Explanation/Background: ICANN is posting a summary of actions it has taken in response to recommendations made by JAS Communications LLC (JAS), an external consultant, related to ICANN's IANA functions process. The JAS Evaluation document, " IANA Process for Implementing Root Zone Change Requests - Review and Assessment of Risk Management strategy and Comparison of Implementation Options", is also posted in order to share with the community the findings and recommendations made by the external consultant and to add transparency to how ICANN manages the IANA functions process. The review was conducted from August –November 2009 and initial findings were submitted to ICANN on 28 October 2009, with the final Report being delivered on 14 December 2009. This report reflects JAS's perspective on ICANN's IANA's functions processes and procedures. Furthermore, the report was intended to focus solely on the roles and responsibilities of ICANN as the IANA functions operator. ICANN prematurely posted the "IANA Process for Implementing Root Zone Change Requests - Review and Assessment of Risk Management strategy and Comparison of Implementation Options" before reviews were completed, which included pages that were left unintentionally marked "Confidential". After further internal review, the document is being reposted with an explanation as to how ICANN addressed the nine recommendations contained in the report.

Explanatory Memoranda regarding the Report "IANA Process for Implementing Root Zone Change Requests - Review and Assessment of Risk Management strategy and Comparison of Implementation Options"

During August – November 2009, ICANN engaged JAS Communications, LLC (JAS)to conduct an external review of the root zone change process, analyzing the current manual and proposed automated processes and procedures. The final Report was delivered to ICANN on 14 December 2009. The external review fulfills ICANN's commitment to Business Excellence and Business Continuity, two related projects meant to ensure full availability and excellent performance of the IANA functions and services. This report reflects JAS's perspective on ICANN's root zone change processes and procedures. Furthermore, the report was intended to focus solely on the roles and responsibilities of ICANN as the IANA functions operator. ICANN prematurely posted the "IANA Process for Implementing Root Zone Change Requests - Review and Assessment of Risk Management strategy and Comparison of Implementation Options" before reviews were completed, which included pages that were left unintentionally marked "Confidential".

JAS submitted its results to ICANN with nine recommendations for improved security and stability of operations. After the November 24, 2009 tabletop/discussion-based exercise ICANN chose to adopt many of the recommendations. Particularly, ICANN addressed infrastructure, communications, and resource disruption concerns. Subsequently, after the no-notice full-scale business continuity/disaster recovery exercise in January 2010, JAS revised the risk assessment of ICANN's IANA functions process. The revised assessment is contained in Appendix G to the Report. The disaster recovery exercise was designed to validate efforts by ICANN to improve the resiliency of critical business processes in ICANN's performance of the IANA functions.

ICANN for the last five months, addressed the nine recommendations for improved security and stability of operation:

RECOMMENDATION 1: Clarify overall Risk Governance –

ICANN has clarified several critical questions of risk governance by clearly listing critical ICANN processes and systems in the ICANN Business Continuity plan and introducing a requirement limiting acceptable service downtime following a continuity event to a maximum of four hours.

RECOMMENDATION 2: Clarify operational relationship with ICANN IT.

ICANN has documented policies, responsibilities, and procedures for disaster recovery of the critical systems such as the RT Ticket system and the RZMS system.

RECOMMENDATION 3: Formalize governance of the development of the new RZMS system.

ICANN has assigned a Program Manager to the RZMS development project to document and track the implementation and development schedule. ICANN has dedicated internal resources testing the delivered product against internally defined test scenarios.

RECOMMENDATION 4: Formalize policies regarding key employees including training and certification programs, employee screening, and the use of "two person rules."

ICANN recognizes the importance of training and certification programs. Developing programs to formally cross-train employees is a project that we are considering for 2011. As for the other recommendations about changing our HR policies, ICANN has no intention at this time to adopt these recommendations.

RECOMMENDATION 5: Increase physical distribution of critical resources.

ICANN established a datacenter in Northern Virginia with hot standby systems in the event the Los Angeles facilities are unavailable for an extended period of time.

RECOMMENDATION 6: Increase resiliency of communications with partners.

ICANN has focused its efforts in 2010 on increasing the resiliency of its critical systems and operational capability with the establishment of a datacenter in Northern Virginia. We collaborate closely with our partners and ICANN does have a satellite office in the DC area.

RECOMMENDATION 7: Increase resiliency of communications with employees and customers.

ICANN has procured GETS/WPS capabilities for critical employees and has distributed satellite phones strategically.

RECOMMENDATION 8: Exercise business continuity operations regularly.

ICANN is formulating its business continuity operations schedule for 2011. This is a continuing work in progress.

RECOMMENDATION 9: Formalize multiple service levels.

ICANN is evaluating the pros and cons of this recommendation. Our current request-driven process has served us well and it is unclear at this time if there is a business reason to adopt this recommendation.

JAS COMMUNICATIONS LLC
INFORMATION TECHNOLOGY · RISK MANAGEMENT · GOVERNANCE

IANA Process for Implementing Root Zone Change Requests

Review and Assessment of Risk Management Strategy

and

Comparison of Implementation Options

ICANN

JAS Communications LLC

19 April 2010

Founded in 2003, JAS Communications LLC is a unique professional services firm delivering risk management, technology, and governance solutions to a wide range of commercial and government clients.

http://www.jascommunications.com

Table of Contents

1 Preface to 1Q 2010 Report

JAS Communications LLC was engaged in August, 2009 to provide a risk assessment of the ICANN/IANA root zone change process. The analysis that comprises the majority of the following pages is based on data obtained through November, 2009.

JAS would like to call attention to the rapid pace of business process improvement, continuity planning, and formalization within ICANN's IANA department that has taken place since November. The IANA department, with assistance and support from multiple areas within ICANN, has made significant progress improving the resiliency of their business processes.

In the months since August, 2009, significant accomplishments include:

1. Clarification of risk governance requirements by clearly listing critical IANA departmental systems and introducing a requirement limiting service downtime to a maximum of four hours;
2. Creation of a hot datacenter in Reston, Virginia;
3. Completion of a detailed ICANN/IANA Business Continuity plan;
4. Execution of multiple business continuity tabletop exercises (TTX);
5. Successful completion of a no-notice exercise in which production personnel and IT systems in the greater Los Angeles area were removed from service and replaced by staff outside of California and IT systems in Reston.

Please see Appendix G for more information about the recent improvements and the impact on the IANA department's overall risk posture.

2 Executive Summary

ICANN manages the IANA functions under a contract with the United States Department of Commerce, National Telecommunications and Information Administration (NTIA) division. In the performance of this contract, ICANN has created an internal department named "IANA." The ICANN/IANA root zone management processes are critical to the operation of the Internet. Endeavoring to provide the highest quality of service, ICANN management is undertaking a comprehensive business process improvement initiative designed to:

- Document long-standing processes to industry standards;
- Implement automated systems enabling IANA departmental processes to scale in support of anticipated new demands stemming from the introduction of new TLDs, DNSSEC, and IDN;
- Avoid the introduction of unmanaged risks during automation and scale-up;
- Enable ongoing and proactive monitoring of risk and compliance;
- Provide demonstrable evidence that the IANA departmental processes are tightly managed and consistent with industry best practice.

Regarding the root zone management process, ICANN is charged with managing the risks that may result in the following failure modes:

- Unable to complete a change request in a timely fashion (process resiliency)
- Unintentional introduction of an error (process engineering)
- Intentional introduction of an error (security)

To assist ICANN with this undertaking, JAS has provided a rigorous, scientific, and quantitative analysis of the IANA department's business process risks and the mechanisms deployed to assess, monitor, and manage these risks. JAS was also asked to compare the overall posture of the current "manual" process implementation and a future "automated" process implementation.

