Project Overview

to the

Request for Proposal

For

PTI SOC2 and SOC3 Audits

Date of Issue: 11 August 2017

1.0 Introduction

1.1 About this Document

The Internet Corporation for Assigned Names and Numbers ("ICANN") is seeking a provider to conduct audits mandated by the various contracts between ICANN and the Internet Engineering Task Force (IETF) and the Regional Internet Registries (RIR). The audits are also part of the contract between ICANN and the Public Technical Identifiers (PTI).

In seeking a comprehensive proposal for these services, ICANN is placing maximum emphasis on several key components of value including expertise with similar processes, demonstrated practices, and the ability to work within the guidelines established in this RFP.

1.2 Objective

The objective of this RFP is to select an independent audit firm to examine the security, process integrity and availability of: (1) The controls created as part of the Trust Services Criteria for the Service Organization Control (SOC)2 and (2) The controls created as part of the Trust Services Criteria for the Service Organization Control (SOC)3. The defined audit periods are October 1, 2017 through September 30, 2018 for the SOC2 and December 1, 2017 through November 30, 2018 for the SOC3.

1.3 Overview of the Public Technical Identifiers (PTI), an affiliate of ICANN

Public Technical Identifiers (PTI) is responsible for the operational aspects of coordinating the Internet's unique identifiers and maintaining the trust of the community to provide these services in an unbiased, responsible and effective manner. Mainly, PTI is responsible for the operation of the Internet Assigned Numbers Authority (IANA) functions; Domain Names, Number Resources, and Protocol Parameter Assignments.
The IANA functions are the services by which the top-most level of all globally unique identifiers used on the Internet are allocated and managed. These functions, first performed by Dr. Jon Postel in the 1970s, are critical to the Internet today. The efficient, secure, and stable performance of the IANA functions ensures that the Internet's Domain Name System (DNS), Internet numbering, and protocol parameter assignments continue to be globally unique and can support the continued operation and evolution of the global Internet. Since its inception in 1998, ICANN has provided the IANA functions to the Internet community and views this responsibility as core to our corporate mission of ensuring "the stable and secure operation of the Internet's unique identifier systems".

Public Technical Identifiers (PTI) was incorporated in August 2016 as an affiliate of ICANN, and, through contracts and subcontracts with ICANN, began performing the IANA functions on behalf of ICANN in October 2016.

For more information on PTI, please visit www.iana.org.

2.0 SOC2 and SOC3 Background and Scope

2.1 Period of this Audit

This is an annual audit. The final report as well as any attachments should be delivered no later than 15 December 2018 for the SOC2 and 28 February 2019 for the SOC3.

2.2 Background

In June of 2010, ICANN held its first Root Zone DNSSEC Key Signing Key (KSK) ceremony to secure the root zone of the DNS. The contract between ICANN and the National Telecommunications and Information Administration (NTIA) called for ICANN to engage a third party to ensure the appropriate internal controls were in place to meet the availability, processing integrity and security objectives for the Root Zone DNSSEC KSK System. For this system, the SOC3 framework was chosen (formerly know as SysTrust). Due to the fact that this was going to be a new, important process, ICANN selected a well established and globally recognized audit firm. That firm has been conducting the annual third party audits since 2010 to the present. The SOC3 reports are public and available on the iana.org website.

In 2013, ICANN expanded its audit of the IANA functions to cover additional systems. ICANN engaged the auditor for a SOC2 audit of the key systems used to support the IANA function's transaction processing. These systems are referred to as our Registry Assignment and Maintenance Systems (RAMS), and include the Root Zone Management System and the system used to manage protocol parameter and number allocation requests. The RAMS are audited using the SOC2 framework, which ensures that we have the appropriate internal controls to meet the availability, processing integrity and security objectives for the key systems. The firm that was chosen to conduct the annual SOC3 audit was chosen to conduct the SOC2. The annual SOC2 report has a controlled distribution.

On October 1, 2016 ICANN's contract for the IANA functions with NTIA expired. ICANN entered into contracts with the Internet Engineering Task Force (IETF) and the five Regional Internet Registries (RIRs) to provide the IANA functions. ICANN created its affiliate, PTI, to provide the IANA functions and third party audits of the Root Zone DNSSEC Key Signing Ceremonies and the Registry Assignment and Maintenance Systems are a contractual terms in the contracts between PTI and ICANN.

