vii), as supplemented by the PDP Manual.

Section 8. **Preparation of the Board Report**

If the PDP recommendations contained in the Final Report are approved by the GNSO Council, a Recommendations Report shall be approved by the GNSO Council for delivery to the Board.

Section 9. **Board Approval Processes**

The Board will meet to discuss the GNSO Council recommendation as soon as feasible, but preferably not later than the second meeting after receipt of the

Board Report from the Staff Manager. Board deliberation on the PDP Recommendations contained within the Recommendations Report shall proceed as follows:

a. Any PDP Recommendations approved by a GNSO Supermajority Vote shall be adopted by the Board unless, by a vote of more than two-thirds (2/3) of the Board, the Board determines that such policy is not in the best interests of the ICANN community or ICANN. If the GNSO Council recommendation was approved by less than a GNSO Supermajority Vote, a majority vote of the Board will be sufficient to determine that such policy is not in the best interests of the ICANN community or ICANN.

b. In the event that the Board determines, in accordance with paragraph a above, that the policy recommended by a GNSO Supermajority Vote or less than a GNSO Supermajority vote is not in the best interests of the ICANN community or ICANN (the Corporation), the Board shall (i) articulate the reasons for its determination in a report to the Council (the "**Board Statement**"); and (ii) submit the Board Statement to the Council.

c. The Council shall review the Board Statement for discussion with the Board as soon as feasible after the Council's receipt of the Board Statement. The Board shall determine the method (e.g., by teleconference, e-mail, or otherwise) by which the Council and Board will discuss the Board Statement.

d. At the conclusion of the Council and Board discussions, the Council shall meet to affirm or modify its recommendation, and communicate that conclusion (the "**Supplemental Recommendation**") to the Board, including an explanation for the then-current recommendation. In the event that the Council is able to reach a GNSO Supermajority Vote on the Supplemental Recommendation, the Board shall adopt the recommendation unless more than two-thirds (2/3) of the Board determines that such policy is not in the interests of the ICANN community or ICANN. For any Supplemental Recommendation approved by less than a GNSO Supermajority Vote, a majority vote of the Board shall be sufficient to determine that the policy in the Supplemental Recommendation is not in the best interest of the ICANN community or ICANN.

Section 10. **Implementation of Approved Policies**

Upon a final decision of the Board adopting the policy, the Board shall, as appropriate, give authorization or direction to ICANN staff to work with the GNSO Council to create an implementation plan based upon the implementation recommendations identified in the Final Report, and to implement the policy. The GNSO Council may, but is not required to, direct the creation of an implementation

review team to assist in implementation of the policy.

Section 11. **Maintenance of Records**

Throughout the PDP, from policy suggestion to a final decision by the Board, ICANN will maintain on the Website, a status web page detailing the progress of each PDP issue. Such status page will outline the completed and upcoming steps in the PDP process, and contain links to key resources (e.g. Reports, Comments Fora, WG Discussions, etc.).

Section 12. **Additional Definitions**

"**Comment Site**", "**Comment Forum**", "**Comments For a**" and "**Website**" refer to one or more websites designated by ICANN on which notifications and comments regarding the PDP will be posted.

"**Supermajority Vote**" means a vote of more than sixty-six (66) percent of the members present at a meeting of the applicable body, with the exception of the GNSO Council.

"**Staff Manager**" means an ICANN staff person(s) who manages the PDP.

"**GNSO Supermajority Vote**" shall have the meaning set forth in the Bylaws.

Section 13. **Applicability**

The procedures of this Annex A shall be applicable to all requests for Issue Reports and PDPs initiated after 8 December 2011. For all ongoing PDPs initiated prior to 8 December 2011, the Council shall determine the feasibility of transitioning to the procedures set forth in this Annex A for all remaining steps within the PDP. If the Council determines that any ongoing PDP cannot be feasibly transitioned to these updated procedures, the PDP shall be concluded according to the procedures set forth in Annex A in force on 7 December 2011.

Annex A-1: GNSO Expedited Policy Development Process

The following process shall govern the specific instances where the GNSO Council invokes the GNSO Expedited Policy Development Process ("**EPDP**"). The GNSO Council may invoke the EPDP in the following limited circumstances: (1) to address a narrowly defined policy issue that was identified and scoped after either the adoption of a GNSO policy recommendation by the Board or the implementation of such an adopted recommendation; or (2) to create new or additional recommendations for a specific policy issue that had been substantially

scoped previously such that extensive, pertinent background information already exists, e.g. (a) in an Issue Report for a possible PDP that was not initiated; (b) as part of a previous PDP that was not completed; or (c) through other projects such as a GGP. The following process shall be in place until such time as modifications are recommended to and approved by the Board. Where a conflict arises in relation to an EPDP between the PDP Manual (see Annex 2 of the GNSO Operating Procedures) and the procedures described in this Annex A-1, the provisions of this Annex A-1 shall prevail.

The role of the GNSO is outlined in Article 11 of these Bylaws. Provided the Council believes and documents via Council vote that the above-listed criteria are met, an EPDP may be initiated to recommend an amendment to an existing Consensus Policy; however, in all cases where the GNSO is conducting policy-making activities that do not meet the above criteria as documented in a Council vote, the Council should act through a Policy Development Process (see Annex A).

Section 1. **Required Elements of a GNSO Expedited Policy Development Process**

The following elements are required at a minimum to develop expedited GNSO policy recommendations, including recommendations that could result in amendments to an existing Consensus Policy, as part of a GNSO Expedited Policy Development Process:

a. Formal initiation of the GNSO Expedited Policy Development Process by the GNSO Council, including an EPDP scoping document;

b. Formation of an EPDP Team or other designated work method;

c. Initial Report produced by an EPDP Team or other designated work method;

d. Final EPDP Policy Recommendation(s) Report produced by an EPDP Team, or other designated work method, and forwarded to the Council for deliberation;

e. GNSO Council approval of EPDP Policy Recommendations contained in the Final EPDP Policy Recommendation(s) Report, by the required thresholds;

f. EPDP Recommendations and Final EPDP Recommendation(s) Report forwarded to the Board through a Recommendations Report approved by the Council; and

g. Board approval of EPDP Recommendation(s).

Section 2. **Expedited Policy Development Process Manual**

The GNSO shall include a specific section(s) on the EPDP process as part of its maintenance of the GNSO Policy Development Process Manual (PDP Manual), described in Annex 5 of the GNSO Operating Procedures. The EPDP Manual shall contain specific additional guidance on completion of all elements of an EPDP, including those elements that are not otherwise defined in these Bylaws. The E PDP Manual and any amendments thereto are subject to a twenty-one (21) day public comment period at minimum, as well as Board oversight and review, as specified at Section 11.3(d) .

Section 3. **Initiation of the EPDP**

The Council may initiate an EPDP as follows:

The Council may only initiate the EPDP by a vote of the Council. Initiation of an EPDP requires an affirmative Supermajority vote of the Council (as defined in Section 11.3(i)(xii) of these Bylaws) in favor of initiating the EPDP.

The request to initiate an EPDP must be accompanied by an EPDP scoping document, which is expected to include at a minimum the following information:

1. Name of Council Member / SG / C;
2. Origin of issue (e.g. previously completed PDP);
3. Scope of the effort (detailed description of the issue or question that the EPDP is expected to address);
4. Description of how this issue meets the criteria for an EPDP, i.e. how the EPDP will address either: (1) a narrowly defined policy issue that was identified and scoped after either the adoption of a GNSO policy recommendation by the Board or the implementation of such an adopted recommendation, or (2) new or additional policy recommendations on a specific GNSO policy issue that had been scoped previously as part of a PDP that was not completed or other similar effort, including relevant supporting information in either case;
5. If not provided as part of item 4, the opinion of the ICANN General Counsel as to whether the issue proposed for consideration is properly within the scope of the Mission, policy process and more specifically the role of the GNSO;
6. Proposed EPDP mechanism (e.g. WG, DT, individual volunteers);

7. Method of operation, if different from GNSO Working Group Guidelines;

8. Decision-making methodology for EPDP mechanism, if different from GNSO Working Group Guidelines;

9. Target completion date.

Section 4. **Council Deliberation**

Upon receipt of an EPDP Final Recommendation(s) Report, whether as the result of an EPDP Team or otherwise, the Council chair will (i) distribute the Final EPDP Recommendation(s) Report to all Council members; and (ii) call for Council deliberation on the matter in accordance with the PDP Manual.

Approval of EPDP Recommendation(s) requires an affirmative vote of the Council meeting the thresholds set forth in Section 11.3(i)(xiv) and (xv), as supplemented by the PDP Manual.

Section 5. **Preparation of the Board Report**

If the EPDP Recommendation(s) contained in the Final EPDP Recommendation(s) Report are approved by the GNSO Council, a Recommendation(s) Report shall be approved by the GNSO Council for delivery to the Board.

Section 6. **Board Approval Processes**

The Board will meet to discuss the EPDP recommendation(s) as soon as feasible, but preferably not later than the second meeting after receipt of the Recommendations Report from the Staff Manager. Board deliberation on the EPDP Recommendations contained within the Recommendations Report shall proceed as follows:

a. Any EPDP Recommendations approved by a GNSO Supermajority Vote shall be adopted by the Board unless, by a vote of more than two-thirds (2/3) of the Board, the Board determines that such policy is not in the best interests of the ICANN community or ICANN. If the GNSO Council recommendation was approved by less than a GNSO Supermajority Vote, a majority vote of the Board will be sufficient to determine that such policy is not in the best interests of the ICANN community or ICANN.

b. In the event that the Board determines, in accordance with paragraph a above, that the proposed EPDP Recommendations are not in the best interests of the ICANN community or ICANN (the Corporation), the Board shall (i) articulate the reasons for its determination in a report to the Council

(the "Board Statement"); and (ii) submit the Board Statement to the Council.

c. The Council shall review the Board Statement for discussion with the Board as soon as feasible after the Council's receipt of the Board Statement. The Board shall determine the method (e.g., by teleconference, e-mail, or otherwise) by which the Council and Board will discuss the Board Statement.

At the conclusion of the Council and Board discussions, the Council shall meet to affirm or modify its recommendation, and co mmunicate that conclusion (the "Supplemental Recommendation") to the Board, including an explanation for the then-current recommendation. In the event that the Council is able to reach a GNSO Supermajority Vote on the Supplemental Recommendation, the Board shall adopt the recommendation unless more than two-thirds (2/3) of the Board determines that such guidance is not in the interests of the ICANN community or ICANN. For any Supplemental Recommendation approved by less than a GNSO Supermajority Vote, a majority vote of the Board shall be sufficient to determine that the guidance in the Supplemental Recommendation is not in the best interest of the ICANN community or ICANN.

Section 7. **Implementation of Approved Policies**

Upon a final decision of the Board adopting the EPDP recommendations, the Board shall, as appropriate, give authorization or direction to ICANN staff to implement the EPDP Recommendations. If deemed necessary, the Board shall direct ICANN staff to work with the GNSO Council to create a guidance implementation plan, based upon the guidance recommendations identified in the Final EPDP Recommendation(s) Report.

Section 8. **Maintenance of Records**

Throughout the EPDP, from initiation to a final decision by the Board, ICANN will maintain on the Website, a status web page detailing the progress of each EPDP issue. Such status page will outline the completed and upcoming steps in the EPDP process, and contain links to key resources (e.g. Reports, Comments Fora, EPDP Discussions, etc.).

Section 9. **Applicability**

The procedures of this Annex A-1 shall be applicable from 28 September 2015 onwards.

Annex A-2: GNSO Guidance Process

The following process shall govern the GNSO guidance process ("**GGP**") until such time as modifications are recommended to and approved by the Board . The role of the GNSO is outlined in Article 11 of these Bylaws. If the GNSO is conducting activities that are intended to result in a Consensus Policy, the Council should act through a Policy Development Process (see Annex A).

Section 1. **Required Elements of a GNSO Guidance Process**

The following elements are required at a minimum to develop GNSO guidance:

1. Formal initiation of the GNSO Guidance Process by the Council, including a GGP scoping document;
2. Identification of the types of expertise needed on the GGP Team;
3. Recruiting and formation of a GGP Team or other designated work method;
4. Proposed GNSO Guidance Recommendation(s) Report produced by a GGP Team or other designated work method;
5. Final GNSO Guidance Recommendation(s) Report produced by a GGP Team, or other designated work method, and forwarded to the Council for deliberation;
6. Council approval of GGP Recommendations contained in the Final Recommendation(s) Report, by the required thresholds;
7. GGP Recommendations and Final Recommendation(s) Report shall be forwarded to the Board through a Recommendations Report approved by the Council; and
8. Board approval of GGP Recommendation(s).

Section 2. **GNSO Guidance Process Manual**

The GNSO shall maintain a GNSO Guidance Process (GGP Manual) within the operating procedures of the GNSO maintained by the GNSO Council. The GGP Manual shall contain specific additional guidance on completion of all elements of a GGP, including those elements that are not otherwise defined in these Bylaws. The GGP Manual and any amendments thereto are subject to a twenty-one (21) day public comment period at minimum, as well as Board oversight and review, as specified at Section 11.3(d).

Section 3. **Initiation of the GGP**

The Council may initiate a GGP as follows:

The Council may only initiate the GGP by a vote of the Council or at the formal request of the ICANN Board. Initiation of a GGP requires a vote as set forth in Section 11.3(i)(xvi) in favor of initiating the GGP. In the case of a GGP requested by the Board, a GGP will automatically be initiated unless the GNSO Council votes against the initiation of a GGP as set forth in Section 11.3(i)(xvii).

The request to initiate a GGP must be accompanied by a GGP scoping document, which is expected to include at a minimum the following information:

1. Name of Council Member / SG / C
2. Origin of issue (e.g., board request)
3. Scope of the effort (detailed description of the issue or question that the GGP is expected to address)
4. Proposed GGP mechanism (e.g. WG, DT, individual volunteers)
5. Method of operation, if different from GNSO Working Group Guidelines
6. Decision-making methodology for GGP mechanism, if different from GNSO Working Group Guidelines
7. Desired completion date and rationale

In the event the Board makes a request for a GGP, the Board should provide a mechanism by which the GNSO Council can consult with the Board to provide information on the scope, timing, and priority of the request for a GGP.

Section 4. **Council Deliberation**

Upon receipt of a Final Recommendation(s) Report, whether as the result of a GGP Team or otherwise, the Council chair will (i) distribute the Final Recommendation(s) Report to all Council members; and (ii) call for Council deliberation on the matter in accordance with the GGP Manual.

The Council approval process is set forth in Section 11.3(xviii) as supplemented by the GGP Manual.

Section 5. **Preparation of the Board Report**

If the GGP recommendations contained in the Final Recommendation(s) Report are approved by the GNSO Council, a Recommendations Report shall be approved by the GNSO Council for delivery to the Board.

Section 6. **Board Approval Processes**

The Board will meet to discuss the GNSO Guidance recommendation(s) as soon as feasible, but preferably not later than the second meeting after receipt of the Board Report from the Staff Manager. Board deliberation on the GGP Recommendations contained within the Recommendations Report shall proceed as follows:

a. Any GGP Recommendations approved by a GNSO Supermajority Vote shall be adopted by the Board unless, by a vote of more than two-thirds (2/3) of the Board, the Board determines that such guidance is not in the best interests of the ICANN community or ICANN.

b. In the event that the Board determines, in accordance with paragraph a above, that the proposed GNSO Guidance recommendation(s) adopted by a GNSO Supermajority Vote is not in the best interests of the ICANN community or ICANN (the Corporation), the Board shall (i) articulate the reasons for its determination in a report to the Council (the "Board Statement"); and (ii) submit the Board Statement to the Council.

c. The Council shall review the Board Statement for discussion with the Board as soon as feasible after the Council's receipt of the Board Statement. The Board shall determine the method (e.g., by teleconference, e-mail, or otherwise) by which the Council and Board will discuss the Board Statement.

d. At the conclusion of the Council and Board discussions, the Council shall meet to affirm or modify its recommendation, and communicate that conclusion (the "Supplemental Recommendation") to the Board, including an explanation for the then-current recommendation. In the event that the Council is able to reach a GNSO Supermajority Vote on the Supplemental Recommendation, the Board shall adopt the recommendation unless more than two-thirds (2/3) of the Board determines that such guidance is not in the interests of the ICANN community or ICANN.

Section 7. **Implementation of Approved GNSO Guidance**

Upon a final decision of the Board adopting the guidance, the Board shall, as appropriate, give authorization or direction to ICANN staff to implement the GNSO Guidance. If deemed necessary, the Board may direct ICANN Staff to work with the GNSO Council to create a guidance implementation plan, if deemed necessary, based upon the guidance recommendations identified in the Final Recommendation(s) Report.

Section 8. **Maintenance of Records**

Throughout the GGP, from initiation to a final decision by the Board, ICANN will maintain on the Website, a status web page detailing the progress of each GGP issue. Such status page will outline the completed and upcoming steps in the GGP process, and contain links to key resources (e.g. Reports, Comments Fora, GGP Discussions, etc.).

Section 9. **Additional Definitions**

"**Comment Site**", "**Comment Forum**", "**Comments Fora**" and "**Website**" refer to one or more websites designated by ICANN on which notifications and comments regarding the GGP will be posted.

"**GGP Staff Manager**" means an ICANN staff person(s) who manages the GGP.

Annex B: ccNSO Policy-Development Process (ccPDP)

The following process shall govern the ccNSO policy-development process ("**PDP**").