2.1 Current "Manual" Implementation

The security and resiliency risks associated with the current manual implementation are largely managed through reliance on the availability of a small, expert, and loyal staff routinely exercising judgment and processing a light workload of approximately one request per day on average. Business continuity planning is largely informal and also dependent on the flexibility and loyalty of expert staff handing a light workload in a highly manual fashion. Communications - between ICANN staff performing IANA functions, and with partners VeriSign and NTIA - are critical. While several IT systems operated by ICANN's internal IT department, namely email and the RT ticketing system, are key resource dependencies, no formal service level agreements are in place, and these systems have no known operational certifications. A significant amount of manual rekeying is currently required and has been the root cause of several historical errors.

History has shown the current approach to be effective with a very low error rate (less than 1%), with no significant failures to meet service level commitments. However, this approach has never been significantly stressed with a workload spike, a major business continuity event, or a serious security event (successful or attempted).

2.2 Future "Automated" Implementation

With the probable introduction of new top level domains (gTLDs and IDNs), ICANN is preparing to increase the scalability and formality of their business processes, including those in the IANA department. The primary process change for root zone management will be the implementation of an IT system (RZMS), which will automate a significant proportion of the currently manual root zone change process. The stated goal of the automation system is to increase the scalability of the process by offloading several currently manual operations, and to reduce the error rate by almost completely removing the need to rekey.

The automated implementation maintains the critical dependency on highly skilled and loyal employees successfully exercising judgment, and on critical IT systems operated by ICANN's internal IT department. Similarly, availability of communications between partners remains critical, particularly mutual access to the Internet. The availability and security of the new RZMS IT system is a new critical dependency in this implementation and is additive to the existing critical dependency on the RT IT system. Both systems will continue to be operated by ICANN's internal IT department.

The RZMS system is being co-developed with a third party, and security and resiliency requirements have not been formalized. In general, increased reliance on the newly implemented RZMS system opens security and resiliency vulnerabilities ranging from intentional malice to unintentional "bugs," missing/unclear requirements, and/or unintended functional consequences. Similarly, outsourcing development, particularly to firms located outside the United States, opens supply chain risks, including the possibility of allowances for unauthorized access. ICANN plans to mitigate these vulnerabilities through pre-implementation testing, code review, and penetration testing by third parties. Furthermore, ICANN/IANA intends to operate the new system alongside the existing system for an extended period of "real-world" testing.

2.3 Comparison

Both the manual and automated implementations of the business process have similar critical dependency requirements. Both implementations are highly dependent on available, loyal, and expert staff with access to several IT systems. Both implementations depend on the availability and security of critical supporting IT systems: RT, RZMS, and email. Both implementations depend on communications between ICANN, NTIA, and VeriSign, and both have nearly all critical resource dependencies physically located in the greater Los Angeles area. The key difference between the implementations is the improved scalability, efficiency, and reduction in manual rekeying that are the primary value drivers of the automated implementation.

The automated implementation enables a higher level of security through logging, audit, and enforcement of "two person rules" authorizing activities. However, security requirements for the RZMS system are not formalized, and it is not clear to what extent these safeguards will be implemented.

2.4 Recommendations

RECOMMENDATION 1: Clarify overall Risk Governance. Lack of clarity surrounding the level of risk ICANN is willing to accept makes it difficult for ICANN/IANA Management to manage risk properly. ICANN Directors and Senior Management must specify the degree of acceptable risk and desired posture during business continuity events and resource the business managers appropriately. For example, a very low tolerance for the introduction of intentional errors will result in requirements for certified high security system implementations, multifactor personnel authentication, high physical security, multiple levels of manual review and authorization, extensive logging and auditing, etc. Similarly, if the desire is to maintain full processing capacity and generally "not miss a beat" during business continuity operations, the result will be multiple redundant "hot" sites, a physically distributed staff of trained and certified employees, multiple resilient communications paths between partners, high availability IT systems, highly disciplined IT operations, tight Service Level Agreements, etc. The level of acceptable risk drives the implementation of controls and compliance mechanisms, and of course cost.

Absent this clarity, portions of this analysis are based on ICANN and JAS' best understanding of the appropriate risk posture for the root zone management process. These assumptions are fully described in Section 5.

RECOMMENDATION 2: Clarify operational relationship with ICANN-IT. ICANN's IANA department has critical dependencies on multiple systems operated by ICANN's IT department, namely email, the RT ticket system, and the new RZMS system. Depending on the level of risk ICANN/IANA is willing to accept, differing levels of service will be required from ICANN-IT. This relationship must be discussed, mutually agreed upon, and memorialized in the form of business continuity operational procedures, security, and system administration requirements.

RECOMMENDATION 3: Formalize governance of the development of the new RZMS system. The new RZMS system is a critical component of the new automated root zone management process. Significant parts of the development of this system are being provided through an international supply chain with limited specification formality. No formal requirements exist regarding the security and resiliency of these systems, making it impossible to know whether the system has been built to specification. JAS recommends formal requirements around security and resiliency be provided to the developers, and ICANN/IANA rigorously test and audit the delivered product against these requirements.

RECOMMENDATION 4: Formalize policies regarding key employees including training and certification programs, employee screening, and the use of "two person rules." ICANN/IANA is highly dependent on the availability, judgment, and historical/institutional knowledge of a small number of highly specialized critical employees. However, limited formality is in place to manage the risks presented by this dependency. As Information Technology professionals in large metropolitan areas are especially vulnerable to churn, and critical employees are uniquely positioned to negatively affect system integrity and availability (the "insider threat"), this is a relevant risk necessitating formal controls and compliance mechanisms. Moreover, it is reasonable to assume that the IANA department will need to scale-up operations at some point in the future to support root zone expansion; this scale-up will almost certainly require the expansion of the critical employee pool.

JAS recommends a formal training and certification program covering the job responsibilities of employees involved in the root zone change process. These programs will improve process documentation, scalability and resiliency of the IANA department's human resources, and enable a greater degree of capacity planning.

Because of the high degree of trust ICANN/IANA must have in their employees, ICANN is especially susceptible to the insider threat. System administrators and superusers within the IANA department and ICANN-IT almost certainly have unique abilities to forge/alter requests, modify logs, and perform other malicious activities that can have significant impact on the availability and accuracy of the root zone change process. While present employees are certainly loyal and trustworthy, unfortunately, it is not safe to assume this will always be the case. As such, JAS recommends a formal program to vet potential new hires, and to periodically re-vet employees over time. Such a vetting program would include screening for illegal drugs, evaluation of consumer credit, and psychiatric evaluation, which are all established risk factors for unreliable and/or malicious insider activity and are routinely a part of employee screening in government and critical infrastructure providers.

Finally, JAS recommends implementing "two-person rules" at critical gates in the root zone change process. A two-person rule requires two distinct individuals to "sign-off" on a change before it is committed to the system, providing a valuable second set of eyes as well as a solid audit trail. Two-person rules are highly effective controls against both accidental and intentional human errors.

RECOMMENDATION 5: Increase physical distribution of critical resources. Currently, nearly all critical resources are physically located in the greater Los Angeles area. While it is feasible that highly manual continuity operations could continue even in the face of a major regional event, the significant reduction in process capacity coupled with the probable increase in root zone change requests as a result of such an event would have a negative impact both on process throughput and error rate. Exacerbating the lack of resource distribution, the Los Angeles metropolitan area is burdened with a higher than average level of risk to a wide range of both natural and manmade disruptions. As such, JAS recommends reducing the dependence on the greater Los Angeles area to the extent required to implement ICANN's risk governance guidance (Recommendation 1).