2.3 Scope of Work

There are two annual audits for PTI's registry systems. The SOC2 (type 2) focuses on the availability, process integrity and security of the systems used to perform the IANA functions. These systems are referred to as the Registry Assignment and Maintenance Systems (RAMS) and include the Root Zone Management System (RZMS) and Request Tracker (RT). RAMS are managed by ICANN's IT department. The SOC3 audits the availability, processing integrity and security objectives for our Root Zone DNSSEC Key Signing Key (RZ DNSSEC KSK) System. Confidentiality and privacy criteria are not a necessary part of the two audits due to the fact that policies and procedures involving IANA services are public.

PTI operates the Root Zone DNSSEC Key Signing Key System. The RZ DNSSEC KSK System is used to manage the root zone DNSSEC key life cycle, which includes generating, storing, publishing, and backing up of the Key Signing Key (KSK). The RZ DNSSEC KSK System's operations occur at secure facilities using FIPS 140-2 Level 4 cryptographic hardware security modules (HSMs).

RZ DNSSEC KSK System operations are performed in formal key ceremonies. These key ceremonies occur four times per year. In between key ceremonies, components are stored in secure containers within the secure facilities in a powered off state. The KSK is generated during key ceremonies, and is also used to sign the Zone Signing Key (ZSK) from the Root Zone Maintainer (RZM). Ceremony activities are scripted and filmed for observation and access by the public. Access to the components is limited by physical access controls; there are no logical access controls. Access to key management facilities and activities for key management operations are formally logged.

Trusted Persons, an integral element of the key ceremony, are comprised of respected community members and authorized ICANN staff. Trusted Persons include all employees, contractors, and consultants that control or have access to operations that may materially affect generation and protection of the private component of the RZ DNSSEC KSK, secure export or import of any public components, and zone file data. Trusted roles include, but are not limited to designated system administration personnel, crypto officers, recovery key shareholders, safe security controllers, internal witnesses, and the ceremony administrators.

The work methods are expected to include the following:

- One-on-one interviews with control owners and others relevant to the processes.
- Examination and evaluation of systems, policies, and processes.
- Observation of processes as needed.

ICANN will supply the controls to be used in conducting the audits, which were developed in collaboration with the control owners and/or subject matter experts. There are a total of 50

controls for the SOC2 and 35 controls for the SOC3. These controls include but are not limited to the following areas:

- Computer Operations
- Change Management
- Process Operations
- Access to Programs and Data
- Project Development
- Information Technology

The final reports will be submitted in the English language. The reports will be submitted to ICANN as an electronic document (PDF).

4.0 High Level Selection Criteria

The decision to select a provider as an outcome of this RFP will be based on, but not limited to, the following selection criteria:

1) Reputable and established audit firm
2) Understanding of the assignment
    a. Understanding of the assignment, timeline and expected deliverables
    b. Recognition and understanding that assignment requires ability to work productively and effectively with highly technical experts.
3) Knowledge and expertise
    a. Demonstrated experience conducting SOC2 and SOC3 audits.
    b. Demonstrated understanding of AICPA Guides as related to not-for-profit or non-governmental organizations
    c. Basic knowledge of ICANN, including some experience with Internet Protocols
    d. Knowledge of Cryptographic Key generation and protection methodologies
    e. Knowledge of Key Management Facilities methodologies
    f. Knowledge of Key Ceremony methodologies
    g. Technical competence and understanding of DNS and DNSSEC
    h. Suitability of proposed CVs
4) Proposed methodology
    a. Work organization, project management approach, timelines
    b. Suitability of tools and methods or work
    c. Clarity of deliverables

5) Flexibility, including but not limited to:
    a. Meeting the timeline
    b. Ability to adjust to circumstances that could modify the period and controls
    c. General adaptability
6) Value added services
7) Financial value
8) Independence including no conflict of interest
9) Reference checks

5.0 High Level Business Requirements

In order to be considered, the providers must be able to demonstrate ability to meet the following business requirements:

i. Ability to provide a complete response based on ICANN specifications by the designated due date.
ii. Ability to execute a professional services agreement substantially in accordance with the terms and conditions of ICANN's Contractor Consulting Agreement.
iii. Demonstrated ability to develop work methods, data gathering mechanisms and evaluation/assessment approaches based on the specific objective and quantifiable criteria supplied by ICANN.
iv. Ability to travel to Key Signing Ceremony sites in El Segundo, CA and Culpeper, VA.
v. Ability to provide the following deliverables (note that deliverables and dates may change due to community work schedules):

6.0 RFP Timeline

The following dates have been established as milestones for this RFP. ICANN reserves the right to modify or change this timeline at any time as necessary.