1. Request for an Issue Report

An Issue Report may be requested by any of the following:

a. *Council.* The ccNSO Council (in this Annex B, the "**Council**") may call for the creation of an Issue Report by an affirmative vote of at least seven of the members of the Council present at any meeting or voting by e-mail.

b. *Board.* The Board may call for the creation of an Issue Report by requesting the Council to begin the policy-development process.

c. *Regional Organization.* One or more of the Regional Organizations representing ccTLDs in the ICANN recognized Regions may call for creation of an Issue Report by requesting the Council to begin the policy-development process.

d. *ICANN Supporting Organization or Advisory Committee.* An ICANN Supporting Organization or an ICANN Advisory Committee may call for creation of an Issue Report by requesting the Council to begin the policy-development process.

e. *Members of the ccNSO.* The members of the ccNSO may call for the creation of an Issue Report by an affirmative vote of at least ten members of the ccNSO present at any meeting or voting by e-mail.

Any request for an Issue Report must be in writing and must set out the issue upon which an Issue Report is requested in sufficient detail to enable the Issue Report to be prepared. It shall be open to the Council to request further information or undertake further research or investigation for the purpose of determining whether or not the requested Issue Report should be created.

2. Creation of the Issue Report and Initiation Threshold

Within seven days after an affirmative vote as outlined in Item 1(a) above or the receipt of a request as outlined in Items 1 (b), (c), or (d) above the Council shall appoint an Issue Manager. The Issue Manager may be a staff member of ICANN (in which case the costs of the Issue Manager shall be borne by ICANN) or such other person or persons selected by the Council (in which case the ccNSO shall be responsible for the costs of the Issue Manager).

Within fifteen (15) calendar days after appointment (or such other time as the Council shall, in consultation with the Issue Manager, deem to be appropriate), the Issue Manager shall create an Issue Report. Each Issue Report shall contain at least the following:

a. The proposed issue raised for consideration;

b. The identity of the party submitting the issue;

c. How that party is affected by the issue;

d. Support for the issue to initiate the PDP;

e. A recommendation from the Issue Manager as to whether the Council should move to initiate the PDP for this issue (the "**Manager Recommendation**"). Each Manager Recommendation shall include, and be supported by, an opinion of the ICANN General Counsel regarding whether the issue is properly within the scope of the ICANN policy process and within the scope of the ccNSO. In coming to his or her opinion, the General Counsel shall examine whether:
   1) The issue is within the scope of the Mission;

   2) Analysis of the relevant factors according to Section 10.6(b) and Annex C affirmatively demonstrates that the issue is within the scope of the ccNSO;

   In the event that the General Counsel reaches an opinion in the affirmative with respect to points 1 and 2 above then the General Counsel shall also consider whether the issue:

3) Implicates or affects an existing ICANN policy;

4) Is likely to have lasting value or applicability, albeit with the need for occasional updates, and to establish a guide or framework for future decision-making.

In all events, consideration of revisions to the ccPDP (this Annex B) or to the scope of the ccNSO (Annex C) shall be within the scope of ICANN and the ccNSO.

In the event that General Counsel is of the opinion the issue is not properly within the scope of the ccNSO Scope, the Issue Manager shall inform the Council of this opinion. If after an analysis of the relevant factors according to Section 10.6 and Annex C a majority of 10 or more Council members is of the opinion the issue is within scope the Chair of the ccNSO shall inform the Issue Manager accordingly. General Counsel and the ccNSO Council shall engage in a dialogue according to agreed rules and procedures to resolve the matter. In the event no agreement is reached between General Counsel and the Council as to whether the issue is within or outside Scope of the ccNSO then by a vote of 15 or more members the Council may decide the issue is within scope. The Chair of the ccNSO shall inform General Counsel and the Issue Manager accordingly. The Issue Manager shall then proceed with a recommendation whether or not the Council should move to initiate the PDP including both the opinion and analysis of General Counsel and Council in the Issues Report.

f. In the event that the Manager Recommendation is in favor of initiating the PDP, a proposed time line for conducting each of the stages of PDP outlined herein ("**PDP Time Line**").

g. g. If possible, the issue report shall indicate whether the resulting output is likely to result in a policy to be approved by the Board. In some circumstances, it will not be possible to do this until substantive discussions on the issue have taken place. In these cases, the issue report should indicate this uncertainty. Upon completion of the Issue Report, the Issue Manager shall distribute it to the full Council for a vote on whether to initiate the PDP.

3. Initiation of PDP

The Council shall decide whether to initiate the PDP as follows:

a. Within 21 days after receipt of an Issue Report from the Issue Manager, the Council shall vote on whether to initiate the PDP. Such vote should be

taken at a meeting held in any manner deemed appropriate by the Council, including in person or by conference call, but if a meeting is not feasible the vote may occur by e-mail.

b. A vote of ten or more Council members in favor of initiating the PDP shall be required to initiate the PDP provided that the Issue Report states that the issue is properly within the scope of the Mission and the ccNSO Scope.

4. Decision Whether to Appoint Task Force; Establishment of Time Line

At the meeting of the Council where the PDP has been initiated (or, where the Council employs a vote by e-mail, in that vote) pursuant to Item 3 above, the Council shall decide, by a majority vote of members present at the meeting (or voting by e-mail), whether or not to appoint a task force to address the issue. If the Council votes:

a. In favor of convening a task force, it shall do so in accordance with Item 7 below.

b. Against convening a task force, then it shall collect information on the policy issue in accordance with Item 8 below.

The Council shall also, by a majority vote of members present at the meeting or voting by e-mail, approve or amend and approve the PDP Time Line set out in the Issue Report.

5. Composition and Selection of Task Forces

a. Upon voting to appoint a task force, the Council shall invite each of the Regional Organizations (see Section 10.5) to appoint two individuals to participate in the task force (the "**Representatives**"). Additionally, the Council may appoint up to three advisors (the "**Advisors**") from outside the ccNSO and, following formal request for GAC participation in the Task Force, accept up to two Representatives from the Governmental Advisory Committee to sit on the task force. The Council may increase the number of Representatives that may sit on a task force in its discretion in circumstances that it deems necessary or appropriate.

b. Any Regional Organization wishing to appoint Representatives to the task force must provide the names of the Representatives to the Issue Manager within ten (10) calendar days after such request so that they are included on the task force. Such Representatives need not be members of the Council, but each must be an individual who has an interest, and ideally knowledge and expertise, in the subject matter, coupled with the ability to devote a substantial amount of time to the task force's activities.

c. The Council may also pursue other actions that it deems appropriate to assist in the PDP, including appointing a particular individual or organization to gather information on the issue or scheduling meetings for deliberation or briefing. All such information shall be submitted to the Issue Manager in accordance with the PDP Time Line.

6. Public Notification of Initiation of the PDP and Comment Period

After initiation of the PDP, ICANN shall post a notification of such action to the Website and to the other ICANN Supporting Organizations and Advisory Committees. A comment period (in accordance with the PDP Time Line, and ordinarily at least 21 days long) shall be commenced for the issue. Comments shall be accepted from ccTLD managers, other Supporting Organizations, Advisory Committees, and from the public. The Issue Manager, or some other designated Council representative shall review the comments and incorporate them into a report (the "**Comment Report**") to be included in either the Preliminary Task Force Report or the Initial Report, as applicable.

7. Task Forces

a. *Role of Task Force.* If a task force is created, its role shall be responsible for (i) gathering information documenting the positions of the ccNSO members within the Geographic Regions and other parties and groups; and (ii) otherwise obtaining relevant information that shall enable the Task Force Report to be as complete and informative as possible to facilitate the Council's meaningful and informed deliberation.

The task force shall not have any formal decision-making authority. Rather, the role of the task force shall be to gather information that shall document the positions of various parties or groups as specifically and comprehensively as possible, thereby enabling the Council to have a meaningful and informed deliberation on the issue.

b. *Task Force Charter or Terms of Reference.* The Council, with the assistance of the Issue Manager, shall develop a charter or terms of reference for the task force (the "**Charter**") within the time designated in the PDP Time Line. Such Charter shall include:

1. The issue to be addressed by the task force, as such issue was articulated for the vote before the Council that initiated the PDP;

2. The specific time line that the task force must adhere to, as set forth below, unless the Council determines that there is a compelling reason to extend the timeline; and

3. Any specific instructions from the Council for the task force, including whether or not the task force should solicit the advice of outside advisors on the issue.

The task force shall prepare its report and otherwise conduct its activities in accordance with the Charter. Any request to deviate from the Charter must be formally presented to the Council and may only be undertaken by the task force upon a vote of a majority of the Council members present at a meeting or voting by e-mail. The quorum requirements of Section 10.3(n) shall apply to Council actions under this Item 7(b).

c. *Appointment of Task Force Chair.* The Issue Manager shall convene the first meeting of the task force within the time designated in the PDP Time Line. At the initial meeting, the task force members shall, among other things, vote to appoint a task force chair. The chair shall be responsible for organizing the activities of the task force, including compiling the Task Force Report. The chair of a task force need not be a member of the Council.

d. *Collection of Information*.

1. *Regional Organization Statements.* The Representatives shall each be responsible for soliciting the position of the Regional Organization for their Geographic Region, at a minimum, and may solicit other comments, as each Representative deems appropriate, including the comments of the ccNSO members in that region that are not members of the Regional Organization, regarding the issue under consideration. The position of the Regional Organization and any other comments gathered by the Representatives should be submitted in a formal statement to the task force chair (each, a "**Regional Statement**") within the time designated in the PDP Time Line. Every Regional Statement shall include at least the following:

(i) If a Supermajority Vote (as defined by the Regional Organization) was reached, a clear statement of the Regional Organization's position on the issue;

(ii) If a Supermajority Vote was not reached, a clear statement of all positions espoused by the members of the Regional Organization;

(iii) A clear statement of how the Regional Organization arrived at its position(s). Specifically, the statement should detail specific meetings, teleconferences, or other means of deliberating an issue, and a list of all members who participated or otherwise submitted their views;

(iv) A statement of the position on the issue of any ccNSO members that are not

members of the Regional Organization;

(v) An analysis of how the issue would affect the Region, including any financial impact on the Region; and

(vi) An analysis of the period of time that would likely be necessary to implement the policy.

2. Outside Advisors. The task force may, in its discretion, solicit the opinions of outside advisors, experts, or other members of the public. Such opinions should be set forth in a report prepared by such outside advisors, and (i) clearly labeled as coming from outside advisors; (ii) accompanied by a detailed statement of the advisors' (a) qualifications and relevant experience and (b) potential conflicts of interest. These reports should be submitted in a formal statement to the task force chair within the time designated in the PDP Time Line.

e. *Task Force Report.* The chair of the task force, working with the Issue Manager, shall compile the Regional Statements, the Comment Report, and other information or reports, as applicable, into a single document ("**Preliminary Task Force Report**") and distribute the Preliminary Task Force Report to the full task force within the time designated in the PDP Time Line. The task force shall have a final task force meeting to consider the issues and try and reach a Supermajority Vote. After the final task force meeting, the chair of the task force and the Issue Manager shall create the final task force report (the "**Task Force Report**") and post it on the Website and to the other ICANN Supporting Organizations and Advisory Committees. Each Task Force Report must include:

1. A clear statement of any Supermajority Vote (being 66% of the task force) position of the task force on the issue;

2. If a Supermajority Vote was not reached, a clear statement of all positions espoused by task force members submitted within the time line for submission of constituency reports. Each statement should clearly indicate (i) the reasons underlying the position and (ii) the Regional Organizations that held the position;

3. An analysis of how the issue would affect each Region, including any financial impact on the Region;

4. An analysis of the period of time that would likely be necessary to implement the policy; and

5. The advice of any outside advisors appointed to the task force by the Council, accompanied by a detailed statement of the advisors' (i) qualifications and relevant experience and (ii) potential conflicts of interest.

8. Procedure if No Task Force is Formed

a. If the Council decides not to convene a task force, each Regional Organization shall, within the time designated in the PDP Time Line, appoint a representative to solicit the Region's views on the issue. Each such representative shall be asked to submit a Regional Statement to the Issue Manager within the time designated in the PDP Time Line.

b. The Council may, in its discretion, take other steps to assist in the PDP, including, for example, appointing a particular individual or organization, to gather information on the issue or scheduling meetings for deliberation or briefing. All such information shall be submitted to the Issue Manager within the time designated in the PDP Time Line.

c. The Council shall formally request the Chair of the GAC to offer opinion or advice.

d. The Issue Manager shall take all Regional Statements, the Comment Report, and other information and compile (and post on the Website) an Initial Report within the time designated in the PDP Time Line. Thereafter, the Issue Manager shall, in accordance with Item 9 below, create a Final Report.

9. Comments to the Task Force Report or Initial Report

a. A comment period (in accordance with the PDP Time Line, and ordinarily at least 21 days long) shall be opened for comments on the Task Force Report or Initial Report. Comments shall be accepted from ccTLD managers, other Supporting Organizations, Advisory Committees, and from the public. All comments shall include the author's name, relevant experience, and interest in the issue.

b. At the end of the comment period, the Issue Manager shall review the comments received and may, in the Issue Manager's reasonable discretion, add appropriate comments to the Task Force Report or Initial Report, to prepare the "**Final Report**". The Issue Manager shall not be obligated to include all comments made during the comment period, nor shall the Issue Manager be obligated to include all comments submitted by any one individual or organization.

c. The Issue Manager shall prepare the Final Report and submit it to the Council chair within the time designated in the PDP Time Line.

10. Council Deliberation

a. Upon receipt of a Final Report, whether as the result of a task force or otherwise, the Council chair shall (i) distribute the Final Report to all Council members; (ii) call for a Council meeting within the time designated in the PDP Time Line wherein the Council shall work towards achieving a recommendation to present to the Board; and (iii) formally send to the GAC Chair an invitation to the GAC to offer opinion or advice. Such meeting may be held in any manner deemed appropriate by the Council, including in person or by conference call. The Issue Manager shall be present at the meeting.

b. The Council may commence its deliberation on the issue prior to the formal meeting, including via in-person meetings, conference calls, e-mail discussions, or any other means the Council may choose.

c. The Council may, if it so chooses, solicit the opinions of outside advisors at its final meeting. The opinions of these advisors, if relied upon by the Council, shall be (i) embodied in the Council's report to the Board, (ii) specifically identified as coming from an outside advisor; and (iii) accompanied by a detailed statement of the advisor's (a) qualifications and relevant experience and (b) potential conflicts of interest.

11. Recommendation of the Council

In considering whether to make a recommendation on the issue (a "**Council Recommendation**"), the Council shall seek to act by consensus. If a minority opposes a consensus position, that minority shall prepare and circulate to the Council a statement explaining its reasons for opposition. If the Council's discussion of the statement does not result in consensus, then a recommendation supported by 14 or more of the Council members shall be deemed to reflect the view of the Council, and shall be conveyed to the Members as the Council's Recommendation. Notwithstanding the foregoing, as outlined below, all viewpoints expressed by Council members during the PDP must be included in the Members Report.

12. Council Report to the Members

In the event that a Council Recommendation is adopted pursuant to Item 11 then the Issue Manager shall, within seven days after the Council meeting, incorporate the Council's Recommendation together with any other viewpoints of the Council members into a Members Report to be approved by the Council and then to be submitted to the Members (the "**Members Report**"). The Members Report must contain at least the following:

a. A clear statement of the Council's recommendation;

b. The Final Report submitted to the Council; and

c. A copy of the minutes of the Council's deliberation on the policy issue (see Item 10), including all the opinions expressed during such deliberation, accompanied by a description of who expressed such opinions.

13. Members Vote

Following the submission of the Members Report and within the time designated by the PDP Time Line, the ccNSO members shall be given an opportunity to vote on the Council Recommendation. The vote of members shall be electronic and members' votes shall be lodged over such a period of time as designated in the PDP Time Line (at least 21 days long).

In the event that at least 50% of the ccNSO members lodge votes within the voting period, the resulting vote will be employed without further process. In the event that fewer than 50% of the ccNSO members lodge votes in the first round of voting, the first round will not be employed and the results of a final, second round of voting, conducted after at least thirty days notice to the ccNSO members, will be employed if at least 50% of the ccNSO members lodge votes. In the event that more than 66% of the votes received at the end of the voting period shall be in favor of the Council Recommendation, then the recommendation shall be conveyed to the Board in accordance with Item 14 below as the ccNSO Recommendation.

14. Board Report

The Issue Manager shall within seven days after a ccNSO Recommendation being made in accordance with Item 13 incorporate the ccNSO Recommendation into a report to be approved by the Council and then to be submitted to the Board (the "**Board Report**"). The Board Report must contain at least the following:

a. A clear statement of the ccNSO recommendation;

b. The Final Report submitted to the Council; and

c. the Members' Report.

15. Board Vote

a. The Board shall meet to discuss the ccNSO Recommendation as soon as feasible after receipt of the Board Report from the Issue Manager, taking into account procedures for Board consideration.

b. The Board shall adopt the ccNSO Recommendation unless by a vote of more

than 66% the Board determines that such policy is not in the best interest of the ICANN community or of ICANN.

1. In the event that the Board determines not to act in accordance with the ccNSO Recommendation, the Board shall (i) state its reasons for its determination not to act in accordance with the ccNSO Recommendation in a report to the Council (the "**Board Statement**"); and (ii) submit the Board Statement to the Council.

2. The Council shall discuss the Board Statement with the Board within thirty days after the Board Statement is submitted to the Council. The Board shall determine the method (e.g., by teleconference, e-mail, or otherwise) by which the Council and Board shall discuss the Board Statement. The discussions shall be held in good faith and in a timely and efficient manner, to find a mutually acceptable solution.