RECOMMENDATION 6: Increase resiliency of communications with partners. The root zone management process requires tight communication and coordination between ICANN/IANA, VeriSign, and the NTIA. Presently, this communication leverages the Internet (email), and the public telephone system with email being the primary mechanism. The automated implementation of the process shifts almost all ICANN-VeriSign communications to the Extended Provisioning Protocol (EPP), which leverages Internet connectivity between the IANA department's RZMS system and VeriSign's systems. This introduces significant dependence on a functioning Internet connection between the RZMS system - physically located in the Greater Los Angeles area - and VeriSign's systems - physically located in Northern Virginia. Similarly, the ICANN-NTIA communications leverage Internet email connectivity between Los Angeles and Washington, DC. These dependencies are significant to the point that a large-scale Internet disruption affecting traffic between the East and West Coasts of the United States would have a debilitating effect on ICANN/IANA's ability to execute the process. Such a large-scale Internet disruption, particularly in conjunction with other stressors such as a natural disaster, is not unforeseeable; several sources assign the probability of such an event at up to 20% in the next 20 years (see Section 4.4.4).

JAS recommends increasing the resiliency of communications between the three critical parties. The easiest and most cost effective way to accomplish this may be for ICANN/IANA to staff a satellite office physically proximate to both partners in the Greater Washington, DC area. A physically proximate office would enable cost effective alternate communications between the three parties including private telecommunications circuits and in-person meetings. It is also unlikely that resources in both the Los Angeles and Washington offices would be simultaneously affected by an incident requiring continuity operations.

RECOMMENDATION 7: Increase resiliency of communications with employees and customers. Non-standard operations during times of stress require resilient communications among ICANN/IANA employees and with customers. Even though highly manual operation is possible, the requests must first get to ICANN/IANA employees, and these employees must be capable of communicating among themselves, their partners, the requestor, and potentially with ICANN/IANA senior management. Currently, all inbound requests have a dependency on resources in the greater Los Angeles area: email and Internet IT systems as well as telephone communications, FAX and postal mail delivery all leverage resources in LA (it is probable that calls to the ICANN/IANA 3rd party answering service in the United Kingdom are routed through Los Angeles). JAS recommends increasing communication resiliency by procuring satellite telephones and GETS/WPS[1] priority telephone service for critical employees, and by publishing to customers backup contact instructions that do not have a dependency on the Los Angeles area. For example, landline telephone and FAX numbers for the UK answering service and/or an East Coast ICANN/IANA office.

RECOMMENDATION 8: Exercise business continuity operations regularly. While the nature of the root zone change process facilitates highly manual, human-oriented emergency continuity operations, JAS recommends business continuity operations be formalized and regularly exercised. Exercises are a useful compliance mechanism to assure management that the controls in place are effective.

One typical exercise routine is to artificially fail-over to continuity operations/sites on a regular basis. For example, several sophisticated entities in the banking and finance sector regularly process 80% of their daily transactions at the primary site and 20% at a backup facility. Similarly, other enterprises activate continuity operations on a regular basis to handle the full regular load for a day, for example the second Thursday of each month. As continuity operations/policies tend to get "stale" very quickly, the advantage of these approaches is that the firm is always aware of their continuity posture and relatively assured it will be available in a pinch.

[1] http://gets.ncs.gov and http://wps.ncs.gov

While the operation of ICANN's IT department is beyond the scope of this analysis, JAS recommends that the IANA department work with ICANN-IT to regularly test backup/restore operations for critical IANA systems.

RECOMMENDATION 9: Formalize multiple service levels. Whether formal or not, most request-driven business processes like the root zone change process have multiple levels of service. "Normal" requests are submitted using the standard channels and handled roughly in sequence. "Emergency" requests may have a formal priority submission channel and/or markings, or may receive priority handling informally by calling a known contact, appealing to a manager, asking for a "favor," or otherwise requesting an expedite out of band. JAS' experience is that these informal priority channels always exist, are nearly impossible to stamp-out, and that inconsistent service levels realized through these priority channels are often a source of periodic tension. JAS has found that formalized priority service levels offer an important triage in time of stress, particularly because stressors such as natural disasters often cause an increase in requests while reducing processing capacity. JAS recommends formalizing priority handling by implementing normal and expedited service levels and publishing commensurate service levels.

3 Methodology

JAS was charged with evaluating the business process risks that may result in inability to complete the process, or the introduction of intentional or unintentional errors. JAS systematically applied the following methodology.

3.1 Document and Model the Process

Based on in-person interviews with IANA departmental Staff and documentation of the Root Zone Update Procedure, JAS built a Unified Markup Language (UML) Activity Diagram of the business process. Each Activity has a set of Resources on which it depends; JAS built a list of Resources and mapped each Activity's dependence on Resources through an equation expressed in Boolean Algebra. The Algebraic equations permit modeling complex resource dependency relationships such as groups of absolute dependencies (AND) and interchangeable Resources (OR). The result is a list of Resources, and an equation for each Activity capturing its' resource dependencies. These representations can be found in the Appendices.

3.2 Identify Risk Governance

ICANN and JAS discussed the level of risk tolerance surrounding the process, the controls and compliance mechanisms in place, and coping mechanisms to deal with failures. Past error rates and modes were also discussed and used as inputs into the modeling. Guidance provided by ICANN Senior Management to the IANA department regarding the level of risk tolerance was also discussed.

3.3 Evaluate Resource Dependencies

One potential shortcoming of informal business process security and continuity planning is unintentionally focusing on the wrong problems. In many cases, cursory review or qualitative "gut feeling" analysis of a business process provides inadequate or incorrect awareness of the overall Resource dependency landscape. JAS avoids this pitfall through mathematical modeling of the Resource dependencies. Based on a model of the business process and the Resource dependencies at each step of the process, multiple stochastic and probabilistic Monte Carlo-type simulations were run to determine the behavior of the process given various Resource failure scenarios. The result is a clear, quantitative understanding of the areas that warrant analysis. Further details concerning the simulation analysis are given in Appendix E.

Since an objective of the study was to compare the current "manual" implementation of the process with a future "automated" implementation, two Resource equations were created for each Activity: one capturing the Resource dependencies in the "manual" implementation, the other capturing the Resource dependencies in the "auto" implementation. Both implementations of the process are sufficiently similar as not to warrant individual Activity Diagrams. Several Activities are rendered obsolete by the "auto" implementation; this behavior is easily modeled for our purposes by removing all Resource dependencies for the obsolete Activity.

3.4 Analyze Controls and Compliance Mechanisms; Make Recommendations

Based on the resource dependency models, JAS analyzed the current controls and compliance mechanisms for the critical resources. Risks can be under-managed, over-managed, or properly managed based on the risk tolerance guidance provided to business managers. JAS analyzed the effectiveness of the controls and compliance mechanisms based on our understanding of the risk governance and desired risk posture as described in Section 5. Areas where risks were over or under managed, JAS made recommendations to bring exposure in-line with tolerable levels.

3.5 Compare Process Implementations

Based on models for both the "manual" and "automated" process implementations, JAS compared the overall risk posture of the two process implementations.

4 Process Description

This section was substantially provided by the ICANN/IANA department. Resource dependencies for each activity may be found in Appendix D.

4.1 Request Creation

The individual requesting the change ("requester") submits the change to ICANN/IANA for consideration.

Manual Implementation: Receive request via email, phone or fax. Request is formulated using a standard template. A reference number is automatically sent back by the RT ticket system if lodged via email.

Automated Implementation: Manual methods still accepted, with addition of submission via web form. ICANN/IANA staff will key request into the web form if received by manual methods.