Activity	Estimated Dates
RFP published with announcement	11 August 2017
Participants to indicate interest in submitting RFP proposal	**By 23 August 2017**
Participants submit any questions to ICANN (see Excel template in RFP packet)	**By 29 August 2017 by 18:00 PDT**
ICANN responds to participant questions	By 1 September 2017
Participant proposals due by	**8 September 2017 by 18:00 PDT**
Preliminary evaluation of responses	11-22 September 2017
Target for participant presentations (finalists)	Week of 25 September 2017
Target for final evaluations, contracting and award	By 31 October 2017

7.0 Project Timeline

	Timeline for SOC2	**Estimated Due Date**
a)	Estimated Audit Kickoff for SOC2	1 March 2018
b)	Audit Walkthroughs for Phase 1	12 March 2018
c)	Audit Walkthroughs for Phase 2	20 August 2018
d)	Final Report issued	15 December 2018

	Timeline for SOC3	**Estimated Due Date**
a)	Estimated Kickoff for SOC3	1 February 2018
b)	Attend KSK Ceremony 1 for SOC3	February 2018
c)	Attend KSK Ceremony 2 for SOC3	April/May 2018
d)	Attend KSK Ceremony 3 for SOC3	August 2018
e)	Attend KSK Ceremony 4 for SOC3	October 2018
f)	Final Report issued	28 February 2019

8.0 Terms and Conditions

General Terms and Conditions

1. Submission of a proposal shall constitute Respondent's acknowledgment and acceptance of all the specifications, requirements and terms and conditions in this RFP.

2. All costs of preparing and submitting its proposal, responding to or providing any other assistance to ICANN in connection with this RFP will be borne by the Respondent.

3. All submitted proposals including any supporting materials or documentation will become the property of ICANN. If Respondent's proposal contains any proprietary information that should not be disclosed or used by ICANN other than for the purposes of evaluating the proposal, that information should be marked with appropriate confidentiality markings.

Discrepancies, Omissions and Additional Information

1. Respondent is responsible for examining this RFP and all addenda. Failure to do so will be at the sole risk of Respondent. Should Respondent find discrepancies, omissions, unclear or ambiguous intent or meaning, or should any question arise concerning this RFP, Respondent must notify ICANN of such findings immediately in writing via e-mail no later than three (3) days prior to the deadline for bid submissions. Should such matters remain unresolved by ICANN, in writing, prior to Respondent's preparation of its proposal, such matters must be addressed in Respondent's proposal.

2. ICANN is not responsible for oral statements made by its employees, agents, or representatives concerning this RFP. If Respondent requires additional information, Respondent must request that the issuer of this RFP furnish such information in writing.

3. A Respondent's proposal is presumed to represent its best efforts to respond to the RFP. Any significant inconsistency, if unexplained, raises a fundamental issue of the Respondent's understanding of the nature and scope of the work required and of its ability to perform the contract as proposed and may be cause for rejection of the proposal. The burden of proof as to cost credibility rests with the Respondent.

4. If necessary, supplemental information to this RFP will be provided to all prospective Respondents receiving this RFP. All supplemental information issued by ICANN will form part of this RFP. ICANN is not responsible for any failure by prospective Respondents to receive supplemental information.

Assessment and Award

1. ICANN reserves the right, without penalty and at its discretion, to accept or reject any proposal, withdraw this RFP, make no award, to waive or permit the correction of any informality or irregularity and to disregard any non-conforming or conditional proposal.

2. ICANN may request a Respondent to provide further information or documentation to support Respondent's proposal and its ability to provide the products and/or services contemplated by this RFP.

3. ICANN is not obliged to accept the lowest priced proposal. Price is only one of the determining factors for the successful award.

4. ICANN will assess proposals based on compliant responses to the requirements set out in this RFP, any further issued clarifications (if any) and consideration of any other issues or evidence relevant to the Respondent's ability to successfully provide and implement the products and/or services contemplated by this RFP and in the best interests of ICANN.

5. ICANN reserves the right to enter into contractual negotiations and if necessary, modify any terms and conditions of a final contract with the Respondent whose proposal offers the best value to ICANN.