3. At the conclusion of the Council and Board discussions, the Council shall meet to affirm or modify its Council Recommendation. A recommendation supported by 14 or more of the Council members shall be deemed to reflect the view of the Council (the Council's "**Supplemental Recommendation**"). That Supplemental Recommendation shall be conveyed to the Members in a Supplemental Members Report, including an explanation for the Supplemental Recommendation. Members shall be given an opportunity to vote on the Supplemental Recommendation under the same conditions outlined in Item 13 . In the event that more than 66% of the votes cast by ccNSO Members during the voting period are in favor of the Supplemental Recommendation then that recommendation shall be conveyed to Board as the ccNSO Supplemental Recommendation and the Board shall adopt the recommendation unless by a vote of more than 66% of the Board determines that acceptance of such policy would constitute a breach of the fiduciary duties of the Board to the Company.

4. In the event that the Board does not accept the ccNSO Supplemental Recommendation, it shall state its reasons for doing so in its final decision ("**Supplemental Board Statement**").

5. In the event the Board determines not to accept a ccNSO Supplemental Recommendation, then the Board shall not be entitled to set policy on the issue addressed by the recommendation and the status quo shall be preserved until such time as the ccNSO shall, under the ccPDP, make a recommendation on the issue that is deemed acceptable by the Board.

16. Implementation of the Policy

Upon adoption by the Board of a ccNSO Recommendation or ccNSO

Supplemental Recommendation, the Board shall, as appropriate, direct or authorize ICANN staff to implement the policy.

17. Maintenance of Records

With respect to each ccPDP for which an Issue Report is requested (see Item 1), ICANN shall maintain on the Website a status web page detailing the progress of each ccPDP, which shall provide a list of relevant dates for the ccPDP and shall also link to the following documents, to the extent they have been prepared pursuant to the ccPDP:

a. Issue Report;

b. PDP Time Line;

c. Comment Report;

d. Regional Statement(s);

e. Preliminary Task Force Report;

f. Task Force Report;

g. Initial Report;

h. Final Report;

i. Members' Report;

j. Board Report;

k. Board Statement;

l. Supplemental Members' Report; and

m. Supplemental Board Statement.

In addition, ICANN shall post on the Website comments received in electronic written form specifically suggesting that a ccPDP be initiated.

Annex C: The Scope of the ccNSO

This annex describes the scope and the principles and method of analysis to be used in any further development of the scope of the ccNSO's policy-development role. As provided in Section 10.6(b) of the Bylaws, that scope shall be defined according to the procedures of the ccPDP.

The scope of the ccNSO's authority and responsibilities must recognize the

complex relation between ICANN and ccTLD managers/registries with regard to policy issues. This annex shall assist the ccNSO, the ccNSO Council, and the Board and staff in delineating relevant global policy issues.

Policy areas

The ccNSO's policy role should be based on an analysis of the following functional model of the DNS:

1. Data is registered/maintained to generate a zone file,
2. A zone file is in turn used in TLD name servers.

Within a **TLD** two functions have to be performed (these are addressed in greater detail below):

1. Entering data into a database ("**Data Entry Function**") and
2. Maintaining and ensuring upkeep of name-servers for the TLD ("**Name Server Function**").

These two core functions must be performed at the ccTLD registry level as well as at a higher level (IANA function and root servers) and at lower levels of the DNS hierarchy. This mechanism, as RFC 1591 points out, is recursive:

There are no requirements on sub domains of top-level domains beyond the requirements on higher-level domains themselves. That is, the requirements in this memo are applied recursively. In particular, all sub domains shall be allowed to operate their own domain name servers, providing in them whatever information the sub domain manager sees fit (as long as it is true and correct).

The Core Functions

1. Data Entry Function (DEF):

Looking at a more detailed level, the first function (entering and maintaining data in a database) should be fully defined by a naming policy. This naming policy must specify the rules and conditions:

a. under which data will be collected and entered into a database or data changed (at the TLD level among others, data to reflect a transfer from registrant to registrant or changing registrar) in the database.

b. for making certain data generally and publicly available (be it, for example, through Whois or nameservers).

2. The Name-Server Function (NSF)

The name-server function involves essential interoperability and stability issues at the heart of the domain name system. The importance of this function extends to nameservers at the ccTLD level, but also to the root servers (and root-server system) and nameservers at lower levels.

On its own merit and because of interoperability and stability considerations, properly functioning nameservers are of utmost importance to the individual, as well as to the local and the global Internet communities.

With regard to the nameserver function, therefore, policies need to be defined and established. Most parties involved, including the majority of ccTLD registries, have accepted the need for common policies in this area by adhering to the relevant RFCs, among others RFC 1591.

Respective Roles with Regard to Policy, Responsibilities, and Accountabilities

It is in the interest of ICANN and ccTLD managers to ensure the stable and proper functioning of the domain name system. ICANN and the ccTLD registries each have a distinctive role to play in this regard that can be defined by the relevant policies. The scope of the ccNSO cannot be established without reaching a common understanding of the allocation of authority between ICANN and ccTLD registries.

Three roles can be distinguished as to which responsibility must be assigned on any given issue:

- Policy role: i.e. the ability and power to define a policy;
- Executive role: i.e. the ability and power to act upon and implement the policy; and
- Accountability role: i.e. the ability and power to hold the responsible entity accountable for exercising its power.

Firstly, responsibility presupposes a policy and this delineates the policy role. Depending on the issue that needs to be addressed those who are involved in defining and setting the policy need to be determined and defined. Secondly, this presupposes an executive role defining the power to implement and act within the boundaries of a policy. Finally, as a counter-balance to the executive role, the accountability role needs to defined and determined.

The information below offers an aid to:

1. delineate and identify specific policy areas;

2. define and determine roles with regard to these specific policy areas.

This annex defines the scope of the ccNSO with regard to developing policies. The scope is limited to the policy role of the ccNSO policy-development process for functions and levels explicitly stated below. It is anticipated that the accuracy of the assignments of policy, executive, and accountability roles shown below will be considered during a scope-definition ccPDP process.

Name Server Function (as to ccTLDs)

Level 1: Root Name Servers
Policy role: IETF, RSSAC (ICANN)
Executive role: Root Server System Operators
Accountability role: RSSAC (ICANN)

Level 2: ccTLD Registry Name Servers in respect to interoperability
Policy role: ccNSO Policy Development Process (ICANN), for best practices a ccNSO process can be organized
Executive role: ccTLD Manager
Accountability role: part ICANN (IANA), part Local Internet Community, including local government

Level 3: User's Name Servers
Policy role: ccTLD Manager, IETF (RFC)
Executive role: Registrant
Accountability role: ccTLD Manager

Data Entry Function (as to ccTLDs)

Level 1: Root Level Registry
Policy role: ccNSO Policy Development Process (ICANN)
Executive role: ICANN (IANA)
Accountability role: ICANN community, ccTLD Managers, (national authorities in some cases)

Level 2: ccTLD Registry
Policy role: Local Internet Community, including local government, and/or ccTLD Manager according to local structure
Executive role: ccTLD Manager
Accountability role: Local Internet Community, including national authorities in some cases

Level 3: Second and Lower Levels
Policy role: Registrant
Executive role: Registrant
Accountability role: Registrant, users of lower-level domain names

ANNEX D: EC MECHANISM

ARTICLE 1 PROCEDURE FOR EXERCISE OF EC'S RIGHTS TO APPROVE APPROVAL ACTIONS

Section 1.1. APPROVAL ACTIONS

The processes set forth in this Article 1 shall govern the escalation procedures for the EC's exercise of its right to approve the following (each, an "**Approval Action**") under the Bylaws:

a. Fundamental Bylaw Amendments, as contemplated by Section 25.2 of the Bylaws;

b. Articles Amendments, as contemplated by Section 25.2 of the Bylaws; and

c. Asset Sales, as contemplated by Article 26 of the Bylaws.

Section 1.2. APPROVAL PROCESS

Following the delivery of a Board Notice for an Approval Action ("**Approval Action Board Notice**") by the Secretary to the EC Administration and the Decisional Participants (which delivery date shall be referred to herein as the "**Approval Action Board Notification Date**"), the Decisional Participants shall thereafter promptly inform their constituents of the delivery of the Approval Action Board Notice. Any Approval Action Board Notice relating to a Fundamental Bylaw Amendment or Articles Amendment shall include a statement, if applicable, that the Fundamental Bylaw Amendment or Articles Amendment, as applicable, is based solely on the outcome of a PDP, citing the specific PDP and the provision in the Fundamental Bylaw Amendment or Articles Amendment subject to the Approval Action Board Notice that implements such PDP (as applicable, a "**PDP Fundamental Bylaw Statement**" or "**PDP Articles Statement**") and the name of the Supporting Organization that is a Decisional Participant that undertook the PDP relating to the Fundamental Bylaw Amendment or Articles Amendment, as applicable (as applicable, the "**Fundamental Bylaw Amendment PDP Decisional Participant**" or "**Articles Amendment PDP Decisional Participant**"). The process set forth in this Section 1.2 of this Annex D as it relates to a particular Approval Action is referred to herein as the "**Approval Process**."

Section 1.3. APPROVAL ACTION COMMUNITY FORUM

a. ICANN shall, at the direction of the EC Administration, convene a forum at which the Decisional Participants and interested parties may discuss the Approval Action (an "**Approval Action Community Forum**").

b. If the EC Administration requests a publicly-available conference call by providing a notice to the Secretary, ICANN shall, at the direction of the EC Administration, schedule such call prior to any Approval Action Community Forum, and inform the Decisional Participants of the date, time and participation methods of such conference call, which ICANN shall promptly post on the Website.

c. The Approval Action Community Forum shall be convened and concluded during the period beginning upon the Approval Action Board Notification Date and ending at 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 30th day after the Approval Action Board Notification Date ("**Approval Action Community Forum Period**"). If the EC Administration requests that the Approval Action Community Forum be held during the next scheduled ICANN public meeting, the Approval Action Community Forum shall be held during the next scheduled ICANN public meeting on the date and at the time determined by ICANN, taking into account any date and/or time requested by the EC Administration. If the Approval Action Community Forum is held during the next scheduled ICANN public meeting and that public meeting is held after 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 30th day after the Approval Action Board Notification Date, the Approval Action Community Forum Period for the Approval Action shall expire at 11:59 p.m., local time of the city hosting such ICANN public meeting on the official last day of such ICANN public meeting.

d. The Approval Action Community Forum shall be conducted via remote participation methods such as teleconference, web-based meeting room and/or such other form of remote participation as the EC Administration selects, and/or, only if the Approval Action Community Forum is held during an ICANN public meeting, face-to-face meetings. If the Approval Action Community Forum will not be held during an ICANN public meeting, the EC Administration shall promptly inform ICANN of the date, time and participation methods of such Approval Action Community Forum, which ICANN shall promptly post on the Website.

e. The EC Administration shall manage and moderate the Approval Action Community Forum in a fair and neutral manner.

f. ICANN and any Supporting Organization or Advisory Committee (including

Decisional Participants) may deliver to the EC Administration in writing its views and questions on the Approval Action prior to the convening of and during the Approval Action Community Forum. Any written materials delivered to the EC Administration shall also be delivered to the Secretary for prompt posting on the Website in a manner deemed appropriate by ICANN.

g. ICANN staff and Directors representing the Board are expected to attend the Approval Action Community Forum in order to address any questions or concerns regarding the Approval Action.

h. For the avoidance of doubt, the Approval Action Community Forum is not a decisional body.

i. During the Approval Action Community Forum Period, an additional one or two Community Forums may be held at the discretion of the Board or the EC Administration. If the Board decides to hold an additional one or two Approval Action Community Forums, it shall provide a rationale for such decision, which rationale ICANN shall promptly post on the Website.

j. ICANN will provide support services for the Approval Action Community Forum and shall promptly post on the Website a public record of the Approval Action Community Forum as well as all written submissions of ICANN and any Supporting Organization or Advisory Committee (including Decisional Participants) related to the Approval Action Community Forum.

Section 1.4. DECISION WHETHER TO APPROVE AN APPROVAL ACTION

(a) Following the expiration of the Approval Action Community Forum Period, at any time or date prior to 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 21st day after the expiration of the Approval Action Community Forum Period (such period, the "**Approval Action Decision Period**"), with respect to each Approval Action, each Decisional Participant shall inform the EC Administration in writing as to whether such Decisional Participant (i) supports such Approval Action, (ii) objects to such Approval Action or (iii) has determined to abstain from the matter (which shall not count as supporting or objecting to such Approval Action), and each Decisional Participant shall forward such notice to the Secretary for ICANN to promptly post on the Website. If a Decisional Participant does not inform the EC Administration of any of the foregoing prior to the expiration of the Approval Action Decision Period, the Decisional Participant shall be deemed to have abstained from the matter (even if such Decisional Participant informs the EC Administration of its support or objection following the expiration of the Approval Action Decision Period).

(b) The EC Administration shall, within twenty-four (24) hours of the expiration of

the Approval Action Decision Period, deliver a written notice ("**EC Approval Notice**") to the Secretary certifying that, pursuant to and in compliance with the procedures and requirements of this Article 1 of this Annex D, the EC has approved the Approval Action if:

> (i) The Approval Action does not relate to a Fundamental Bylaw Amendment or Articles Amendment and is (A) supported by three or more Decisional Participants and (B) not objected to by more than one Decisional Participant;
>
> (ii) The Approval Action relates to a Fundamental Bylaw Amendment and is (A) supported by three or more Decisional Participants (including the Fundamental Bylaw Amendment PDP Decisional Participant if the Board Notice included a PDP Fundamental Bylaw Statement) and (B) not objected to by more than one Decisional Participant; or
>
> (iii) The Approval Action relates to an Articles Amendment and is (A) supported by three or more Decisional Participants (including the Articles Amendment PDP Decisional Participant if the Board Notice included a PDP Articles Statement) and (B) not objected to by more than one Decisional Participant.

(c) If the Approval Action does not obtain the support required by Section 1.4(b)(i), (ii) or (iii) of this Annex D, as applicable, the Approval Process will automatically be terminated and the EC Administration shall, within twenty-four (24) hours of the expiration of the Approval Action Decision Period, deliver to the Secretary a notice certifying that the Approval Process has been terminated with respect to the Approval Action ("**Approval Process Termination Notice**").

(d) ICANN shall promptly post to the Website any (i) Approval Action Board Notice, (ii) EC Approval Notice, (iii) Approval Process Termination Notice, (iv) written explanation provided by the EC Administration related to any of the foregoing, and (v) other notices the Secretary receives under this Article 1.

ARTICLE 2 PROCEDURE FOR EXERCISE OF EC'S RIGHTS TO REJECT SPECIFIED ACTIONS

Section 2.1. Rejection Actions

The processes set forth in this Article 2 shall govern the escalation procedures for the EC's exercise of its right to reject the following (each, a "**Rejection Action**")

under the Bylaws:

a. PTI Governance Actions, as contemplated by Section 16.2(d) of the Bylaws;

b. IFR Recommendation Decisions, as contemplated by Section 18.6(d) of the Bylaws;

c. Special IFR Recommendation Decisions, as contemplated by Section 18.12(e) of the Bylaws;

d. SCWG Creation Decisions, as contemplated by Section 19.1(d) of the Bylaws;

e. SCWG Recommendation Decisions, as contemplated by Section 19.4(d) of the Bylaws;

f. ICANN Budgets, as contemplated by Section 22.4(a)(v) of the Bylaws;

g. IANA Budgets, as contemplated by Section 22.4(b)(v) of the Bylaws;

h. Operating Plans, as contemplated by Section 22.5(a)(v) of the Bylaws;

i. Strategic Plans, as contemplated by Section 22.5(b)(v) of the Bylaws; and

j. Standard Bylaw Amendments, as contemplated by Section 25.1(e) of the Bylaws.

Section 2.2. PETITION PROCESS FOR SPECIFIED ACTIONS

(a) Following the delivery of a Board Notice for a Rejection Action ("**Rejection Action Board Notice**") by the Secretary to the EC Administration and Decisional Participants (which delivery date shall be referred to herein as the "**Rejection Action Board Notification Date**"), the Decisional Participants shall thereafter promptly inform their constituents of the delivery of the Rejection Action Board Notice. The process set forth in this Section 2.2 of this Annex D as it relates to a particular Rejection Action is referred to herein as the "**Rejection Process**."

(b) During the period beginning on the Rejection Action Board Notification Date and ending at 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the date that is the 21st day after the Rejection Action Board Notification Date (as it relates to a particular Rejection Action, the "**Rejection Action Petition Period**"), subject to the procedures and requirements developed by the applicable Decisional Participant, an individual may submit a petition to a Decisional Participant, seeking to reject the Rejection Action and initiate the Rejection Process (a "**Rejection Action Petition**").

(c) A Decisional Participant that has received a Rejection Action Petition shall either accept or reject such Rejection Action Petition; provided that a Decisional Participant may only accept such Rejection Action Petition if it was received by such Decisional Participant during the Rejection Action Petition Period.

(i) If, in accordance with the requirements of Section 2.2(c) of this Annex D, a Decisional Participant accepts a Rejection Action Petition during the Rejection Action Petition Period, the Decisional Participant shall promptly provide to the EC Administration, the other Decisional Participants and the Secretary written notice ("**Rejection Action Petition Notice**") of such acceptance (such Decisional Participant, the "**Rejection Action Petitioning Decisional Participant**"), and ICANN shall promptly post such Rejection Action Petition Notice on the Website. The Rejection Action Petition Notice shall also include:

(A) the rationale upon which rejection of the Rejection Action is sought. Where the Rejection Action Petition Notice relates to an ICANN Budget, an IANA Budget, an Operating Plan or a Strategic Plan, the Rejection Action Petition Notice shall not be valid and shall not be accepted by the EC Administration unless the rationale set forth in the Rejection Action Petition Notice is based on one or more significant issues that were specifically raised in the applicable public comment period(s) relating to perceived inconsistencies with the Mission, purpose and role set forth in ICANN's Articles of Incorporation and Bylaws, the global public interest, the needs of ICANN's stakeholders, financial stability, or other matter of concern to the community; and

(B) where the Rejection Action Petition Notice relates to a Standard Bylaw Amendment, a statement, if applicable, that the Standard Bylaw Amendment is based solely on the outcome of a PDP, citing the specific PDP and the provision in the Standard Bylaw Amendment subject to the Board Notice that implements such PDP ("**PDP Standard Bylaw Statement**") and the name of the Supporting Organization that is a Decisional Participant that undertook the PDP relating to the Standard Bylaw Amendment ("**Standard Bylaw Amendment PDP Decisional Participant**").