4.2 Pre-review

For documents that are not submitted electronically via the web interface, the submitted request is checked that it is well-formed, and that the intentions are clearly understood by ICANN/IANA staff.

Manual Implementation: Staff review the application, and clarifications are sought from the applicant if necessary.

Automated Implementation: None. (Not used because well-formed requests are ensured by the web interface, disallowing irregular input and providing real-time feedback to the requester prior to request submission.)

4.3 Pre-review clarification

The requester has been asked to provide clarification on the request, and ICANN/IANA staff are waiting for this clarification before processing can proceed.

Manual Implementation: Staff have sent a request for further information to the requester.

Automated Implementation: Not applicable.

4.4 Technical Check

The request is tested for compliance against various technical requirements for name servers, URLs, WHOIS servers and DNSSEC data.

Manual Implementation: Staff manually test the supplied data using a variety of internal tools.

Automated Implementation: The system automatically checks for adherence against all technical requirements.

4.5 Technical Check Remedy

If deficiencies are encountered during the technical check, the applicant is advised and the process stalls until they are remedied.

Manual Implementation: Staff wait for the applicant to respond in order to retest, or to waive the requirements.

Automated Implementation: The system regularly retests against the criteria. If the domain becomes compliant, it advances; or if the requester seeks a waiver, staff manually advance the request.

4.6 Contact Confirmations

ICANN/IANA staff ask the relevant contacts to consent to the request. The relevant contacts are deemed to be the administrative contact ("AC") and technical contact ("TC"), and in the event of the change of either, the proposed administrative contact ("PAC"), and/or the proposed technical contact ("PTC").

Manual Implementation: Staff prepare requests to relevant contacts and ask them whether they consent to the request.

Automated Implementation: The system generates emails with unique tokens that can be confirmed either via email or via a web interface.

4.7 Sponsor Endorsement

In the event contact persons are unreachable or unable to respond authoritatively for the request, the Sponsoring Organization is contacted to provide formalized documentation authorizing the change.

Manual Implementation: Staff contact the organization to arrange for appropriate documentation.

Automated Implementation: Same as Manual Implementation.

4.8 Impacted Party Confirmations

For changes to shared name serves, all impacted top-level domain operators must also consent to the change.

Manual Implementation: Staff prepare requests to relevant contacts and ask them whether they consent to the request.

Automated Implementation: The system generates emails with unique tokens that can be confirmed either via email or via a web interface.

4.9 Manual Review

Staff reviews the request to perform assessments that cannot be automatically conducted. This includes review for satisfaction of legal and regulatory compliance, any special handling instructions, and normalization of the supplied request.

Manual Implementation: ICANN/IANA staff perform regulatory check procedure; Check special instructions for special handling requirements; Check if it is a substantive change requiring a delegation evaluation; Normalize the data to correct spelling mistakes; and to use consistent formatting.

Automated Implementation: Same as Manual Implementation.

4.10 Delegation Evaluation

For changes where the change is deemed to be a material change in the operator of the domain, then additional evaluation is required, usually involving agreement by the ICANN Board of Directors.

Manual Implementation: Staff perform the delegation evaluation process, including preparing a staff report, scheduling it with the ICANN Board of Directors, and awaiting a board resolution on the matter. During this process they will confer with the requester for any additional documentation required.

Automated Implementation: Same as Manual Implementation.

4.11 Supplemental Technical Check

The request is tested a second time for compliance against various technical requirements. This is executed as a significant amount of time may have elapsed since the initial application, during which time problems may have been introduced to the applicant's configuration.

Manual Implementation: Staff manually test the supplied data using a variety of internal tools.

Automated Implementation: The system automatically checks for adherence against all technical requirements.

4.12 Supplemental Technical Check Remedy

If deficiencies are encountered during the supplementary technical check, the applicant is advised and the process stalls until they are remedied.

Manual Implementation: Staff wait for the applicant to respond in order to retest, or to waive the requirements.

Automated Implementation: The system regularly retests against the criteria. If the domain becomes compliant, it advances; or if the requester seeks a waiver, staff manually advance the request.

4.13 US Government Authorization

The US Government is required to authorize all changes to the DNS root zone, and the root zone database.

Manual Implementation: Staff prepare a specially formatted transmittal letter, which is sent to NTIA for authorization.

Automated Implementation: System initiates EPP transaction with VeriSign, and formulates transmittal letter based on attributes of that exchange, which is sent to NTIA for authorization.

4.14 US Government Clarification

If the US Government seeks clarifications relating to the request, ICANN/IANA staff will seek answers to those questions prior to authorization being granted.

Manual Implementation: NTIA contacts ICANN/IANA staff, who address the questions raised, and then ask NTIA again for authorization.

Automated Implementation: NTIA contacts ICANN/IANA staff, who move request into this state, which concludes the outstanding EPP transaction with VeriSign. Once the questions have been addressed, ICANN/IANA staff trigger the system to initiative a new EPP transaction and recommence USDOC approval stage.

4.15 Root Zone Implementation

If the request alters the root zone, upon authorization it is independently tested, scheduled and then implemented in the root zone by VeriSign.

Manual Implementation: Upon authorization, VeriSign perform internal tests. If successful, signal to ICANN/IANA they are ready to proceed and advise an implementation schedule. After successful implementation, VeriSign advise ICANN/IANA they have implemented the change.

Automated Implementation: Upon authorization, VeriSign conducts workflow, and ICANN/IANA system is kept updated on process through EPP poll messages.

4.16 Verification and Implementation

Any change to the root zone is verified, and changes to the root zone database are implemented.

Manual Implementation: ICANN/IANA verifies any changes to the root zone are implemented correctly, updates the WHOIS database with the changes.

Automated Implementation: Verify root zone changes match expectation, commit transaction’s changes to the database.

4.17 Completion

This is the terminal state of a successfully completed request.

Manual Implementation: Notice of completion is drafted and sent to the requester and contacts.

Automated Implementation: Automatically generated notice of completion sent.

5 Results

The ICANN/IANA Root Zone Change process is presently a low volume, highly manual process completed by trustworthy experts of exceptional professional caliber. As a result, the process has proven quite stable with a historical error rate of less than 1 error per year, yielding an error rate of approximately 0.2%. Note that this calculation only takes into consideration errors that made it entirely through the process and into the root zone file. While the IANA department endeavors to collect data on these "caught errors," no such data was available for this analysis. Similarly, with one exception, no rigorous historical data is available regarding processing delays due to system/IT or other resource failures. However, empirical data indicates that such delays are extremely limited given the rather large time window allotted for process completion and a range of flexible process execution options.

5.1 Modality of Historical Errors

ICANN/IANA has explored each historical error in detail. The result of this research indicates that the root cause of all known errors to date has fallen into the following categories:

- Human Judgment Error
- Human Rekey Error
- Unanticipated System Behavior/Bug

The JAS findings are consistent with the ICANN/IANA historical analysis.

5.2 Factors Impacting Timeliness

As previously stated, empirical data indicates that the timely completion of the process is typically not a factor given the rather large window allotted for process completion. The exception to this is the Confirm_Impacted_Parties Activity, which introduces the potential for an open-ended wait on third parties. Unlike other Activities with callbacks to third parties, as a matter of policy this Activity has no timeout provision; as such, a third party may hold-up a change request indefinitely and with few options for recourse. This reality is an artifact of policy and cannot be addressed in the process itself. It should be noted that a technical workaround is available that effectively drops the "impacted party" relationship permitting unilateral changes to the root zone file.

Confirm_Impacted_Parties is the only Activity in the process with an unbounded time to completion property that has been problematic.