The Rejection Process shall thereafter continue pursuant to Section 2.2(d) of this Annex D.

(ii) If the EC Administration has not received a Rejection Action Petition Notice pursuant to Section 2.2(c)(i) of this Annex D during the Rejection

Action Petition Period, the Rejection Process shall automatically be terminated and the EC Administration shall, within twenty-four (24) hours of the expiration of the Rejection Action Petition Period, deliver to the Secretary a notice certifying that the Rejection Process has been terminated with respect to the Rejection Action contained in the Approval Notice ("**Rejection Process Termination Notice**"). ICANN shall promptly post such Rejection Process Termination Notice on the Website.

(d) Following the delivery of a Rejection Action Petition Notice to the EC Administration pursuant to Section 2.2(c)(i) of this Annex D, the Rejection Action Petitioning Decisional Participant shall contact the EC Administration and the other Decisional Participants to determine whether any other Decisional Participants support the Rejection Action Petition. The Rejection Action Petitioning Decisional Participant shall forward such communication to the Secretary for ICANN to promptly post on the Website.

(i) If the Rejection Action Petitioning Decisional Participant obtains the support of at least one other Decisional Participant (a "**Rejection Action Supporting Decisional Participant**") during the period beginning upon the expiration of the Rejection Action Petition Period and ending at 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 7th day after the expiration of the Rejection Action Petition Period (the "**Rejection Action Petition Support Period**"), the Rejection Action Petitioning Decisional Participant shall provide a written notice to the EC Administration, the other Decisional Participants and the Secretary ("**Rejection Action Supported Petition**") within twenty-four (24) hours of receiving the support of at least one Rejection Action Supporting Decisional Participant, and ICANN shall promptly post such Rejection Action Supported Petition on the Website. Each Rejection Action Supporting Decisional Participant shall provide a written notice to the EC Administration, the other Decisional Participants and the Secretary within twenty-four (24) hours of providing support to the Rejection Action Petition, and ICANN shall promptly post each such notice on the Website. Such Rejection Action Supported Petition shall include:

(A) a supporting rationale in reasonable detail;

(B) contact information for at least one representative who has been designated by the Rejection Action Petitioning Decisional Participant who shall act as a liaison with respect to the Rejection Action Supported Petition;

(C) a statement as to whether or not the Rejection Action Petitioning Decisional Participant and/or the Rejection Action Supporting Decisional Participant requests that ICANN organize a publicly-available conference call prior to the Rejection Action Community Forum (as defined in Section 2.3 of this Annex D) for the community to discuss the Rejection Action Supported Petition;

(D) a statement as to whether the Rejection Action Petitioning Decisional Participant and the Rejection Action Supporting Decisional Participant have determined to hold the Rejection Action Community Forum during the next scheduled ICANN public meeting, taking into account the limitation on holding such a Rejection Action Community Forum when the Rejection Action Supported Petition relates to an ICANN Budget or IANA Budget as described in Section 2.3(c) of this Annex D; and

(E) a PDP Standard Bylaw Statement, if applicable.

The Rejection Process shall thereafter continue for such Rejection Action Supported Petition pursuant to Section 2.3 of this Annex D. The foregoing process may result in more than one Rejection Action Supported Petition relating to the same Rejection Action.

(ii) The Rejection Process shall automatically be terminated and the EC Administration shall, within twenty-four (24) hours of the expiration of the Rejection Action Petition Support Period, deliver to the Secretary a Rejection Process Termination Notice, which ICANN shall promptly post on the Website, if:

(A) no Rejection Action Petitioning Decisional Participant is able to obtain the support of at least one other Decisional Participant for its Rejection Action Petition during the Rejection Action Petition Support Period; or

(B) where the Rejection Action Supported Petition includes a PDP Standard Bylaw Statement, the Standard Bylaw Amendment PDP Decisional Participant is not (x) the Rejection Action Petitioning Decisional Participant or (y) one of the Rejection Action Supporting Decisional Participants.

Section 2.3. REJECTION ACTION COMMUNITY FORUM

a. If the EC Administration receives a Rejection Action Supported Petition under Section 2.2(d) of this Annex D during the Rejection Action Petition Support Period, ICANN shall, at the direction of the EC Administration, convene a forum at which the Decisional Participants and interested parties

may discuss the Rejection Action Supported Petition ("**Rejection Action Community Forum**"). If the EC Administration receives more than one Rejection Action Supported Petition relating to the same Rejection Action, all such Rejection Action Supported Petitions shall be discussed at the same Rejection Action Community Forum.

b. If a publicly-available conference call has been requested in a Rejection Action Supported Petition, ICANN shall, at the direction of the EC Administration, schedule such call prior to any Rejection Action Community Forum relating to that Rejection Action Supported Petition, and inform the Decisional Participants of the date, time and participation methods of such conference call, which ICANN shall promptly post on the Website. If a conference call has been requested in relation to more than one Rejection Action Supported Petition relating to the same Rejection Action, all such Rejection Action Supported Petitions shall be discussed during the same conference call.

c. The Rejection Action Community Forum shall be convened and concluded during the period beginning upon the expiration of the Rejection Action Petition Support Period and ending at 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 21st day after the expiration of the Rejection Action Petition Support Period ("**Rejection Action Community Forum Period**") unless all Rejection Action Supported Petitions relating to the same Rejection Action requested that the Rejection Action Community Forum be held during the next scheduled ICANN public meeting, in which case the Rejection Action Community Forum shall be held during the next scheduled ICANN public meeting (except as otherwise provided below with respect to a Rejection Action Supported Petition relating to an ICANN Budget or IANA Budget) on the date and at the time determined by ICANN, taking into account any date and/or time requested by the Rejection Action Petitioning Decisional Participant(s) and the Rejection Action Supporting Decisional Participant(s). If the Rejection Action Community Forum is held during the next scheduled ICANN public meeting and that public meeting is held after 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 21st day after the expiration of the Rejection Action Petition Support Period, the Rejection Action Community Forum Period shall expire at 11:59 p.m., local time of the city hosting such ICANN public meeting on the official last day of such ICANN public meeting. Notwithstanding the foregoing and notwithstanding any statement in the Rejection Action Supported Petition, a Rejection Action Community Forum to discuss a Rejection Action Supported Petition relating to an ICANN Budget or IANA Budget may only be held at a scheduled ICANN public meeting if such Rejection Action Community Forum occurs during the Rejection Action Community Forum Period,

without any extension of such Rejection Action Community Forum Period.

d. The Rejection Action Community Forum shall be conducted via remote participation methods such as teleconference, web-based meeting room and/or such other form of remote participation as the EC Administration selects, and/or, only if the Rejection Action Community Forum is held during an ICANN public meeting, face-to-face meetings. If the Rejection Action Community Forum will not be held during an ICANN public meeting, the EC Administration shall promptly inform ICANN of the date, time and participation methods of such Rejection Action Community Forum, which ICANN shall promptly post on the Website.

e. The EC Administration shall manage and moderate the Rejection Action Community Forum in a fair and neutral manner.

f. ICANN and any Supporting Organization or Advisory Committee (including Decisional Participants) may deliver to the EC Administration in writing its views and questions on the Rejection Action Supported Petition prior to the convening of and during the Rejection Action Community Forum. Any written materials delivered to the EC Administration shall also be delivered to the Secretary for prompt posting on the Website in a manner deemed appropriate by ICANN.

g. ICANN staff (including the CFO when the Rejection Action Supported Petition relates to an ICANN Budget, IANA Budget or Operating Plan) and Directors representing the Board are expected to attend the Rejection Action Community Forum in order to address the concerns raised in the Rejection Action Supported Petition.

h. If the Rejection Action Petitioning Decisional Participant and each of the Rejection Action Supporting Decisional Participants for an applicable Rejection Action Supported Petition agree before, during or after the Rejection Action Community Forum that the issue raised in such Rejection Action Supported Petition has been resolved, such Rejection Action Supported Petition shall be deemed withdrawn and the Rejection Process with respect to such Rejection Action Supported Petition will be terminated. If all Rejection Action Supported Petitions relating to a Rejection Action are withdrawn, the Rejection Process will automatically be terminated. If a Rejection Process is terminated, the EC Administration shall, within twenty-four (24) hours of the resolution of the issue raised in the Rejection Action Supported Petition, deliver to the Secretary a Rejection Process Termination Notice. For the avoidance of doubt, the Rejection Action Community Forum is not a decisional body and the foregoing resolution process shall be handled pursuant to the internal procedures of the Rejection Action Petitioning Decisional Participant and the Rejection Action

Supporting Decisional Participant(s).

i. During the Rejection Action Community Forum Period, an additional one or two Rejection Action Community Forums may be held at the discretion of a Rejection Action Petitioning Decisional Participant and a related Rejection Action Supporting Decisional Participant, or the EC Administration.

j. ICANN will provide support services for the Rejection Action Community Forum and shall promptly post on the Website a public record of the Rejection Action Community Forum as well as all written submissions of ICANN and any Supporting Organization or Advisory Committee (including Decisional Participants) related to the Rejection Action Community Forum.

Section 2.4. DECISION WHETHER TO REJECT A REJECTION ACTION

(a) Following the expiration of the Rejection Action Community Forum Period, at any time or date prior to 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 21st day after the expiration of the Rejection Action Community Forum Period (such period, the "**Rejection Action Decision Period**"), with respect to each Rejection Action Supported Petition, each Decisional Participant shall inform the EC Administration in writing as to whether such Decisional Participant (i) supports such Rejection Action Supported Petition and has determined to reject the Rejection Action, (ii) objects to such Rejection Action Supported Petition or (iii) has determined to abstain from the matter (which shall not count as supporting or objecting to such Rejection Action Supported Petition), and each Decisional Participant shall forward such notice to the Secretary for ICANN to promptly post on the Website. If a Decisional Participant does not inform the EC Administration of any of the foregoing prior to expiration of the Rejection Action Decision Period, the Decisional Participant shall be deemed to have abstained from the matter (even if such Decisional Participant informs the EC Administration of its support or objection following the expiration of the Rejection Action Decision Period).

(b) The EC Administration, within twenty-four (24) hours of the expiration of the Rejection Action Decision Period, shall promptly deliver a written notice ("**EC Rejection Notice**") to the Secretary certifying that, pursuant to and in compliance with the procedures and requirements of this Article 2 of Annex D, the EC has resolved to reject the Rejection Action if (after accounting for any adjustments to the below as required by the GAC Carve-out pursuant to Section 3.6(e) of the Bylaws if the Rejection Action Supported Petition included a GAC Consensus Statement):

> (i) A Rejection Action Supported Petition relating to a Rejection Action other

> than a Standard Bylaw Amendment is (A) supported by four or more Decisional Participants and (B) not objected to by more than one Decisional Participant; or
>
> (ii) A Rejection Action Supported Petition relating to a Standard Bylaw Amendment that is (A) supported by three or more Decisional Participants (including the Standard Bylaw Amendment PDP Decisional Participant if the Rejection Action Supported Petition included a PDP Standard Bylaw Statement) and (B) not objected to by more than one Decisional Participant.

(c) If no Rejection Action Supported Petition obtains the support required by Section 2.4(b)(i) or (ii) of this Annex D, as applicable, the Rejection Process will automatically be terminated and the EC Administration shall, within twenty-four (24) hours of the expiration of the Rejection Action Decision Period, deliver to the Secretary a Rejection Process Termination Notice.

(d) ICANN shall promptly post to the Website any (i) Rejection Action Board Notice, (ii) Rejection Action Petition, (iii) Rejection Action Petition Notice, (iv) Rejection Action Supported Petition, (v) EC Rejection Notice and the written explanation provided by the EC Administration as to why the EC has chosen to reject the Rejection Action, (vi) Rejection Process Termination Notice, and (vii) other notices the Secretary receives under this Article 2.

ARTICLE 3 PROCEDURE FOR EXERCISE OF EC'S RIGHTS TO REMOVE DIRECTORS AND RECALL THE BOARD

Section 3.1. NOMINATING COMMITTEE DIRECTOR REMOVAL PROCESS

(a) Subject to the procedures and requirements developed by the applicable Decisional Participant, an individual may submit a petition to a Decisional Participant seeking to remove a Director holding Seats 1 through 8 and initiate the Nominating Committee Director Removal Process ("**Nominating Committee Director Removal Petition**"). Each Nominating Committee Director Removal Petition shall set forth the rationale upon which such individual seeks to remove such Director. The process set forth in this Section 3.1 of Annex D is referred to herein as the "**Nominating Committee Director Removal Process**."

(b) During the period beginning on the date that the Decisional Participant received the Nominating Committee Director Removal Petition (such date of receipt, the "**Nominating Committee Director Removal Petition Date**") and ending at 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the date that is the 21st day after the Nominating Committee

Director Removal Petition Date (as it relates to a particular Director, the "**Nominating Committee Director Removal Petition Period**"), the Decisional Participant that has received a Nominating Committee Director Removal Petition ("**Nominating Committee Director Removal Petitioned Decisional Participant**") shall either accept or reject such Nominating Committee Director Removal Petition; provided that a Nominating Committee Director Removal Petitioned Decisional Participant shall not accept a Nominating Committee Director Removal Petition if, during the same term, the Director who is the subject of such Nominating Committee Director Removal Petition had previously been subject to a Nominating Committee Director Removal Petition that led to a Nominating Committee Director Removal Community Forum (as discussed in Section 3.1(e) of this Annex D).

(c) During the Nominating Committee Director Removal Petition Period, the Nominating Committee Director Removal Petitioned Decisional Participant shall invite the Director subject to the Nominating Committee Director Removal Petition and the Chair of the Board (or the Vice Chair of the Board if the Chair is the affected Director) to a dialogue with the individual(s) bringing the Nominating Committee Director Removal Petition and the Nominating Committee Director Removal Petitioned Decisional Participant's representative on the EC Administration. The Nominating Committee Director Removal Petition may not be accepted unless this invitation has been extended upon reasonable notice and accommodation to the affected Director's availability. If the invitation is accepted by either the Director who is the subject of the Nominating Committee Director Removal Petition or the Chair of the Board (or the Vice Chair of the Board if the Chair is the affected Director), the Nominating Committee Director Removal Petitioned Decisional Participant shall not accept the Nominating Committee Director Removal Petition until the dialogue has occurred or there have been reasonable efforts to have the dialogue.

(i) If, in accordance with Section 3.1(b) of this Annex D, a Nominating Committee Director Removal Petitioned Decisional Participant accepts a Nominating Committee Director Removal Petition during the Nominating Committee Director Removal Petition Period (such Decisional Participant, the "**Nominating Committee Director Removal Petitioning Decisional Participant**"), the Nominating Committee Director Removal Petitioning Decisional Participant shall, within twenty-four (24) hours of its acceptance of the Nominating Committee Director Removal Petition, provide written notice ("**Nominating Committee Director Removal Petition Notice**") of such acceptance to the EC Administration, the other Decisional Participants and the Secretary. The Nominating Committee Director Removal Petition Notice shall include the rationale upon which removal of the affected

Director is sought. The Nominating Committee Director Removal Process shall thereafter continue pursuant to Section 3.1(d) of this Annex D.

(ii) If the EC Administration has not received a Nominating Committee Director Removal Petition Notice pursuant to Section 3.1(c)(i) of this Annex D during the Nominating Committee Director Removal Petition Period, the Nominating Committee Director Removal Process shall automatically be terminated with respect to the applicable Nominating Committee Director Removal Petition and the EC Administration shall, within twenty-four (24) hours of the expiration of the Nominating Committee Director Removal Petition Period, deliver to the Secretary a notice certifying that the Nominating Committee Director Removal Process has been terminated with respect to the applicable Nominating Committee Director Removal Petition ("**Nominating Committee Director Removal Process Termination Notice**").

(d) Following the delivery of a Nominating Committee Director Removal Petition Notice to the EC Administration by a Nominating Committee Director Removal Petitioning Decisional Participant pursuant to Section 3.1(c)(i) of this Annex D, the Nominating Committee Director Removal Petitioning Decisional Participant shall contact the EC Administration and the other Decisional Participants to determine whether any other Decisional Participants support the Nominating Committee Director Removal Petition. The Nominating Committee Director Removal Petitioning Decisional Participant shall forward such communication to the Secretary for ICANN to promptly post on the Website.

(i) If the Nominating Committee Director Removal Petitioning Decisional Participant obtains the support of at least one other Decisional Participant (a "**Nominating Committee Director Removal Supporting Decisional Participant**") during the period beginning upon the expiration of the Nominating Committee Director Removal Petition Period and ending at 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 7th day after the expiration of the Nominating Committee Director Removal Petition Period (the "**Nominating Committee Director Removal Petition Support Period**"), the Nominating Committee Director Removal Petitioning Decisional Participant shall provide a written notice to the EC Administration, the other Decisional Participants and the Secretary ("**Nominating Committee Director Removal Supported Petition**") within twenty-four (24) hours of receiving the support of at least one Nominating Committee Director Removal Supporting Decisional Participant. Each Nominating Committee Director Removal Supporting Decisional Participant

shall provide a written notice to the EC Administration, the other Decisional Participants and the Secretary within twenty-four (24) hours of providing support to the Nominating Committee Director Removal Petition. Such Nominating Committee Director Removal Supported Petition shall include:

(A) a supporting rationale in reasonable detail;

(B) contact information for at least one representative who has been designated by the Nominating Committee Director Removal Petitioning Decisional Participant who shall act as a liaison with respect to the Nominating Committee Director Removal Supported Petition;

(C) a statement as to whether or not the Nominating Committee Director Removal Petitioning Decisional Participant and/or the Nominating Committee Director Removal Supporting Decisional Participant requests that ICANN organize a publicly-available conference call prior to the Nominating Committee Director Removal Community Forum (as defined in Section 3.1(e) of this Annex D) for the community to discuss the Nominating Committee Director Removal Supported Petition; and

(D) a statement as to whether the Nominating Committee Director Removal Petitioning Decisional Participant and the Nominating Committee Director Removal Supporting Decisional Participant have determined to hold the Nominating Committee Director Removal Community Forum during the next scheduled ICANN public meeting.

The Nominating Committee Director Removal Process shall thereafter continue for such Nominating Committee Director Removal Petition pursuant to Section 3.1(e) of this Annex D.

(ii) The Nominating Committee Director Removal Process shall automatically be terminated and the EC Administration shall, within twenty-four (24) hours of the expiration of the Nominating Committee Director Removal Petition Support Period, deliver to the Secretary a Nominating Committee Director Removal Process Termination Notice if the Nominating Committee Director Removal Petitioning Decisional Participant is unable to obtain the support of at least one other Decisional Participant for its Nominating Committee Director Removal Petition during the Nominating Committee Director Removal Petition Support Period.

(e) If the EC Administration receives a Nominating Committee Director Removal Supported Petition under Section 3.1(d) of this Annex D during the Nominating Committee Director Removal Petition Support Period, ICANN shall, at the

direction of the EC Administration, convene a forum at which the Decisional Participants and interested parties may discuss the Nominating Committee Director Removal Supported Petition ("**Nominating Committee Director Removal Community Forum**").

(i) If a publicly-available conference call has been requested in a Nominating Committee Director Removal Supported Petition, ICANN shall, at the direction of the EC Administration, schedule such call prior to any Nominating Committee Director Removal Community Forum, and inform the Decisional Participants of the date, time and participation methods of such conference call, which ICANN shall promptly post on the Website. The date and time of any such conference call shall be determined after consultation with the Director who is the subject of the Nominating Committee Director Removal Supported Petition regarding his or her availability.

(ii) The Nominating Committee Director Removal Community Forum shall be convened and concluded during the period beginning upon the expiration of the Nominating Committee Director Removal Petition Support Period and ending at 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 21st day after the expiration of the Nominating Committee Director Removal Petition Support Period ("**Nominating Committee Director Removal Community Forum Period**") unless the Nominating Committee Director Removal Supported Petition requested that the Nominating Committee Director Removal Community Forum be held during the next scheduled ICANN public meeting, in which case the Nominating Committee Director Removal Community Forum shall be held during the next scheduled ICANN public meeting on the date and at the time determined by ICANN, taking into account any date and/or time requested by the Nominating Committee Director Removal Petitioning Decisional Participant and the Nominating Committee Director Removal Supporting Decisional Participant(s); provided, that, the date and time of any Nominating Committee Director Removal Community Forum shall be determined after consultation with the Director who is the subject of the Nominating Committee Director Removal Supported Petition regarding his or her availability. If the Nominating Committee Director Removal Community Forum is held during the next scheduled ICANN public meeting and that public meeting is held after 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 21st day after the expiration of the Nominating Committee Director Removal Petition Support Period, the Nominating Committee Director Removal Community Forum Period shall expire at 11:59 p.m., local time of the city hosting such ICANN public meeting on the official last day of such ICANN public meeting.

(iii) The Nominating Committee Director Removal Community Forum shall be conducted via remote participation methods such as teleconference, web-based meeting room and/or such other form of remote participation as the EC Administration selects, and/or, only if the Nominating Committee Director Removal Community Forum is held during an ICANN public meeting, face-to-face meetings. If the Nominating Committee Director Removal Community Forum will not be held during an ICANN public meeting, the EC Administration shall promptly inform ICANN of the date, time and participation methods of the Nominating Committee Director Removal Community Forum, which ICANN shall promptly post on the Website.

(iv) The EC Administration shall manage and moderate the Nominating Committee Director Removal Community Forum in a fair and neutral manner; provided that no individual from the Nominating Committee Director Removal Petitioning Decisional Participant or the Nominating Committee Director Removal Supporting Decisional Participant, nor the individual who initiated the Nominating Committee Director Removal Petition, shall be permitted to participate in the management or moderation of the Nominating Committee Director Removal Community Forum.

(v) The Director subject to the Nominating Committee Director Removal Supported Petition, ICANN and any Supporting Organization or Advisory Committee (including Decisional Participants) may deliver to the EC Administration in writing its views and questions on the Nominating Committee Director Removal Supported Petition prior to the convening of and during the Nominating Committee Director Removal Community Forum. Any written materials delivered to the EC Administration shall also be delivered to the Secretary for prompt posting on the Website in a manner deemed appropriate by ICANN.

(vi) The Director who is the subject of the Nominating Committee Director Removal Supported Petition and the Chair of the Board (or the Vice Chair of the Board if the Chair is the affected Director) are expected to attend the Nominating Committee Director Removal Community Forum in order to address the issues raised in the Nominating Committee Director Removal Supported Petition.

(vii) If the Nominating Committee Director Removal Petitioning Decisional Participant and each of the Nominating Committee Director Removal Supporting Decisional Participants for an applicable Nominating Committee Director Removal Supported Petition agree before, during or after the Nominating Committee Director Removal Community Forum that the issue

raised in such Nominating Committee Director Removal Supported Petition has been resolved, such Nominating Committee Director Removal Supported Petition shall be deemed withdrawn and the Nominating Committee Director Removal Process with respect to such Nominating Committee Director Removal Supported Petition will be terminated. If a Nominating Committee Director Removal Process is terminated, the EC Administration shall, within twenty-four (24) hours of the resolution of the issue raised in the Nominating Committee Director Removal Supported Petition, deliver to the Secretary a Nominating Committee Director Removal Process Termination Notice. For the avoidance of doubt, the Nominating Committee Director Removal Community Forum is not a decisional body and the foregoing resolution process shall be handled pursuant to the internal procedures of the Nominating Committee Director Removal Petitioning Decisional Participant and the Nominating Committee Director Removal Supporting Decisional Participant(s).

(viii) During the Nominating Committee Director Removal Community Forum Period, an additional one or two Nominating Committee Director Removal Community Forums may be held at the discretion of a Nominating Committee Director Removal Petitioning Decisional Participant and a related Nominating Committee Director Removal Supporting Decisional Participant, or the EC Administration.

(ix) ICANN will provide support services for the Nominating Committee Director Removal Community Forum and shall promptly post on the Website a public record of the Nominating Committee Director Removal Community Forum as well as all written submissions of the Director who is the subject of the Nominating Committee Director Removal Supported Petition, ICANN and any Supporting Organization or Advisory Committee (including Decisional Participants) related to the Nominating Committee Director Removal Community Forum.

(f) Following the expiration of the Nominating Committee Director Removal Community Forum Period, at any time or date prior to 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 21st day after the expiration of the Nominating Committee Director Removal Community Forum Period (such period, the "**Nominating Committee Director Removal Decision Period**"), each Decisional Participant shall inform the EC Administration in writing as to whether such Decisional Participant (i) supports such Nominating Committee Director Removal Supported Petition, (ii) objects to such Nominating Committee Director Removal Supported Petition or (iii) has determined to abstain from the matter (which shall not count as supporting or objecting to the Nominating

Committee Director Removal Supported Petition), and each Decisional Participant shall forward such notice to the Secretary for ICANN to promptly post on the Website. If a Decisional Participant does not inform the EC Administration of any of the foregoing prior to the expiration of the Nominating Committee Director Removal Decision Period, the Decisional Participant shall be deemed to have abstained from the matter (even if such Decisional Participant informs the EC Administration of its support or objection following the expiration of the Nominating Committee Director Removal Decision Period).

(g) The EC Administration shall, within twenty-four (24) hours of the expiration of the Nominating Committee Director Removal Decision Period, deliver a written notice ("**Nominating Committee Director Removal Notice**") to the Secretary certifying that, pursuant to and in compliance with the procedures and requirements of Section 3.1 of this Annex D, the EC has approved of the removal of the Director who is subject to the Nominating Committee Director Removal Process if the Nominating Committee Director Removal Supported Petition is (i) supported by three or more Decisional Participants and (ii) not objected to by more than one Decisional Participant.

(h) Upon the Secretary's receipt of a Nominating Committee Director Removal Notice, the Director subject to such Nominating Committee Director Removal Notice shall be effectively removed from office and shall no longer be a Director and such Director's vacancy shall be filled in accordance with Section 7.12 of the Bylaws.

(i) If the Nominating Committee Director Removal Supported Petition does not obtain the support required by Section 3.1(g) of this Annex D, the Nominating Committee Director Removal Process will automatically be terminated and the EC Administration shall, within twenty-four (24) hours of the expiration of the Nominating Committee Director Removal Decision Period, deliver to the Secretary a Nominating Committee Director Removal Process Termination Notice. The Director who was subject to the Nominating Committee Director Removal Process shall remain on the Board and not be subject to the Nominating Committee Director Removal Process for the remainder of the Director's current term.

(j) If neither a Nominating Committee Director Removal Notice nor a Nominating Committee Director Removal Process Termination Notice are received by the Secretary prior to 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 21st day after the expiration of the Nominating Committee Director Removal Community Forum Period, the Nominating Committee Director Removal Process shall automatically terminate and the Director who was subject to the Nominating Committee Director Removal Process shall remain on the Board and shall not be subject to the Nominating Committee Director Removal Process for the remainder of the Director's current term.

(k) Notwithstanding anything in this Section 3.1 to the contrary, if, for any reason, including due to resignation, death or disability, a Director who is the subject of a Nominating Committee Director Removal Process ceases to be a Director, the Nominating Committee Director Removal Process for such Director shall automatically terminate without any further action of ICANN or the EC Administration.

(l) ICANN shall promptly post to the Website any (i) Nominating Committee Director Removal Petition, (ii) Nominating Committee Director Removal Petition Notice, (iii) Nominating Committee Director Removal Supported Petition, (iv) Nominating Committee Director Removal Notice and the written explanation provided by the EC Administration as to why the EC has chosen to remove the relevant Director, (v) Nominating Committee Director Removal Process Termination Notice, and (vi) other notices the Secretary receives under this Section 3.1.

Section 3.2. SO/AC DIRECTOR REMOVAL PROCESS

(a) Subject to the procedures and requirements developed by the applicable Decisional Participant, an individual may submit a petition to the ASO, ccNSO, GNSO or At-Large Community (as applicable, the "**Applicable Decisional Participant**") seeking to remove a Director who was nominated by that Supporting Organization or the At-Large Community in accordance with Section 7.2(a) of the Bylaws, and initiate the SO/AC Director Removal Process ("**SO/AC Director Removal Petition**"). The process set forth in this Section 3.2 of this Annex D is referred to herein as the "**SO/AC Director Removal Process**."

(b) During the period beginning on the date that the Applicable Decisional Participant received the SO/AC Director Removal Petition (such date of receipt, the "**SO/AC Director Removal Petition Date**") and ending at 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the date that is the 21st day after the SO/AC Director Removal Petition Date (as it relates to a particular Director, the "**SO/AC Director Removal Petition Period**"), the Applicable Decisional Participant shall either accept or reject such SO/AC Director Removal Petition pursuant to the internal procedures of the Applicable Decisional Participant for the SO/AC Director Removal Petition; provided that the Applicable Decisional Participant shall not accept an SO/AC Director Removal Petition if, during the same term, the Director who is the subject of such SO/AC Director Removal Petition had previously been subject to an SO/AC Director Removal Petition that led to an SO/AC Director Removal Community Forum (as defined in Section 3.2(d) of this Annex D).

(c) During the SO/AC Director Removal Petition Period, the Applicable Decisional

Participant shall invite the Director subject to the SO/AC Director Removal Petition and the Chair of the Board (or the Vice Chair of the Board if the Chair is the affected Director) to a dialogue with the individual(s) bringing the SO/AC Director Removal Petition and the Applicable Decisional Participant's representative on the EC Administration. The SO/AC Director Removal Petition may not be accepted unless this invitation has been extended upon reasonable notice and accommodation to the affected Director's availability. If the invitation is accepted by either the Director who is the subject of the SO/AC Director Removal Petition or the Chair of the Board (or the Vice Chair of the Board if the Chair is the affected Director), the Applicable Decisional Participant shall not accept the SO/AC Director Removal Petition until the dialogue has occurred or there have been reasonable efforts to have the dialogue.

(i) If, in accordance with Section 3.2(b), the Applicable Decisional Participant accepts an SO/AC Director Removal Petition during the SO/AC Director Removal Petition Period, the Applicable Decisional Participant shall, within twenty-four (24) hours of the Applicable Decisional Participant's acceptance of the SO/AC Director Removal Petition, provide written notice ("**SO/AC Director Removal Petition Notice**") of such acceptance to the EC Administration, the other Decisional Participants and the Secretary. Such SO/AC Director Removal Petition Notice shall include:

(A) a supporting rationale in reasonable detail;

(B) contact information for at least one representative who has been designated by the Applicable Decisional Participant who shall act as a liaison with respect to the SO/AC Director Removal Petition Notice;

(C) a statement as to whether or not the Applicable Decisional Participant requests that ICANN organize a publicly-available conference call prior to the SO/AC Director Removal Community Forum (as defined in Section 3.2(d) of this Annex D) for the community to discuss the SO/AC Director Removal Petition; and

(D) a statement as to whether the Applicable Decisional Participant has determined to hold the SO/AC Director Removal Community Forum during the next scheduled ICANN public meeting.

The SO/AC Director Removal Process shall thereafter continue for such SO/AC Director Removal Petition pursuant to Section 3.2(d) of this Annex D.

(ii) If the EC Administration has not received an SO/AC Director Removal

Petition Notice pursuant to Section 3.2(c)(i) during the SO/AC Director Removal Petition Period, the SO/AC Director Removal Process shall automatically be terminated with respect to the applicable SO/AC Director Removal Petition and the EC Administration shall, within twenty-four (24) hours of the expiration of the SO/AC Director Removal Petition Period, deliver to the Secretary a notice certifying that the SO/AC Director Removal Process has been terminated with respect to the applicable SO/AC Director Removal Petition ("**SO/AC Director Removal Process Termination Notice**").

(d) If the EC Administration receives an SO/AC Director Removal Petition Notice under Section 3.2(c) of this Annex D during the SO/AC Director Removal Petition Period, ICANN shall, at the direction of the EC Administration, convene a forum at which the Decisional Participants and interested parties may discuss the SO/AC Director Removal Petition Notice ("**SO/AC Director Removal Community Forum**").

(i) If a publicly-available conference call has been requested in an SO/AC Director Removal Petition Notice, ICANN shall, at the direction of the EC Administration, schedule such call prior to any SO/AC Director Removal Community Forum, and inform the Decisional Participants of the date, time and participation methods of such conference call, which ICANN shall promptly post on the Website. The date and time of any such conference call shall be determined after consultation with the Director who is the subject of the SO/AC Director Removal Petition Notice regarding his or her availability.

(ii) The SO/AC Director Removal Community Forum shall be convened and concluded during the period beginning upon the expiration of the SO/AC Director Removal Petition Period and ending at 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 21st day after the expiration of the SO/AC Director Removal Petition Period ("**SO/AC Director Removal Community Forum Period**") unless the SO/AC Director Removal Petition Notice requested that the SO/AC Director Removal Community Forum be held during the next scheduled ICANN public meeting, in which case the SO/AC Director Removal Community Forum shall be held during the next scheduled ICANN public meeting on the date and at the time determined by ICANN, taking into account any date and/or time requested by the Applicable Decisional Participant; provided, that the date and time of any SO/AC Director Removal Community Forum shall be determined after consultation with the Director who is the subject of the

SO/AC Director Removal Petition Notice regarding his or her availability. If the SO/AC Director Removal Community Forum is held during the next scheduled ICANN public meeting and that public meeting is held after 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 21st day after the expiration of the SO/AC Director Removal Petition Period, the SO/AC Director Removal Community Forum Period shall expire at 11:59 p.m., local time of the city hosting such ICANN public meeting on the official last day of such ICANN public meeting.

(iii) The SO/AC Director Removal Community Forum shall be conducted via remote participation methods such as teleconference, web-based meeting room and/or such other form of remote participation as the EC Administration selects, and/or, only if the SO/AC Director Removal Community Forum is held during an ICANN public meeting, face-to-face meetings. If the SO/AC Director Removal Community Forum will not be held during an ICANN public meeting, the EC Administration shall promptly inform ICANN of the date, time and participation methods of the SO/AC Director Removal Community Forum, which ICANN shall promptly post on the Website.

(iv) The EC Administration shall manage and moderate the SO/AC Director Removal Community Forum in a fair and neutral manner; provided that no individual from the Applicable Decisional Participant, nor the individual who initiated the SO/AC Director Removal Petition, shall be permitted to participate in the management or moderation of the SO/AC Director Removal Community Forum.