5.3 Critical Resources

Overall, the ICANN/IANA Root Zone Change process is a consolidated business process in that there is a high level of dependency on a relatively small subset of Resources. For both implementations of the business process, the critical resource dependencies are listed below. The top quartile of resource dependencies are in red while other important resources are in orange.

Manual	Auto	Common
RT (*)	RZMS & RT (*)	Exchange_Email
Exchange_Email	Internet_large_scale (*)	Email_MX
Email_MX	Exchange_Email	Human_Judgement
Human_Rekey (*)	Email_MX	HQ
Human_Judgement	Human_Judgement	Los_Angeles_Metro_Area
Authorized_PGP_Key (*)	HQ	
HQ	Los_Angeles_Metro_Area	(*) Denotes Unique
Los_Angeles_Metro_Area		

Table 1: Critical Resources

These are the resources that have the most significant impact on ICANN/IANA's ability to complete the process correctly and in a timely fashion (See Appendix F for full resource impact table). Note that these are not simply the "single points of failure," rather, they are resources that are the most critical and the most at risk of failure given historical data, industry data and norms, and probabilistic models of cascading failures.

5.4 Dependence on IT Systems

Far and away, the most critical resources, critical to both implementations of the process, are the IT systems: the two components of enterprise email and the ticketing/workflow systems. The manual implementation of the process makes extensive use of the RT ticketing system for workflow, tasking, and general process management. Similarly, the auto implementation is heavily dependent on the proprietary software system we have called "RZMS" in addition to RT, which remains a critical dependency in the "auto" process implementation.

5.4.1 Request Tracker Ticketing System (RT)

Request Tracker (RT) is a mature and widely-deployed Open Source ticket tracking system on which ICANN/IANA has built the current manual process. RT is used internally by ICANN/IANA staff throughout the process to manage the workflow and provide reporting/SLA data. RT is not exposed to ICANN/IANA's customers, rather, staff uses the system through HTTP and email interfaces.

The RT system is operated by ICANN's IT department (ICANN-IT), and no Service Level Agreements are currently in place. No known audits or certifications of ICANN-IT's operations are in place. For the purposes of this study, JAS used baseline assumptions of industry best practices to model the behavior of this system, including a 99.9% ("three nines") availability assumption equating to less than nine hours of downtime per year.

5.4.2 Root Zone Management System (RZMS)

The Root Zone Management System (RZMS) is a new IT system currently being developed to enable an automated root zone change process. RZMS is a classic multi-tier online system comprised of a web front-end, a Java application layer, and a database back-end. This system is being co-developed with a foreign technology firm. When deployed, RZMS will work in conjunction with RT to automate portions of the process, manage internal workflow, and present interfaces directly to ICANN/IANA customers in the form of a web interface and automatically generated emails. Finally, RZMS will interact directly with VeriSign using the Extensible Provisioning Protocol (EPP).

Like the RT system, RZMS is operated by ICANN-IT and no Service Level Agreements are currently in place and no known audits or certifications of ICANN-IT's operations exist. For the purposes of this study, JAS used baseline assumptions of industry best practices to model the behavior of this system, including a 99.9% ("three nines") availability assumption.

5.4.3 Email

Email is the lifeblood of the ICANN/IANA root zone management process. Presently, customers initiate the vast majority of change requests via email. Email is used extensively internally for workflow, management, and interfacing with other staff and RT. Moreover, email is the primary vector of communications with domain owners, impacted parties, NTIA, and VeriSign.

This high level of dependence on email will not change after RZMS is deployed. While customers will interface directly with RZMS through a web portal, RZMS will continue to interface with domain owners, impacted parties, and ICANN/IANA staff via email. While RZMS communicates with VeriSign primarily using EPP, communications with NTIA will continue to leverage email.

External email communications require proper functioning of two resources: a MX host managed by ICANN-IT, and an outsourced provider of ICANN's Exchange Server. All external email and some internal email must traverse both systems in order to be delivered.

The MX host is operated by ICANN-IT, and nothing can be said concerning controls/compliance mechanisms currently in place. The Exchange Server is operated by a third party with an unknown service level agreement and no known SLA monitoring.

Like the other IT systems, for the purposes of this study, JAS used baseline assumptions of industry best practices to model the behavior of both the outsourced email and MX host systems, including a 99.9% ("three nines") availability assumption.

5.4.4 Internet Availability

All of ICANN/IANA's IT systems also depend on the availability of the Internet. All email requires Internet availability in order to be delivered; even internal email requires Internet connectivity due to the use of an outsourced provider. Critical path email to NTIA, impacted parties, and domain owners require mutual Internet access. Access by customers to RZMS over the web interface requires Internet availability by both parties - and connectivity in between. Perhaps most critically, EPP communication between RZMS and VeriSign requires Internet connectivity.

For the purposes of this study, JAS assumed 99.9% local Internet availability/connectivity, with a 10% chance of a significant, medium to long-term, large scale Internet disruption over the next 20 years. The

JAS assumptions are at the low end of the frequently cited Business Roundtable report suggesting a 10-20% probability of such a disruption in the next 10 years.[2]

5.4.5 PGP Keys

Presently, all email communications between ICANN/IANA, NTIA, and VeriSign staff are encrypted using PGP. The PGP keys in use are generated for this purpose only and pre-shared in-person. The keys are generated by and issued to individual staff members; access to a key is required for authenticated email communication among these parties. The keys are stored on individual employee laptops. Because of the increased level of risk surrounding storage on portable devices (and the high frequency of international travel of staff and their laptops), JAS assumed 99% availability of these resources equating to approximately 3.5 days of downtime per year.

5.5 Dependence on Staff

ICANN/IANA processes are highly dependent on the availability and successful performance of a small number of expert staff. The manual system requires a significant amount of rekeying and as such is vulnerable to rekey (copy/paste) errors, and historically this failure mode has been the most significant root cause of error.

Similarly, portions of the process are somewhat subjective and depend on interpretation, judgment, historical perspective, and institutional knowledge of ICANN/IANA staff.

JAS made several assumptions concerning staff: while average turnover for IT positions in large metropolitan areas is just under four years,[3] we assumed ICANN/IANA positions turnover every 5.5 years due to the historically high degree of employee loyalty, low turnover, and attractive culture. We assumed combined rekey and judgment errors at a rate of 0.5%, commensurate with historical rates. We also assumed a 0.01% chance of an employee intentionally introducing error or unavailability into the system.[4]

5.6 Dependence on Physical Locations

All but one of ICANN/IANA's critical staff reside in the greater Los Angeles area and have their office at ICANN Headquarters (HQ) in Marina del Ray. To the best of JAS' knowledge, all ICANN-IT live operations are in facilities in the greater Los Angeles area with backup storage (but not operations) facilities elsewhere in the U.S. As such, significant disruption in the greater Los Angeles area will result in cascading failures affecting the majority of ICANN/IANA resources.

[2] ***Guarding our Future; Protecting our Nation's Critical Infrastructure.*** Toffler Associates. <http://www.toffler.com/images/IN%20-%20Guarding%20Our%20Future%20final%20081108.pdf> (Report commissioned by the U.S. Department of Homeland Security Office of Infrastructure Protection). 2008. Page 19.

[3] ***U.S. Market Watch: Recession Won't Protect IT Organizations From Employee Turnover***, Gartner Report, 18 August, 2009. Subscription only.

[4] These estimates were driven by industry vertical and geographic averages and do not factor in actual employee demographic data which was not made available to JAS.

6 Analysis

The combination of a low volume, highly manual process and a small number of highly capable and trusted staff, have resulted in a process that is both secure and resilient. However, this "brute force" approach comes at the expense of scalability and sustainability. ICANN/IANA's automated process implementation is designed to address these weaknesses by reducing the dependency on human rekeying and automating portions of the process to increase scalability. In addition, the IANA department is moving to "professionalize" their business process, a topic captured and discussed in Section 6.6. Maturing the overall process, particularly by increasing documentation and overall formality, will have a positive impact on process sustainability and resiliency.