(v) The Director subject to the SO/AC Director Removal Petition Notice, ICANN and any Supporting Organization or Advisory Committee (including Decisional Participants) may deliver to the EC Administration in writing its views and questions on the SO/AC Director Removal Petition Notice prior to the convening of and during the SO/AC Director Removal Community Forum. Any written materials delivered to the EC Administration shall also be delivered to the Secretary for prompt posting on the Website in a manner deemed appropriate by ICANN.

(vi) The Director who is the subject of the SO/AC Director Removal Petition Notice and the Chair of the Board (or the Vice Chair of the Board if the Chair is the affected Director) are expected to attend the SO/AC Director Removal Community Forum in order to address the issues raised in the SO/AC Director Removal Petition Notice.

(vii) If the Applicable Decisional Participant agrees before, during or after the SO/AC Director Removal Community Forum that the issue raised in

such SO/AC Director Removal Petition Notice has been resolved, such SO/AC Director Removal Petition Notice shall be deemed withdrawn and the SO/AC Director Removal Process with respect to such SO/AC Director Removal Petition Notice will be terminated. If an SO/AC Director Removal Process is terminated, the EC Administration shall, within twenty-four (24) hours of the resolution of the issue raised in the SO/AC Director Removal Petition Notice, deliver to the Secretary an SO/AC Director Removal Process Termination Notice. For the avoidance of doubt, the SO/AC Director Removal Community Forum is not a decisional body and the foregoing resolution process shall be handled pursuant to the internal procedures of the Applicable Decisional Participant.

(viii) During the SO/AC Director Removal Community Forum Period, an additional one or two SO/AC Director Removal Community Forums may be held at the discretion of the Applicable Decisional Participant or the EC Administration.

(ix) ICANN will provide support services for the SO/AC Director Removal Community Forum and shall promptly post on the Website a public record of the SO/AC Director Removal Community Forum as well as all written submissions of the Director who is the subject of the SO/AC Director Removal Petition Notice, ICANN and any Supporting Organization or Advisory Committee (including Decisional Participants) related to the SO/AC Director Removal Community Forum.

(e) Following the expiration of the SO/AC Director Removal Community Forum Period, ICANN shall, at the request of the EC Administration, issue a request for comments and recommendations from the community, which shall be delivered to the Secretary for prompt posting on the Website along with a means for comments and recommendations to be submitted to ICANN on behalf of the EC Administration. This comment period shall remain open until 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 7th day after the request for comments and recommendations was posted on the Website (the "**SO/AC Director Removal Comment Period**"). ICANN shall promptly post on the Website all comments and recommendations received by ICANN during the SO/AC Director Removal Comment Period.

(f) Following the expiration of the SO/AC Director Removal Comment Period, at any time or date prior to 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 21st day after the expiration of the SO/AC Director Removal Comment Period (such period, the "**SO/AC Director Removal Decision Period**"), the Applicable Decisional Participant shall inform the EC Administration

in writing as to whether the Applicable Decisional Participant has support for the SO/AC Director Removal Petition Notice within the Applicable Decisional Participant of a three-quarters majority as determined pursuant to the internal procedures of the Applicable Decisional Participant ("**SO/AC Director Removal Notice**"). The Applicable Decisional Participant shall, within twenty-four (24) hours of obtaining such support, deliver the SO/AC Director Removal Notice to the EC Administration, the other Decisional Participants and Secretary, and ICANN shall, at the direction of the Applicable Decisional Participant, concurrently post on the Website an explanation provided by the Applicable Decisional Participant as to why the Applicable Decisional Participant has chosen to remove the affected Director. Upon the Secretary's receipt of the SO/AC Director Removal Notice from the EC Administration, the Director subject to such SO/AC Director Removal Notice shall be effectively removed from office and shall no longer be a Director and such Director's vacancy shall be filled in accordance with Section 7.12 of the Bylaws.

(g) If the SO/AC Director Removal Petition Notice does not obtain the support required by Section 3.2(f) of this Annex D, the SO/AC Director Removal Process will automatically be terminated and the EC Administration shall, within twenty-four (24) hours of the failure to obtain such support, deliver to the Secretary an SO/AC Director Removal Process Termination Notice. The Director who was subject to the SO/AC Director Removal Process shall remain on the Board and shall not be subject to the SO/AC Director Removal Process for the remainder of the Director's current term.

(h) If neither an SO/AC Director Removal Notice nor an SO/AC Director Removal Process Termination Notice are received by the Secretary prior to the expiration of the SO/AC Director Removal Decision Period, the SO/AC Director Removal Process shall automatically terminate and the Director who was subject to the SO/AC Director Removal Process shall remain on the Board and shall not be subject to the SO/AC Director Removal Process for the remainder of the Director's current term.

(i) Notwithstanding anything in this Section 3.2 to the contrary, if, for any reason, including due to resignation, death or disability, a Director who is the subject of an SO/AC Director Removal Process ceases to be a Director, the SO/AC Director Removal Process for such Director shall automatically terminate without any further action of ICANN or the EC Administration.

(j) ICANN shall promptly post to the Website any (i) SO/AC Director Removal Petition, (ii) SO/AC Director Removal Petition Notice, (iii) SO/AC Director Removal Notice and the written explanation provided by the EC Administration as to why the EC has chosen to remove the relevant Director, (iv) SO/AC Director Removal Process Termination Notice, and (v) other notices the Secretary receives under

this Section 3.2.

Section 3.3. BOARD RECALL PROCESS

(a) Subject to the procedures and requirements developed by the applicable Decisional Participant, an individual may submit a petition to a Decisional Participant seeking to remove all Directors (other than the President) at the same time and initiate the Board Recall Process ("**Board Recall Petition**"), provided that a Board Recall Petition cannot be submitted solely on the basis of a matter decided by a Community IRP if (i) such Community IRP was initiated in connection with the Board's implementation of GAC Consensus Advice and (ii) the EC did not prevail in such Community IRP. Each Board Recall Petition shall include a rationale setting forth the reasons why such individual seeks to recall the Board. The process set forth in this Section 3.3 of this Annex D is referred to herein as the "**Board Recall Process**."

(b) A Decisional Participant that has received a Board Recall Petition shall either accept or reject such Board Recall Petition during the period beginning on the date the Decisional Participant received the Board Recall Petition ("**Board Recall Petition Date**") and ending at 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the date that is the 21st day after the Board Recall Petition Date (the "**Board Recall Petition Period**").

(i) If, in accordance with Section 3.3(b) of this Annex D, a Decisional Participant accepts a Board Recall Petition during the Board Recall Petition Period (such Decisional Participant, the "**Board Recall Petitioning Decisional Participant**"), the Board Recall Petitioning Decisional Participant shall, within twenty-four (24) hours of the expiration of its acceptance of the Board Recall Petition, provide written notice ("**Board Recall Petition Notice**") of such acceptance to the EC Administration, the other Decisional Participants and the Secretary. The Board Recall Petition Notice shall include the rationale upon which removal of the Board is sought. The Board Recall Process shall thereafter continue pursuant to Section 3.3(c) of this Annex D.

(ii) If the EC Administration has not received a Board Recall Petition Notice pursuant to Section 3.3(b)(i) of this Annex D during the Board Recall Petition Period, the Board Recall Process shall automatically be terminated with respect to the Board Recall Petition and the EC Administration shall, within twenty-four (24) hours of the expiration of the Board Recall Petition Period, deliver to the Secretary a notice certifying that the Board Recall Process has been terminated with respect to the Board Recall Petition

("**Board Recall Process Termination Notice**").

(c) Following the delivery of a Board Recall Petition Notice to the EC Administration by a Board Recall Petitioning Decisional Participant pursuant to Section 3.3(b)(i) of this Annex D, the Board Recall Petitioning Decisional Participant shall contact the EC Administration and the other Decisional Participants to determine whether any other Decisional Participants support the Board Recall Petition. The Board Recall Petitioning Decisional Participant shall forward such communication to the Secretary for ICANN to promptly post on the Website.

(i) If the Board Recall Petitioning Decisional Participant obtains the support of at least two other Decisional Participants (each, a "**Board Recall Supporting Decisional Participant**") during the period beginning upon the expiration of the Board Recall Petition Period and ending at 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 7th day after the expiration of the Board Recall Petition Period (the "**Board Recall Petition Support Period**"), the Board Recall Petitioning Decisional Participant shall provide a written notice to the EC Administration, the other Decisional Participants and the Secretary ("**Board Recall Supported Petition**") within twenty-four hours of receiving the support of at least two Board Recall Supporting Decisional Participants. Each Board Recall Supporting Decisional Participant shall provide a written notice to the EC Administration, the other Decisional Participants and the Secretary within twenty-four (24) hours of providing support to the Board Recall Petition. Such Board Recall Supported Petition shall include:

(A) a supporting rationale in reasonable detail;

(B) contact information for at least one representative who has been designated by the Board Recall Petitioning Decisional Participant who shall act as a liaison with respect to the Board Recall Supported Petition;

(C) a statement as to whether or not the Board Recall Petitioning Decisional Participant and/or the Board Recall Supporting Decisional Participants requests that ICANN organize a publicly-available conference call prior to the Board Recall Community Forum (as defined in Section 3.3(d) of this Annex D) for the community to discuss the Board Recall Supported Petition; and

(D) a statement as to whether the Board Recall Petitioning Decisional

Participant and the Board Recall Supporting Decisional Participants have determined to hold the Board Recall Community Forum during the next scheduled ICANN public meeting.

The Board Recall Process shall thereafter continue for such Board Recall Supported Petition pursuant to Section 3.3(d) of this Annex D.

(ii) The Board Recall Process shall automatically be terminated and the EC Administration shall, within twenty-four (24) hours of the expiration of the Board Recall Petition Support Period, deliver to the Secretary a Board Recall Process Termination Notice if the Board Recall Petitioning Decisional Participant is unable to obtain the support of at least two other Decisional Participants for its Board Recall Petition during the Board Recall Petition Support Period.

(d) If the EC Administration receives a Board Recall Supported Petition under Section 3.3(c) of this Annex D during the Board Recall Petition Support Period, ICANN shall, at the direction of the EC Administration, convene a forum at which the Decisional Participants and interested parties may discuss the Board Recall Supported Petition ("**Board Recall Community Forum**").

(i) If a publicly-available conference call has been requested in a Board Recall Supported Petition, ICANN shall, at the direction of the EC Administration, schedule such call prior to any Board Recall Community Forum, and inform the Decisional Participants of the date, time and participation methods of such conference call, which ICANN shall promptly post on the Website. The date and time of any such conference call shall be determined after consultation with the Board regarding the availability of the Directors.

(ii) The Board Recall Community Forum shall be convened and concluded during the period beginning upon the expiration of the Board Recall Petition Support Period and ending at 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 21st day after the expiration of the Board Recall Petition Support Period ("**Board Recall Community Forum Period**") unless the Board Recall Supported Petition requested that the Board Recall Community Forum be held during the next scheduled ICANN public meeting, in which case the Board Recall Community Forum shall be held during the next scheduled ICANN public meeting on the date and at the time determined by ICANN, taking into account any date and/or time requested by the Board Recall Petitioning Decisional Participant and

the Board Recall Supporting Decisional Participants; provided, that, the date and time of any Board Recall Community Forum shall be determined after consultation with the Board regarding the availability of the Directors. If the Board Recall Community Forum is held during the next scheduled ICANN public meeting and that public meeting is held after 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 21st day after the expiration of the Board Recall Petition Support Period, the Board Recall Community Forum Period shall expire at 11:59 p.m., local time of the city hosting such ICANN public meeting on the official last day of such ICANN public meeting.

(iii) The Board Recall Community Forum shall have at least one face-to-face meeting and may also be conducted via remote participation methods such as teleconference, web-based meeting room and/or such other form of remote participation as the EC Administration selects. If the Board Recall Community Forum will not be held during an ICANN public meeting, the EC Administration shall promptly inform ICANN of the date, time and participation methods of the Board Recall Community Forum, which ICANN shall promptly post on the Website.

(iv) The EC Administration shall manage and moderate the Board Recall Community Forum in a fair and neutral manner; provided that no individual from the Board Recall Petitioning Decisional Participant or a Board Recall Supporting Decisional Participant, nor the individual who initiated the Board Recall Petition, shall be permitted to participate in the management or moderation of the Board Recall Community Forum.

(v) ICANN and any Supporting Organization or Advisory Committee (including Decisional Participants) may deliver to the EC Administration in writing its views and questions on the Board Recall Supported Petition prior to the convening of and during the Board Recall Community Forum. Any written materials delivered to the EC Administration shall also be delivered to the Secretary for prompt posting on the Website in a manner deemed appropriate by ICANN.

(vi) ICANN staff and the full Board are expected to attend the Board Recall Community Forum in order to address the issues raised in the Board Recall Supported Petition.

(vii) If the Board Recall Petitioning Decisional Participant and each of the Board Recall Supporting Decisional Participants for the Board Recall Supported Petition agree before, during or after the Board Recall Community Forum that the issue raised in such Board Recall Supported Petition has been resolved, such Board Recall Supported Petition shall be

deemed withdrawn and the Board Recall Process with respect to such Board Recall Supported Petition will be terminated. If a Board Recall Process is terminated, the EC Administration shall, within twenty-four (24) hours of the resolution of the issue raised in the Board Recall Supported Petition, deliver to the Secretary a Board Recall Process Termination Notice. For the avoidance of doubt, the Board Recall Community Forum is not a decisional body and the foregoing resolution process shall be handled pursuant to the internal procedures of the Board Recall Petitioning Decisional Participant and the Board Recall Supporting Decisional Participants.

(viii) During the Board Recall Community Forum Period, an additional one or two Board Recall Community Forums may be held at the discretion of the Board Recall Petitioning Decisional Participant and the Board Recall Supporting Decisional Participants, or the EC Administration.

(ix) ICANN will provide support services for the Board Recall Community Forum and shall promptly post on the Website a public record of the Board Recall Community Forum as well as all written submissions of ICANN and any Supporting Organization or Advisory Committee (including Decisional Participants) related to the Board Recall Community Forum.

(e) Following the expiration of the Board Recall Community Forum Period, at any time or date prior to 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 21st day after the expiration of the Board Recall Community Forum Period (such period, the "**Board Recall Decision Period**"), each Decisional Participant shall inform the EC Administration in writing as to whether such Decisional Participant (i) supports such Board Recall Supported Petition, (ii) objects to such Board Recall Supported Petition or (iii) has determined to abstain from the matter (which shall not count as supporting or objecting to such Board Recall Supported Petition), and each Decisional Participant shall forward such notice to the Secretary for ICANN to promptly post on the Website. If a Decisional Participant does not inform the EC Administration of any of the foregoing prior to expiration of the Board Recall Decision Period, the Decisional Participant shall be deemed to have abstained from the matter (even if such Decisional Participant informs the EC Administration of its support or objection following the expiration of the Board Recall Decision Period).

(f) The EC Administration shall, within twenty-four (24) hours of the expiration of the Board Recall Decision Period, deliver a written notice ("**EC Board Recall Notice**") to the Secretary certifying that, pursuant to and in compliance with the procedures and requirements of this Section 3.3 of this Annex D, the EC has

resolved to remove all Directors (other than the President) if (after accounting for any adjustments to the below as required by the GAC Carve-out pursuant to Section 3.6(e) of the Bylaws if an IRP Panel found that, in implementing GAC Consensus Advice, the Board acted inconsistently with the Articles or Bylaws) a Board Recall Supported Petition (i) is supported by four or more Decisional Participants, and (ii) is not objected to by more than one Decisional Participant.

(g) Upon the Secretary's receipt of an EC Board Recall Notice, all Directors (other than the President) shall be effectively removed from office and shall no longer be Directors and such vacancies shall be filled in accordance with Section 7.12 of the Bylaws.

(h) If the Board Recall Supported Petition does not obtain the support required by Section 3.3(f) of this Annex D, the Board Recall Process will automatically be terminated and the EC Administration shall, within twenty-four (24) hours of the expiration of the Board Recall Decision Period, deliver to the Secretary a Board Recall Process Termination Notice. All Directors shall remain on the Board.

(i) If neither an EC Board Recall Notice nor a Board Recall Process Termination Notice are received by the Secretary prior to the expiration of the Board Recall Decision Period, the Board Recall Process shall automatically terminate and all Directors shall remain on the Board.

(j) ICANN shall promptly post to the Website any (i) Board Recall Petition, (ii) Board Recall Petition Notice, (iii) Board Recall Supported Petition, (iv) EC Board Recall Notice and the written explanation provided by the EC Administration as to why the EC has chosen to recall the Board, (v) Board Recall Process Termination Notice, and (vi) other notices the Secretary receives under this Section 3.3.

Article 4 PROCEDURE FOR EXERCISE OF EC'S RIGHTS TO INITIATE MEDIATION, A COMMUNITY IRP OR RECONSIDERATION REQUEST

Section 4.1. MEDIATION INITIATION

(a) If the Board refuses or fails to comply with a decision by the EC delivered to the Secretary pursuant to an EC Approval Notice, EC Rejection Notice, Nominating Committee Director Removal Notice, SO/AC Director Removal Notice or EC Board Recall Notice pursuant to and in compliance with Article 1, Article 2 or Article 3 of this Annex D, or rejects or otherwise does not take action that is consistent with a final IFR Recommendation, Special IFR Recommendation, SCWG Creation Recommendation or SCWG Recommendation, as applicable (each, an "**EC Decision**"), the EC Administration representative of any Decisional Participant who supported the exercise by the EC of its rights in the applicable EC

Decision during the applicable decision period may request that the EC initiate mediation with the Board in relation to that EC Decision as contemplated by Section 4.7 of the Bylaws, by delivering a notice to the EC Administration, the Decisional Participants and the Secretary requesting the initiation of a mediation ("**Mediation Initiation Notice**"). ICANN shall promptly post to the Website any Mediation Initiation Notice.

(b) As soon as practicable after receiving a Mediation Initiation Notice, the EC Administration and the Secretary shall initiate mediation, which shall proceed in accordance with Section 4.7 of the Bylaws.

Section 4.2. COMMUNITY IRP

(a) After completion of a mediation under Section 4.7 of the Bylaws, the EC Administration representative of any Decisional Participant who supported the exercise by the EC of its rights in the applicable EC Decision during the applicable decision period may request that the EC initiate a Community IRP (a "**Community IRP Petitioning Decisional Participant**"), as contemplated by Section 4.3 of the Bylaws, by delivering a notice to the EC Administration and the Decisional Participants requesting the initiation of a Community IRP ("**Community IRP Petition**"). The Community IRP Petitioning Decisional Participant shall forward such notice to the Secretary for ICANN to promptly post on the Website. The process set forth in this Section 4.2 of this Annex D as it relates to a particular Community IRP Petition is referred to herein as the "**Community IRP Initiation Process**."

(b) Following the delivery of a Community IRP Petition to the EC Administration by a Community IRP Petitioning Decisional Participant pursuant to Section 4.2(a) of this Annex D (which delivery date shall be referred to herein as the "**Community IRP Notification Date**"), the Community IRP Petitioning Decisional Participant shall contact the EC Administration and the other Decisional Participants to determine whether any other Decisional Participants support the Community IRP Petition. The Community IRP Petitioning Decisional Participant shall forward such communication to the Secretary for ICANN to promptly post on the Website.

> (i) If the Community IRP Petitioning Decisional Participant obtains the support of at least one other Decisional Participant (a "**Community IRP Supporting Decisional Participant**") during the period beginning on the Community IRP Notification Date and ending at 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 21st day after the Community IRP Notification Date (the "**Community IRP Petition Support Period**"), the Community IRP Petitioning Decisional Participant

shall provide a written notice to the EC Administration, the other Decisional Participants and the Secretary ("**Community IRP Supported Petition**") within twenty-four (24) hours of receiving the support of at least one Community IRP Supporting Decisional Participant. Each Community IRP Supporting Decisional Participant shall provide a written notice to the EC Administration, the other Decisional Participants and the Secretary within twenty-four (24) hours of providing support to the Community IRP Petition. Such Community IRP Supported Petition shall include:

(A) a supporting rationale in reasonable detail;

(B) contact information for at least one representative who has been designated by the Community IRP Petitioning Decisional Participant who shall act as a liaison with respect to the Community IRP Supported Petition;

(C) a statement as to whether or not the Community IRP Petitioning Decisional Participant and/or the Community IRP Supporting Decisional Participant requests that ICANN organize a publicly-available conference call prior to the Community IRP Community Forum (as defined in Section 4.2(c) of this Annex D) for the community to discuss the Community IRP Supported Petition;

(D) a statement as to whether the Community IRP Petitioning Decisional Participant and the Community IRP Supporting Decisional Participant have determined to hold the Community IRP Community Forum during the next scheduled ICANN public meeting;

(E) where the Community IRP Supported Petition relates to a Fundamental Bylaw Amendment, a PDP Fundamental Bylaw Statement if applicable and, if so, the name of the Fundamental Bylaw Amendment PDP Decisional Participant;

(F)where the Community IRP Supported Petition relates to an Articles Amendment, a PDP Articles Statement if applicable and, if so, the name of the Articles Amendment PDP Decisional Participant;

(G)where the Community IRP Supported Petition relates to a Standard Bylaw Amendment, a PDP Standard Bylaw Statement if applicable and, if so, the name of the Standard Bylaw Amendment PDP Decisional Participant; and

(H) where the Community IRP Supported Petition relates to a policy recommendation of a cross community working group chartered by more than one Supporting Organization ("**CCWG Policy Recommendation**"), a

statement citing the specific CCWG Policy Recommendation and related provision in the Community IRP Supported Petition ("**CCWG Policy Recommendation Statement**"), and, if so, the name of any Supporting Organization that is a Decisional Participant that approved the CCWG Policy Recommendation ("**CCWG Policy Recommendation Decisional Participant**").

The Community IRP Initiation Process shall thereafter continue for such Community IRP Supported Petition pursuant to Section 4.2(c) of this Annex D.

(ii) The Community IRP Initiation Process shall automatically be terminated and the EC Administration shall, within twenty-four (24) hours of the expiration of the Community IRP Petition Support Period, deliver to the Secretary a notice certifying that the Community IRP Initiation Process has been terminated with respect to the Community IRP included in the Community IRP Petition ("**Community IRP Termination Notice**") if:

(A) no Community IRP Petitioning Decisional Participant is able to obtain the support of at least one other Decisional Participant for its Community IRP Petition during the Community IRP Petition Support Period;

(B) where the Community IRP Supported Petition includes a PDP Fundamental Bylaw Statement, the Fundamental Bylaw Amendment PDP Decisional Participant is not (x) the Community IRP Petitioning Decisional Participant or (y) one of the Community IRP Supporting Decisional Participants;

(C)where the Community IRP Supported Petition includes a PDP Articles Statement, the Articles Amendment PDP Decisional Participant is not (x) the Community IRP Petitioning Decisional Participant or (y) one of the Community IRP Supporting Decisional Participants;

(D)where the Community IRP Supported Petition includes a PDP Standard Bylaw Statement, the Standard Bylaw Amendment PDP Decisional Participant is not (x) the Community IRP Petitioning Decisional Participant or (y) one of the Community IRP Supporting Decisional Participants; or

(E) where the Community IRP Supported Petition includes a CCWG Policy Recommendation Statement, the CCWG Policy Recommendation Decisional Participant is not (x) the Community IRP Petitioning Decisional Participant or (y) one of the Community IRP Supporting Decisional Participants.

(c) If the EC Administration receives a Community IRP Supported Petition under Section 4.2(b) of this Annex D during the Community IRP Petition Support Period, ICANN shall, at the direction of the EC Administration, convene a forum at which the Decisional Participants and interested third parties may discuss the Community IRP Supported Petition ("**Community IRP Community Forum**").

(i) If a publicly-available conference call has been requested in a Community IRP Supported Petition, ICANN shall, at the direction of the EC Administration, schedule such call prior to any Community IRP Community Forum, and inform the Decisional Participants of the date, time and participation methods of such conference call, which ICANN shall promptly post on the Website.

(ii) The Community IRP Community Forum shall be convened and concluded during the period beginning on the expiration of the Community IRP Petition Support Period and ending at 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 30th day after the expiration of the Community IRP Petition Support Period ("**Community IRP Community Forum Period**") unless the Community IRP Supported Petition requested that the Community IRP Community Forum be held during the next scheduled ICANN public meeting, in which case the Community IRP Community Forum shall be held during the next scheduled ICANN public meeting on the date and at the time determined by ICANN, taking into account any date and/or time requested by the Community IRP Petitioning Decisional Participant and the Community IRP Supporting Decisional Participant(s). If the Community IRP Community Forum is held during the next scheduled ICANN public meeting and that public meeting is held after 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 30th day after the expiration of the Community IRP Petition Support Period, the Community IRP Community Forum Period shall expire at 11:59 p.m., local time of the city hosting such ICANN public meeting on the official last day of such ICANN public meeting.

(iii) The Community IRP Community Forum shall be conducted via remote participation methods such as teleconference, web-based meeting room and/or such other form of remote participation as the EC Administration selects and/or, only if the Community IRP Community Forum is held during an ICANN public meeting, face-to-face meetings. If the Community IRP Community Forum will not be held during an ICANN public meeting, the EC Administration shall promptly inform ICANN of the date, time and participation methods of such Community IRP Community Forum, which

ICANN shall promptly post on the Website.

(iv) The EC Administration shall manage and moderate the Community IRP Community Forum in a fair and neutral manner.

(v) ICANN and any Supporting Organization or Advisory Committee (including Decisional Participants) may deliver to the EC Administration in writing its views and questions on the Community IRP Supported Petition prior to the convening of and during the Community IRP Community Forum. Any written materials delivered to the EC Administration shall also be delivered to the Secretary for prompt posting on the Website in a manner deemed appropriate by ICANN.

(vi) ICANN staff and Directors representing the Board are expected to attend the Community IRP Community Forum in order to discuss the Community IRP Supported Petition.

(vii) If the Community IRP Petitioning Decisional Participant and each of the Community IRP Supporting Decisional Participants for the Community IRP Supported Petition agree before, during or after a Community IRP Community Forum that the issue raised in such Community IRP Supported Petition has been resolved, such Community IRP Supported Petition shall be deemed withdrawn and the Community IRP Initiation Process with respect to such Community IRP Supported Petition will be terminated. If a Community IRP Initiation Process is terminated, the EC Administration shall, within twenty-four (24) hours of the resolution of the issue raised in the Community IRP Supported Petition, deliver to the Secretary a Community IRP Termination Notice. For the avoidance of doubt, the Community IRP Community Forum is not a decisional body and the foregoing resolution process shall be handled pursuant to the internal procedures of the Community IRP Petitioning Decisional Participant and the Community IRP Supporting Decisional Participant(s).

(viii) During the Community IRP Community Forum Period, an additional one or two Community IRP Community Forums may be held at the discretion of a Community IRP Petitioning Decisional Participant and a related Community IRP Supporting Decisional Participant, or the EC Administration.

(ix) ICANN will provide support services for the Community IRP Community Forum and shall promptly post on the Website a public record of the Community IRP Community Forum as well as all written submissions of ICANN and any Supporting Organization or Advisory Committee (including Decisional Participants) related to the Community IRP Community Forum.

(d) Following the expiration of the Community IRP Community Forum Period, at any time or date prior to 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 21st day after the expiration of the Community IRP Community Forum Period (such period, the "**Community IRP Decision Period**"), each Decisional Participant shall inform the EC Administration in writing as to whether such Decisional Participant (i) supports such Community IRP Supported Petition, (ii) objects to such Community IRP Supported Petition or (iii) has determined to abstain from the matter (which shall not count as supporting or objecting to the Community IRP Supported Petition), and each Decisional Participant shall forward such notice to the Secretary for ICANN to promptly post on the Website. If a Decisional Participant does not inform the EC Administration of any of the foregoing prior to the expiration of the Community IRP Decision Period, the Decisional Participant shall be deemed to have abstained from the matter (even if such Decisional Participant informs the EC Administration of its support or objection following the expiration of the Community IRP Decision Period).

(e) The EC Administration, within twenty-four (24) hours of the expiration of the Community IRP Decision Period, shall promptly deliver a written notice ("**EC Community IRP Initiation Notice**") to the Secretary certifying that, pursuant to and in compliance with the procedures and requirements of this Section 4.2 of this Annex D, the EC has resolved to accept the Community IRP Supported Petition if:

(i) A Community IRP Supported Petition that does not include a PDP Fundamental Bylaw Statement, a PDP Articles Statement, a PDP Standard Bylaw Statement or a CCWG Policy Recommendation Statement (A) is supported by three or more Decisional Participants, and (B) is not objected to by more than one Decisional Participant;

(ii) A Community IRP Supported Petition that (A) includes a PDP Fundamental Bylaw Statement, (B) is supported by three or more Decisional Participants (including the Fundamental Bylaw Amendment PDP Decisional Participant), and (C) is not objected to by more than one Decisional Participant;

(iii) A Community IRP Supported Petition that (A) includes a PDP Articles Statement, (B) is supported by three or more Decisional Participants (including the Articles Amendment PDP Decisional Participant), and (C) is not objected to by more than one Decisional Participant;

(iv) A Community IRP Supported Petition that (A) includes a PDP Standard Bylaw Statement, (B) is supported by three or more Decisional Participants (including the Standard Bylaw Amendment PDP Decisional Participant), and (C) is not objected to by more than one Decisional Participant; or

(v) A Community IRP Supported Petition that (A) includes a CCWG Policy Recommendation Statement, (B) is supported by three or more Decisional Participants (including the CCWG Policy Recommendation Decisional Participant), and (C) is not objected to by more than one Decisional Participant.

(f) If the Community IRP Supported Petition does not obtain the support required by Section 4.2(e) of this Annex D, the Community IRP Initiation Process will automatically be terminated and the EC Administration shall, within twenty-four (24) hours of the expiration of the Community IRP Decision Period, deliver to the Secretary a Community IRP Termination Notice.

(g) ICANN shall promptly post to the Website any (i) Community IRP Petition, (ii) Community IRP Supported Petition, (iii) EC Community IRP Initiation Notice, (iv) Community IRP Termination Notice, (v) written explanation provided by the EC Administration related to any of the foregoing, and (vi) other notices the Secretary receives under this Section 4.2.

Section 4.3. COMMUNITY RECONSIDERATION REQUEST

(a) Any Decisional Participant may request that the EC initiate a Reconsideration Request (a "**Community Reconsideration Petitioning Decisional Participant**"), as contemplated by Section 4.2(b) of the Bylaws, by delivering a notice to the EC Administration and the other Decisional Participants, with a copy to the Secretary for ICANN to promptly post on the Website, requesting the review or reconsideration of an action or inaction of the ICANN Board or staff ("**Community Reconsideration Petition**"). A Community Reconsideration Petition must be delivered within 30 days after the occurrence of any of the conditions set forth in Section 4.2(g)(i)(A), (B) or (C) of the Bylaws. In that instance, the Community Reconsideration Petition must be delivered within 30 days from the initial posting of the rationale. The process set forth in this Section 4.3 of this Annex D as it relates to a particular Community Reconsideration Petition is referred to herein as the "**Community Reconsideration Initiation Process**."

(b) Following the delivery of a Community Reconsideration Petition to the EC Administration by a Community Reconsideration Petitioning Decisional Participant pursuant to Section 4.3(a) of this Annex D (which delivery date shall be referred to herein as the "**Community Reconsideration Notification Date**"), the Community

Reconsideration Petitioning Decisional Participant shall contact the EC Administration and the other Decisional Participants to determine whether any other Decisional Participants support the Community Reconsideration Petition. The Community Reconsideration Petitioning Decisional Participant shall forward such communication to the Secretary for ICANN to promptly post on the Website.

(i) If the Community Reconsideration Petitioning Decisional Participant obtains the support of at least one other Decisional Participant (a "**Community Reconsideration Supporting Decisional Participant**") during the period beginning on the Community Reconsideration Notification Date and ending at 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 21st day after the Community Reconsideration Notification Date (the "**Community Reconsideration Petition Support Period**"), the Community Reconsideration Petitioning Decisional Participant shall provide a written notice to the EC Administration, the other Decisional Participants and the Secretary ("**Community Reconsideration Supported Petition**") within twenty-four (24) hours of receiving the support of at least one Community Reconsideration Supporting Decisional Participant. Each Community Reconsideration Supporting Decisional Participant shall provide a written notice to the EC Administration, the other Decisional Participants and the Secretary within twenty-four (24) hours of providing support to the Community Reconsideration Petition. Such Community Reconsideration Supported Petition shall include:

(A) a supporting rationale in reasonable detail;

(B) contact information for at least one representative who has been designated by the Community Reconsideration Petitioning Decisional Participant who shall act as a liaison with respect to the Community Reconsideration Supported Petition;

(C) a statement as to whether or not the Community Reconsideration Petitioning Decisional Participant and/or the Community Reconsideration Supporting Decisional Participant requests that ICANN organize a publicly-available conference call prior to the Community Reconsideration Community Forum (as defined in Section 4.3(c) of this Annex D) for the community to discuss the Community Reconsideration Supported Petition; and

(D) a statement as to whether the Community Reconsideration Petitioning Decisional Participant and the Community Reconsideration Supporting

Decisional Participant have determined to hold the Community Reconsideration Community Forum during the next scheduled ICANN public meeting.

The Community Reconsideration Initiation Process shall thereafter continue for such Community Reconsideration Supported Petition pursuant to Section 4.3(c) of this Annex D.

(ii) The Community Reconsideration Initiation Process shall automatically be terminated and the EC Administration shall, within twenty-four (24) hours of the expiration of the Community Reconsideration Petition Support Period, deliver to the Secretary a notice certifying that the Community Reconsideration Initiation Process has been terminated with respect to the Reconsideration Request included in the Community Reconsideration Petition ("**Community Reconsideration Termination Notice**") if the Community Reconsideration Petitioning Decisional Participant is unable to obtain the support of at least one other Decisional Participant for its Community Reconsideration Petition during the Community Reconsideration Petition Support Period.

(c) If the EC Administration receives a Community Reconsideration Supported Petition under Section 4.3(b) of this Annex D during the Community Reconsideration Petition Support Period, ICANN shall, at the direction of the EC Administration, convene a forum at which the Decisional Participants and interested third parties may discuss the Community Reconsideration Supported Petition ("**Community Reconsideration Community Forum**").

(i) If a publicly-available conference call has been requested in a Community Reconsideration Supported Petition, ICANN shall, at the direction of the EC Administration, schedule such call prior to any Community Reconsideration Community Forum, and inform the Decisional Participants of the date, time and participation methods of such conference call, which ICANN shall promptly post on the Website.

(ii) The Community Reconsideration Community Forum shall be convened and concluded during the period beginning on the expiration of the Community Reconsideration Petition Support Period and ending at 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 30th day after the expiration of the Community Reconsideration Petition Support Period ("**Community Reconsideration Forum Period**") unless the Community Reconsideration Supported Petition requested that

the Community Reconsideration Community Forum be held during the next scheduled ICANN public meeting, in which case the Community Reconsideration Community Forum shall be held during the next scheduled ICANN public meeting on the date and at the time determined by ICANN, taking into account any date and/or time requested by the Community Reconsideration Petitioning Decisional Participant and the Community Reconsideration Supporting Decisional Participant(s). If the Community Reconsideration Community Forum is held during the next scheduled ICANN public meeting and that public meeting is held after 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 30th day after the expiration of the Community Reconsideration Petition Support Period, the Community Reconsideration Community Forum Period shall expire at 11:59 p.m., local time of the city hosting such ICANN public meeting on the official last day of such ICANN public meeting.