As the IANA department is lacking specific guidance on the level of acceptable risk, it is impossible to know precisely which risks are managed properly and which are not. For example, is a degradation of process capacity acceptable during continuity operations? If so, to what level? Is it acceptable to rely on partners - namely VeriSign and NTIA - to detect errors and prevent propagation into the root zone, or is the expectation that IANA produce completely error-free output?

Based on discussion with ICANN/IANA staff and JAS' own familiarity with ICANN, we offer the following thesis concerning IANA's risk governance:

> *The ICANN/IANA root zone change process is an important and highly visible process requiring high levels of security and resiliency. TLD operators depend on the process to keep their domains operating, and ICANN faces significant reputational risk should the process produce an error or be unavailable for more than several days. During continuity operations, some reduction in process capacity is acceptable as long as the IANA department is able to continue processing priority submissions. ICANN expects the IANA department to produce outputs devoid of intentional and unintentional errors to their partners VeriSign and NTIA.*

If ICANN Management subscribes to this thesis, the following assessment of overall risk posture holds. If ICANN Management has a differing mandate regarding the IANA department's risk posture, the following assessment would need to be revisited.

Risk Grouping	Overall Adequacy of Risk Management	Mitigating Factors
Unintentional human error	Properly managed	Expert staff, low turnover, workload, RZMS
Intentional human error / Insider Threat	Under-managed	High loyalty, strong culture, low turnover, three party approval process, RZMS
IT Systems	Under-managed	Expert staff, low turnover
Resource disruption / destruction	Under-managed	Expert staff, process flexibility, workload
RZMS Project management / governance	Under-managed	Good working relationship with outsourced development firm

Table 2: Risk Management and Mitigation by Risk Grouping

6.1 Unintentional Human Error

ICANN/IANA's RZMS system almost entirely removes the need to rekey, dramatically reducing the exposure to unintentional rekey errors. Judgment errors are managed due to expert staff and low turnover, and a strong positive culture within ICANN/IANA. Historical error rates in this category are extremely low and trending downward.

6.2 Intentional Human Error / Insider Threat

There are no formal controls in place to manage the insider threat. There is no formal key employee program, and key employees are not subject to more stringent hiring/employment vetting requirements than other ICANN employees. While logging and audit functions are technically available, there is no formal audit/review regime. Superusers are technically capable of modifying logs. As such, a malicious insider could operate nearly unchecked within the IANA department and cause errors to be output to ICANN/IANA partners. While it is extremely probable that errors output from ICANN/IANA would be caught by partners prior to implementation in the root zone file, ICANN risks reputational risk in such a scenario and as such desires to manage this risk.

6.3 IT Systems

Dependency on critical resources are discussed in detail in Section 4. There are no formal controls in place to manage the risks exposed by dependence on several IT systems. The IANA department has no service level agreement with ICANN-IT, and has limited visibility into and influence over their operations, however this is coordinated at the ICANN senior management level. No formal service level monitoring is taking place. Functioning IT systems are critical to the IANA department's ability to complete the process; loss of these systems would result in significant and unacceptable process impairment.

6.4 Resource Disruption / Destruction

Dependency on critical resources are discussed in detail in Section 4. There are no formal business continuity plans in place, although ICANN/IANA is currently in the process of continuity planning. Without a continuity plan and exercise/drill regime, it is probable that the root zone change process would devolve into a completely ad-hoc, manual effort in the face of a significant resource disruption.

6.5 RZMS Project Management / Governance

The current informal approach to RZMS project management exposes several risks, as discussed in Recommendation 3 (see Section 7). Unclear security, stability, and resiliency requirements could lead to an implementation that is not commensurate with the criticality of this IT system. Critical IT systems are typically architected from the ground-up to be highly resilient, redundant, and to implement strong security functionality. When development of such systems is outsourced, extensive requirements enable effective project management by aligning the expectations. Absent a requirements-driven software development process, significant risks emerge that endanger the success of the entire project.

6.6 Risk Management Process Maturity

ICANN/IANA is moving to professionalize their business processes, which includes attention to documentation, sustainability, and formal risk management. One useful metric to measure the IANA department's progress in this regard is the Capability Maturity Model (CMM) that identifies five levels of process maturity:

1. Initial (chaotic, ad hoc): The starting point for an organically-defined process.
2. Repeatable: The process is able to be used repeatedly, with roughly repeatable outcomes.
3. Defined: The process is defined/confirmed as a standard business process.
4. Managed: The process is monitored and managed according to predetermined metrics.
5. Optimized: Process management includes deliberate process optimization/improvement.

The IT Governance Institute has published several Capability Maturity Models with respect to specific risk management disciplines.[5] Based on JAS' analysis of the root zone management process, we believe the IANA department is currently operating between CMM level two and three with respect to risk management. The levels are further defined by ITGI as:

Level 2 (Repeatable)

> *Worst-case loss scenarios are the focus of discussions, although the driving factors for those scenarios may not be understood. Individuals assume responsibility for both risk evaluation and risk response. Some planned risk analysis occurs, but practitioners make major assumptions about the contributing factors for risk. Dependency analysis and scenario analysis are ad hoc and focus on only a limited number of business activities. Minimum skill requirements are identified for critical areas of data collection, risk analysis and risk profiling. Functional and IT silo-specific risk analysis approaches and tools exist but are based on solutions developed by key individuals. (Credit: ITGI)*

Level 3 (Defined)

> *There is an emerging understanding of risk fundamentals. Gaps between IT-related risk and opportunity and overall risk appetite are being recognized. Responsibility and accountability for*

[5] ***Enterprise Risk: Identify, Govern, and Manage IT Risk. The IT Risk Framework.*** IT Governance Institute. 3 February 2009.

> *key risk evaluation practices are defined and process owners have been identified. The capability is in place to evaluate IT risk on an enterprise-wide basis alongside other risk types. Dependency analysis and scenario analysis procedures are defined and performed across multiple business activities, business lines and products. Skill requirements are defined and documented for all enterprise risk areas, with full consideration of data collection, risk analysis and profiling. Data collection tools generally adhere to defined standards and distinguish between threat events, vulnerability events and loss events. (Credit: ITGI)*

JAS believes that CMM level 4 (Managed) is a reasonable and appropriate medium-term goal with continuing attention to process formality, documentation, and systemic risk management.

7 Recommendations

RECOMMENDATION 1: Clarify overall Risk Governance. Lack of clarity surrounding the level of risk ICANN is willing to accept makes it difficult for ICANN/IANA Management to manage risk properly. ICANN Directors and Senior Management must specify the degree of acceptable risk and desired posture during business continuity events and resource the business managers appropriately. For example, a very low tolerance for the introduction of intentional errors will result in requirements for certified high security system implementations, multifactor personnel authentication, high physical security, multiple levels of manual review and authorization, extensive logging and auditing, etc. Similarly, if the desire is to maintain full processing capacity and generally "not miss a beat" during business continuity operations, the result will be multiple redundant "hot" sites, a physically distributed staff of trained and certified employees, multiple resilient communications paths between partners, high availability IT systems, highly disciplined IT operations, tight Service Level Agreements, etc. The level of acceptable risk drives the implementation of controls and compliance mechanisms, and of course cost.

Absent this clarity, portions of this analysis are based on ICANN/IANA and JAS' best understanding of the appropriate risk posture for the root zone management process. These assumptions are fully described in Section 5.