(iii) The Community Reconsideration Community Forum shall be conducted via remote participation methods such as teleconference, web-based meeting room and/or such other form of remote participation as the EC Administration selects and/or, only if the Community Reconsideration Community Forum is held during an ICANN public meeting, face-to-face meetings. If the Community Reconsideration Community Forum will not be held during an ICANN public meeting, the EC Administration shall promptly inform ICANN of the date, time and participation methods of such Community Reconsideration Community Forum, which ICANN shall promptly post on the Website.

(iv) The EC Administration shall manage and moderate the Community Reconsideration Community Forum in a fair and neutral manner.

(v) ICANN and any Supporting Organization or Advisory Committee (including Decisional Participants) may deliver to the EC Administration in writing its views and questions on the Community Reconsideration Supported Petition prior to the convening of and during the Community Reconsideration Community Forum. Any written materials delivered to the EC Administration shall also be delivered to the Secretary for prompt posting on the Website in a manner deemed appropriate by ICANN.

(vi) ICANN staff and Directors representing the Board are expected to attend the Community Reconsideration Community Forum in order to discuss the Community Reconsideration Supported Petition.

(vii) If the Community Reconsideration Petitioning Decisional Participant and each of the Community Reconsideration Supporting Decisional Participants for a Community Reconsideration Supported Petition agree

before, during or after the Community Reconsideration Community Forum that the issue raised in such Community Reconsideration Supported Petition has been resolved, such Community Reconsideration Supported Petition shall be deemed withdrawn and the Community Reconsideration Initiation Process with respect to such Community Reconsideration Supported Petition will be terminated. If a Community Reconsideration Initiation Process is terminated, the EC Administration shall, within twenty-four (24) hours of the resolution of the issue raised in the Community Reconsideration Supported Petition, deliver to the Secretary a Community Reconsideration Termination Notice. For the avoidance of doubt, the Community Reconsideration Community Forum is not a decisional body and the foregoing resolution process shall be handled pursuant to the internal procedures of the Community Reconsideration Petitioning Decisional Participant and the Community Reconsideration Supporting Decisional Participant(s).

(viii) During the Community Reconsideration Community Forum Period, an additional one or two Community Reconsideration Community Forums may be held at the discretion of a Community Reconsideration Petitioning Decisional Participant and a related Community Reconsideration Supporting Decisional Participant, or the EC Administration.

(ix) ICANN will provide support services for the Community Reconsideration Community Forum and shall promptly post on the Website a public record of the Community Reconsideration Community Forum as well as all written submissions of ICANN and any Supporting Organization or Advisory Committee (including Decisional Participants) related to the Community Reconsideration Community Forum.

(d) Following the expiration of the Community Reconsideration Community Forum Period, at any time or date prior to 11:59 p.m. (as calculated by local time at the location of ICANN's principal office) on the 21st day after the expiration of the Community Reconsideration Community Forum Period (such period, the "**Community Reconsideration Decision Period**"), each Decisional Participant shall inform the EC Administration in writing as to whether such Decisional Participant (i) supports such Community Reconsideration Supported Petition, (ii) objects to such Community Reconsideration Supported Petition or (iii) has determined to abstain from the matter (which shall not count as supporting or objecting to the Community Reconsideration Supported Petition), and each Decisional Participant shall forward such notice to the Secretary for ICANN to promptly post on the Website. If a Decisional Participant does not inform the EC Administration of any of the foregoing prior to the expiration of the Community

Reconsideration Decision Period, the Decisional Participant shall be deemed to have abstained from the matter (even if such Decisional Participant informs the EC Administration of its support or objection following the expiration of the Community Reconsideration Decision Period).

(e) If (i) three or more Decisional Participants support the Community Reconsideration Supported Petition and (ii) no more than one Decisional Participant objects to the Community Reconsideration Supported Petition, then the EC Administration shall, within twenty-four (24) hours of the expiration of the Community Reconsideration Decision Period, deliver a notice to the Secretary certifying that, pursuant to and in compliance with the procedures and requirements of this Section 4.3 of this Annex D, the EC has resolved to accept the Community Reconsideration Supported Petition ("**EC Reconsideration Initiation Notice**"). The Reconsideration Request shall then proceed in accordance with Section 4.2 of the Bylaws.

(f) If the Community Reconsideration Supported Petition does not obtain the support required by Section 4.3(e) of this Annex D, the Community Reconsideration Initiation Process will automatically be terminated and the EC Administration shall, within twenty-four (24) hours of the expiration of the Community Reconsideration Decision Period, deliver to the Secretary a Community Reconsideration Termination Notice.

(g) ICANN shall promptly post to the Website any (i) Community Reconsideration Petition, (ii) Community Reconsideration Supported Petition, (iii) EC Reconsideration Initiation Notice, (iv) Community Reconsideration Termination Notice, (v) written explanation provided by the EC Administration related to any of the foregoing, and (vi) other notices the Secretary receives under this Section 4.3.

Annex E: Caretaker ICANN Budget Principles

1. Principles

The caretaker ICANN budget (the "**Caretaker ICANN Budget**") is defined as an annual operating plan and budget that is established by the CFO in accordance with the following principles (the "**Caretaker ICANN Budget Principles**"):

a. It is based on then-current ICANN operations;

b. It allows ICANN to "take good care" and not expose itself to additional enterprise risk(s) as a result of the rejection of an ICANN Budget by the EC pursuant to the Bylaws;

c. It allows ICANN to react to emergency situations in a fashion that

preserves the continuation of its operations;

d. It allows ICANN to abide by its existing obligations (including Articles of Incorporation, Bylaws, and contracts, as well as those imposed under law);

e. It enables ICANN to avoid waste of its resources during the rejection period (i.e., the period between when an ICANN Budget is rejected by the EC pursuant to the Bylaws and when an ICANN Budget becomes effective in accordance with the Bylaws) or immediately thereafter, by being able to continue activities during the rejection period that would otherwise need to be restarted at a materially incremental cost; and

f. Notwithstanding any other principle listed above, it prevents ICANN from initiating activities that remains subject to community consideration (or for which that community consideration has not concluded) with respect to the applicable ICANN Budget, including without limitation, preventing implementation of any expenditure or undertaking any action that was the subject of the ICANN Budget that was rejected by the EC that triggered the need for the Caretaker ICANN Budget.

1. Examples

Below is a non-exhaustive list of examples, to assist with the interpretation of the Caretaker ICANN Budget Principles, of what a Caretaker ICANN Budget would logically include:

i. the functioning of the EC, the Decisional Participants, and any Supporting Organizations or Advisory Committees that are not Decisional Participants;

ii. the functioning of all redress mechanisms, including without limitation the office of the Ombudsman, the IRP, and mediation;

iii. employment of staff (i.e., employees and individual long term paid contractors serving in locations where ICANN does not have the mechanisms to employ such contractors) across all locations, including all related compensation, benefits, social security, pension, and other employment costs;

iv. hiring staff (i.e., employees and individual long term paid contractors serving in locations where ICANN does not have the mechanisms to employ such contractors) in the normal course of business;

v. necessary or time-sensitive travel costs for staff (i.e., employees and individual long term paid contractors serving in locations where ICANN does not have the

mechanisms to employ such contractors) or vendors as needed in the normal course of business;

vi. operating all existing ICANN offices, and continuing to assume obligations relative to rent, utilities, maintenance, and similar matters;

vii. contracting with vendors as needed in the normal course of business;

viii. conducting ICANN meetings and ICANN intercessional meetings previously contemplated; and

ix. participating in engagement activities in furtherance of the approved Strategic Plan.

b. Below is a non-limitative list of examples, to assist with the interpretation of the Caretaker ICANN Budget Principles, of what a Caretaker ICANN Budget would logically exclude:

i. hiring staff (i.e., employees and individual long term paid contractors serving in locations where ICANN does not have the mechanisms to employ such contractors) or entering into new agreements in relation to activities that are the subject of the rejection of the ICANN Budget by the EC pursuant to the Bylaws, unless excluding these actions would violate any of the Caretaker ICANN Budget Principles;

ii. in the normal course of business, travel not deemed indispensable during the rejection period, unless the lack of travel would violate any of the Caretaker ICANN Budget Principles;

iii. entering into new agreements in relation to opening or operating new ICANN locations/offices, unless the lack of commitment would violate any of the Caretaker ICANN Budget Principles;

iv. entering into new agreements with governments (or their affiliates), unless the lack of commitment would violate any of the Caretaker ICANN Budget Principles; and

v. the proposed expenditure that was the basis for the rejection by the EC that triggered the need for the Caretaker ICANN Budget.

Annex F: Caretaker IANA Budget Principles

1. Principles

The caretaker IANA Budget (the "**Caretaker IANA Budget**") is defined as an

annual operating plan and budget that is established by the CFO in accordance with the following principles (the "**Caretaker IANA Budget Principles**"):

a. It is based on then-current operations of the IANA functions;

b. It allows ICANN, in its responsibility to fund the operations of the IANA functions, to "take good care" and not expose itself to additional enterprise risk(s) as a result of the rejection of an IANA Budget by the EC pursuant to the Bylaws;

c. It allows ICANN, in its responsibility to fund the operations of the IANA functions, to react to emergency situations in a fashion that preserves the continuation of its operations;

d. It allows ICANN, in its responsibility to fund the operations of the IANA functions, to abide by its existing obligations (including Articles of Incorporation, Bylaws, and contracts, as well as those imposed under law);

e. It allows ICANN, in its responsibility to fund the operations of the IANA functions, to avoid waste of its resources during the rejection period (i.e., the period between when an IANA Budget is rejected by the EC pursuant to the Bylaws and when an IANA Budget becomes effective in accordance with the Bylaws) or immediately thereafter, by being able to continue activities during the rejection period that would have otherwise need to be restarted at an incremental cost; and

f. Notwithstanding any other principle listed above, it prevents ICANN, in its responsibility to fund the operations of the IANA functions, from initiating activities that remain subject to community consideration (or for which that community consultation has not concluded) with respect to the applicable IANA Budget, including without limitation, preventing implementation of any expenditure or undertaking any action that was the subject of the IANA Budget that was rejected by the EC that triggered the need for the Caretaker IANA Budget.

1. Examples

a. Below is a non-exhaustive list of examples, to assist with the interpretation of the Caretaker IANA Budget Principles, of what a Caretaker IANA Budget would logically include:

i. employment of staff (i.e., employees and individual long term paid contractors serving in locations where the entity or entities performing the IANA functions does not have the mechanisms to employ such contractors) across all locations,

including all related compensation, benefits, social security, pension, and other employment costs;

ii. hiring staff (i.e., employees and individual long term paid contractors serving in locations where the entity or entities performing the IANA functions does not have the mechanisms to employ such contractors) in the normal course of business;

iii. necessary or time-sensitive travel costs for staff (i.e., employees and individual long term paid contractors serving in locations where the entity or entities performing the IANA functions does not have the mechanisms to employ such contractors) or vendors as needed in the normal course of business;

iv. operating all existing offices used in the performance of the IANA functions, and continuing to assume obligations relative to rent, utilities, maintenance, and similar matters;

v. contracting with vendors as needed in the normal course of business;

vi. participating in meetings and conferences previously contemplated;

vii. participating in engagement activities with ICANN's Customer Standing Committee or the customers of the IANA functions;

viii. fulfilling obligations (including financial obligations under agreements and memoranda of understanding to which ICANN or its affiliates is a party that relate to the IANA functions; and

ix. participating in engagement activities in furtherance of the approved Strategic Plan.

b. Below is a non-limitative list of examples, to assist with the interpretation of the Caretaker IANA Budget Principles, of what a Caretaker IANA Budget would logically exclude:

i. hiring staff (i.e., employees and individual long term paid contractors serving in locations where the entity or entities performing the IANA functions does not have the mechanisms to employ such contractors) or entering into new agreements in relation to activities that are the subject of the rejection of the IANA Budget by the EC pursuant to the Bylaws, unless excluding these actions would violate any of the Caretaker IANA Budget Principles;

ii. in the normal course of business, travel not deemed indispensable during the rejection period, unless the lack of travel would violate any of the Caretaker IANA Budget Principles;

iii. entering into new agreements in relation to opening or operating new locations/offices where the IANA functions shall be performed, unless the lack of commitment would violate any of the Caretaker IANA Budget Principles;

iv. entering into new agreements with governments (or their affiliates), unless the lack of commitment would violate any of the Caretaker IANA Budget Principles; and

v. the proposed expenditure that was the basis for the rejection by the EC that triggered the need for the Caretaker IANA Budget.

ANNEX G-1

The topics, issues, policies, procedures and principles referenced in Section 1.1(a)(i) with respect to gTLD registrars are:

- issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, security and/or stability of the Internet, registrar services, registry services, or the DNS;
- functional and performance specifications for the provision of registrar services;
- registrar policies reasonably necessary to implement Consensus Policies relating to a gTLD registry;
- resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names, but including where such policies take into account use of the domain names); or
- restrictions on cross-ownership of registry operators and registrars or resellers and regulations and restrictions with respect to registrar and registry operations and the use of registry and registrar data in the event that a registry operator and a registrar or reseller are affiliated.

Examples of the above include, without limitation:

- principles for allocation of registered names in a TLD (e.g., first-come/first-served, timely renewal, holding period after expiration);
- prohibitions on warehousing of or speculation in domain names by registries or registrars;
- reservation of registered names in a TLD that may not be registered initially or that may not be renewed due to reasons reasonably related to (i) avoidance of confusion among or misleading of users, (ii) intellectual

property, or (iii) the technical management of the DNS or the Internet (e.g., establishment of reservations of names from registration);

- maintenance of and access to accurate and up-to-date information concerning registered names and name servers;
- procedures to avoid disruptions of domain name registrations due to suspension or termination of operations by a registry operator or a registrar, including procedures for allocation of responsibility among continuing registrars of the registered names sponsored in a TLD by a registrar losing accreditation; and
- the transfer of registration data upon a change in registrar sponsoring one or more registered names.

ANNEX G-2

The topics, issues, policies, procedures and principles referenced in Section 1.1(a)(i) with respect to gTLD registries are:

- issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, security and/or stability of the Internet or DNS;
- functional and performance specifications for the provision of registry services;
- security and stability of the registry database for a TLD;
- registry policies reasonably necessary to implement Consensus Policies relating to registry operations or registrars;
- resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names); or
- restrictions on cross-ownership of registry operators and registrars or registrar resellers and regulations and restrictions with respect to registry operations and the use of registry and registrar data in the event that a registry operator and a registrar or registrar reseller are affiliated.

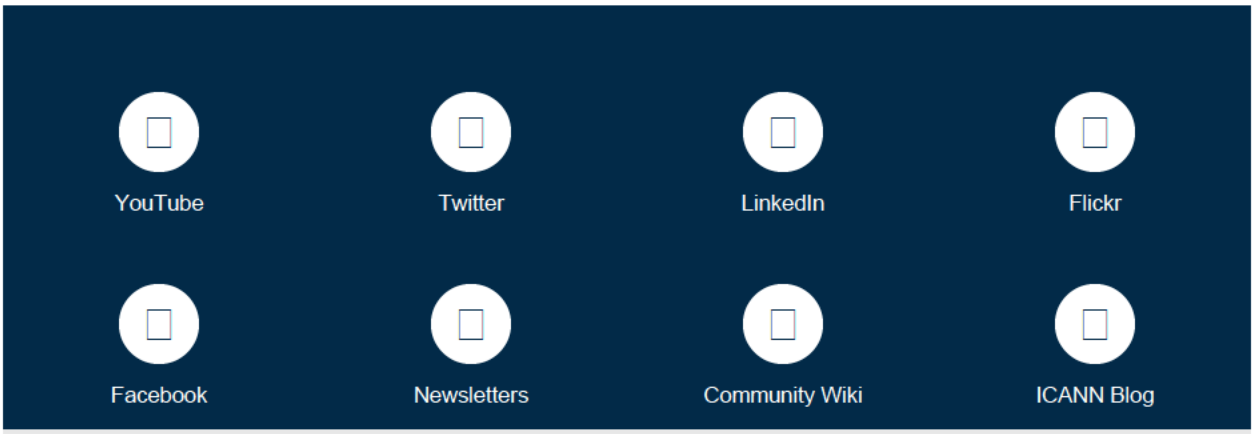
Examples of the above include, without limitation:

- principles for allocation of registered names in a TLD (e.g., first-come/first-served, timely renewal, holding period after expiration);
- prohibitions on warehousing of or speculation in domain names by registries or registrars;

- reservation of registered names in the TLD that may not be registered initially or that may not be renewed due to reasons reasonably related to (i) avoidance of confusion among or misleading of users, (ii) intellectual property, or (iii) the technical management of the DNS or the Internet (e.g., establishment of reservations of names from registration);
- maintenance of and access to accurate and up-to-date information concerning domain name registrations; and
- procedures to avoid disruptions of domain name registrations due to suspension or termination of operations by a registry operator or a registrar, including procedures for allocation of responsibility for serving registered domain names in a TLD affected by such a suspension or termination.

---

[1] When "1 October 2016" is used, that signals that the date that will be used is the effective date of the Bylaws.



Who We Are

Contact Us

Accountability & Transparency

Governance

Help

Data Protection

© 2018 Internet Corporation for Assigned Names and Numbers. Privacy Policy
Terms of Service Cookies Policy