RECOMMENDATION 2: Clarify operational relationship with ICANN-IT. ICANN's IANA department has critical dependencies on multiple systems operated by ICANN's IT department, namely email, the RT ticket system, and the new RZMS system. Depending on the level of risk ICANN/IANA is willing to accept, differing levels of service will be required from ICANN-IT. This relationship must be discussed, mutually agreed upon, and memorialized in the form of business continuity operational procedures, security, and system administration requirements.

RECOMMENDATION 3: Formalize governance of the development of the new RZMS system. The new RZMS system is a critical component of the new automated root zone management process. Significant parts of the development of this system are being provided through an international supply chain with limited specification formality. No formal requirements exist regarding the security and resiliency of these systems, making it impossible to know whether the system has been built to specification. JAS recommends formal requirements around security and resiliency be provided to the developers, and ICANN/IANA rigorously test and audit the delivered product against these requirements.

RECOMMENDATION 4: Formalize policies regarding key employees including training and certification programs, employee screening, and the use of "two person rules." ICANN/IANA is highly dependent on the availability, judgment, and historical/institutional knowledge of a small number of highly specialized critical employees. However, limited formality is in place to manage the risks presented by this dependency. As Information Technology professionals in large metropolitan areas are especially vulnerable to churn, and critical employees are uniquely positioned to negatively affect system integrity and availability (the "insider threat"), this is a relevant risk necessitating formal controls and compliance mechanisms. Moreover, it is reasonable to assume that the IANA department will need to scale-up operations at some point in the future to support root zone expansion; this scale-up will almost certainly require the expansion of the critical employee pool.

JAS recommends a formal training and certification program covering the job responsibilities of employees involved in the root zone change process. These programs will improve process documentation, scalability and resiliency of the IANA department's human resources, and enable a greater degree of capacity planning.

Because of the high degree of trust ICANN/IANA must have in their employees, ICANN is especially susceptible to the insider threat. System administrators and superusers within the IANA department and ICANN-IT almost certainly have unique abilities to forge/alter requests, modify logs, and perform other malicious activities that can have significant impact on the availability and accuracy of the root zone change process. While present employees are certainly loyal and trustworthy, unfortunately, it is not safe to assume this will always be the case. As such, JAS recommends a formal program to vet potential new hires, and to periodically re-vet employees over time. Such a vetting program would include screening for illegal drugs, evaluation of consumer credit, and psychiatric evaluation, which are all established risk factors for unreliable and/or malicious insider activity and are routinely a part of employee screening in government and critical infrastructure providers.

Finally, JAS recommends implementing "two-person rules" at critical gates in the root zone change process. A two-person rule requires two distinct individuals to "sign-off" on a change before it is committed to the system, providing a valuable second set of eyes as well as a solid audit trail. Two-person rules are highly effective controls against both accidental and intentional human errors.

RECOMMENDATION 5: Increase physical distribution of critical resources. Currently, nearly all critical resources are physically located in the greater Los Angeles area. While it is feasible that highly manual continuity operations could continue even in the face of a major regional event, the significant reduction in process capacity coupled with the probable increase in root zone change requests as a result of such an event would have a negative impact both on process throughput and error rate. Exacerbating the lack of resource distribution, the Los Angeles metropolitan area is burdened with a higher than average level of risk to a wide range of both natural and manmade disruptions. As such, JAS recommends reducing the dependence on the greater Los Angeles area to the extent required to implement ICANN's risk governance guidance (Recommendation 1).

RECOMMENDATION 6: Increase resiliency of communications with partners. The root zone management process requires tight communication and coordination between ICANN/IANA, VeriSign, and the NTIA. Presently, this communication leverages the Internet (email), and the public telephone system with email being the primary mechanism. The automated implementation of the process shifts almost all ICANN-VeriSign communications to the Extended Provisioning Protocol (EPP), which leverages Internet connectivity between the IANA department's RZMS system and VeriSign's systems. This introduces significant dependence on a functioning Internet connection between the RZMS system - physically located in the Greater Los Angeles area - and VeriSign's systems - physically located in Northern Virginia. Similarly, the ICANN-NTIA communications leverage Internet email connectivity between Los Angeles and Washington, DC. These dependencies are significant to the point that a large-scale Internet disruption affecting traffic between the East and West Coasts of the United States would have a debilitating effect on ICANN/IANA's ability to execute the process. Such a large-scale Internet disruption, particularly in conjunction with other stressors such as a natural disaster, is not unforeseeable; several sources assign the probability of such an event at up to 20% in the next 20 years (see Section 4.4.4).

JAS recommends increasing the resiliency of communications between the three critical parties. The easiest and most cost effective way to accomplish this may be for ICANN/IANA to staff a satellite office physically proximate to both partners in the Greater Washington, DC area. A physically proximate office would enable cost effective alternate communications between the three parties including private telecommunications circuits and in-person meetings. It is also unlikely that resources in both the Los Angeles and Washington offices would be simultaneously affected by an incident requiring continuity operations.

RECOMMENDATION 7: Increase resiliency of communications with employees and customers. Non-standard operations during times of stress require resilient communications among ICANN/IANA employees and with customers. Even though highly manual operation is possible, the requests must first get to ICANN/IANA employees, and these employees must be capable of communicating among themselves, their partners, the requestor, and potentially with ICANN/IANA senior management. Currently, all inbound requests have a dependency on resources in the greater Los Angeles area: email and Internet IT systems as well as telephone communications, FAX and postal mail delivery all leverage resources in LA (it is probable that calls to the ICANN/IANA 3rd party answering service in the United Kingdom are routed through Los Angeles). JAS recommends increasing communication resiliency by procuring satellite telephones and GETS/WPS[6] priority telephone service for critical employees, and by publishing to customers backup contact instructions that do not have a dependency on the Los Angeles area. For example, landline telephone and FAX numbers for the UK answering service and/or an East Coast ICANN/IANA office.

RECOMMENDATION 8: Exercise business continuity operations regularly. While the nature of the root zone change process facilitates highly manual, human-oriented emergency continuity operations, JAS recommends business continuity operations be formalized and regularly exercised. Exercises are a useful compliance mechanism to assure management that the controls in place are effective.

One typical exercise routine is to artificially fail-over to continuity operations/sites on a regular basis. For example, several sophisticated entities in the banking and finance sector regularly process 80% of their daily transactions at the primary site and 20% at a backup facility. Similarly, other enterprises activate continuity operations on a regular basis to handle the full regular load for a day, for example the second Thursday of each month. As continuity operations/policies tend to get "stale" very quickly, the advantage of these approaches is that the firm is always aware of their continuity posture and relatively assured it will be available in a pinch.

[6] http://gets.ncs.gov and http://wps.ncs.gov

While the operation of ICANN's IT department is beyond the scope of this analysis, JAS recommends that the IANA department work with ICANN-IT to regularly test backup/restore operations for critical IANA systems.

RECOMMENDATION 9: Formalize multiple service levels. Whether formal or not, most request-driven business processes like the root zone change process have multiple levels of service. "Normal" requests are submitted using the standard channels and handled roughly in sequence. "Emergency" requests may have a formal priority submission channel and/or markings, or may receive priority handling informally by calling a known contact, appealing to a manager, asking for a "favor," or otherwise requesting an expedite out of band. JAS' experience is that these informal priority channels always exist, are nearly impossible to stamp-out, and that inconsistent service levels realized through these priority channels are often a source of periodic tension. JAS has found that formalized priority service levels offer an important triage in time of stress, particularly because stressors such as natural disasters often cause an increase in requests while reducing processing capacity. JAS recommends formalizing priority handling by implementing normal and expedited service levels and publishing commensurate service levels.

7.1 Key Risk Indicators (KRIs)

JAS recommends that ICANN begin formal monitoring and reporting on the risk posture of the ICANN/IANA root zone management process. Key Risk Indicators (KRIs) are qualitative metrics that in aggregate capture the overall risk posture of a process. KRIs can be defined as parameters that show that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk tolerance. KRIs allow management to document and analyze trends, and provides a forward-looking perspective, signaling required actions before the risk actually becomes a loss. In practice, KRIs are used in reporting or in dashboards. They not only warn about and flag possible issues or areas that contain risks, but (if selected well) they can provide management with a holistic overview of the current risk management situation.

With respect to the root zone management process, JAS recommends the following KRIs:

Number of Certified Staff

JAS has recommended a formal employee training and certification program to manage the risks associated with key personnel. The number of certified staff members at any given time provides a metric to monitor the human aspect of the process resiliency. A low number of certified staff raises the alarm as the impact of unexpected employee unavailability or turnover would be high. Maintaining the number of certified staff within an acceptable band goes a long way toward managing the key employee risks.

Two-Person Rule Signoffs

Monitoring the number and diversity of two-person rule signoffs on an ongoing basis also provides insight into the key employee risks.

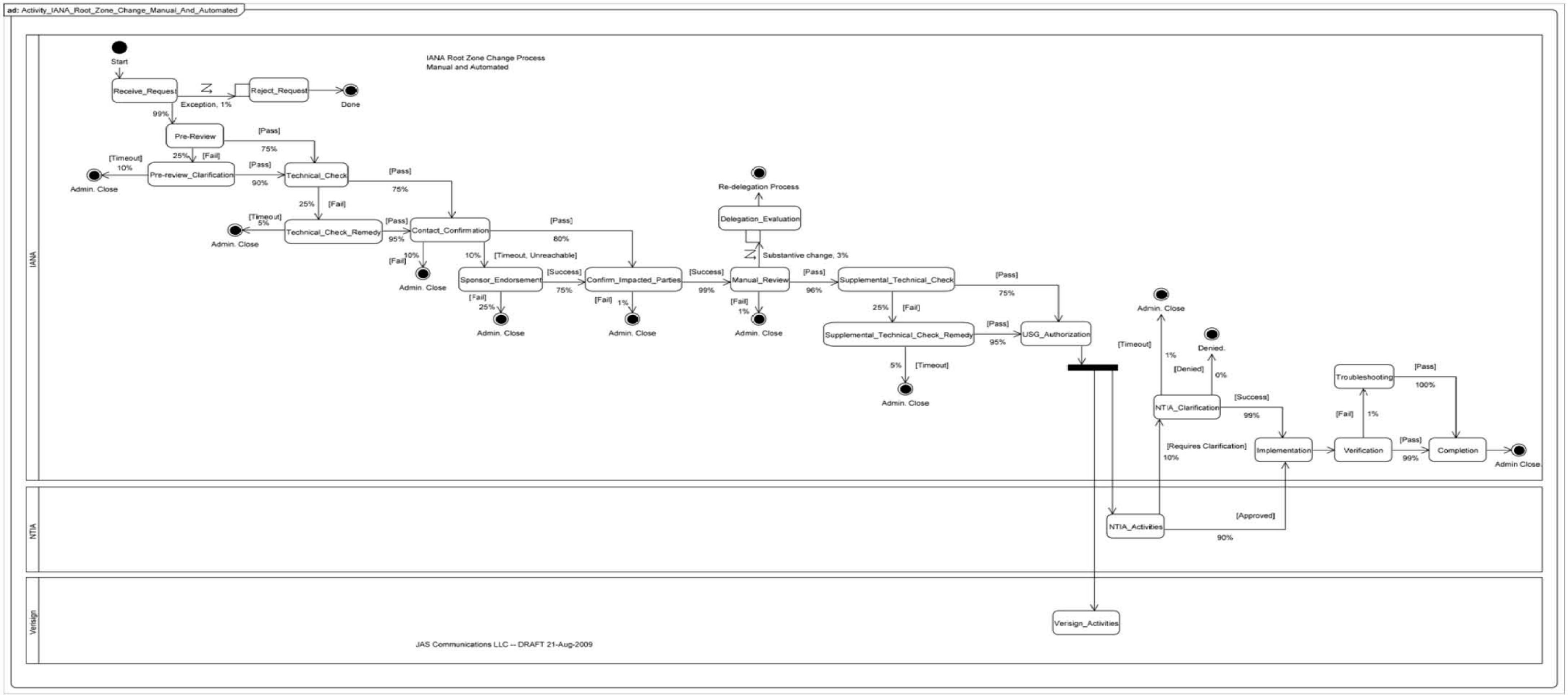
IT Systems Availability/SLA

Ongoing communications and coordination with ICANN-IT will provide insight into the state of the IANA department's IT system dependencies and comfort that IT systems are well administered.

Results of Exercises/Drills

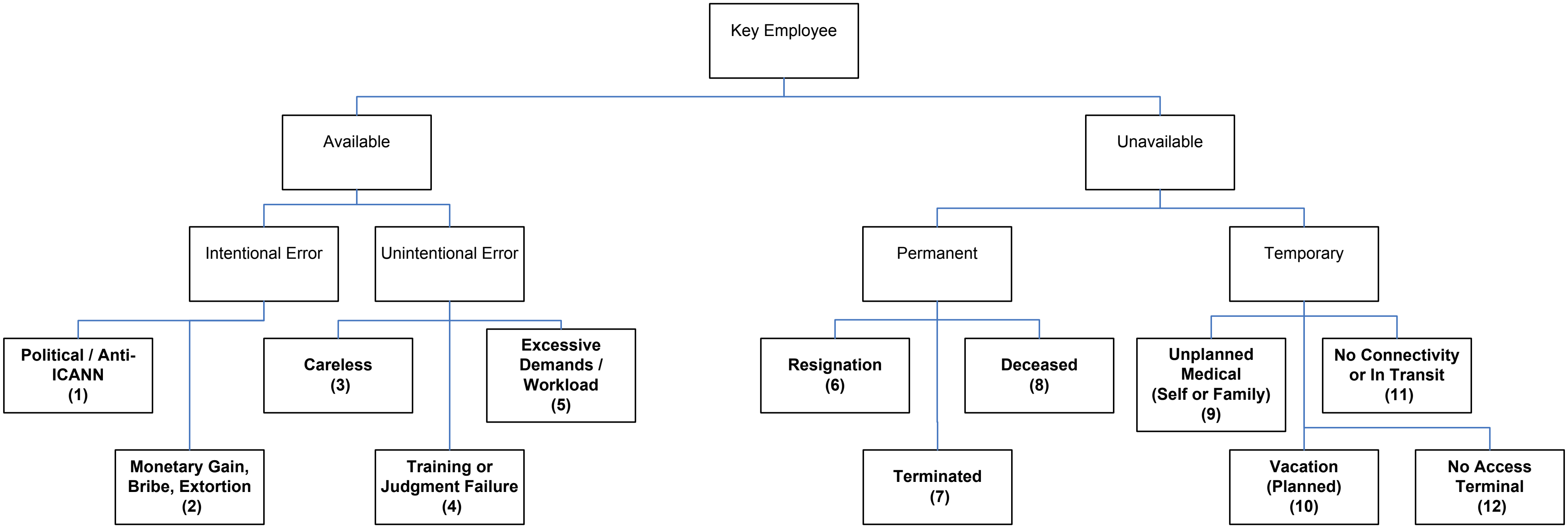
While less quantitative, the results of business continuity exercises/drills over time provide insight into the evolving state and maturity of ICANN/IANA's continuity posture.

8 Appendix A: Process Activity Diagram

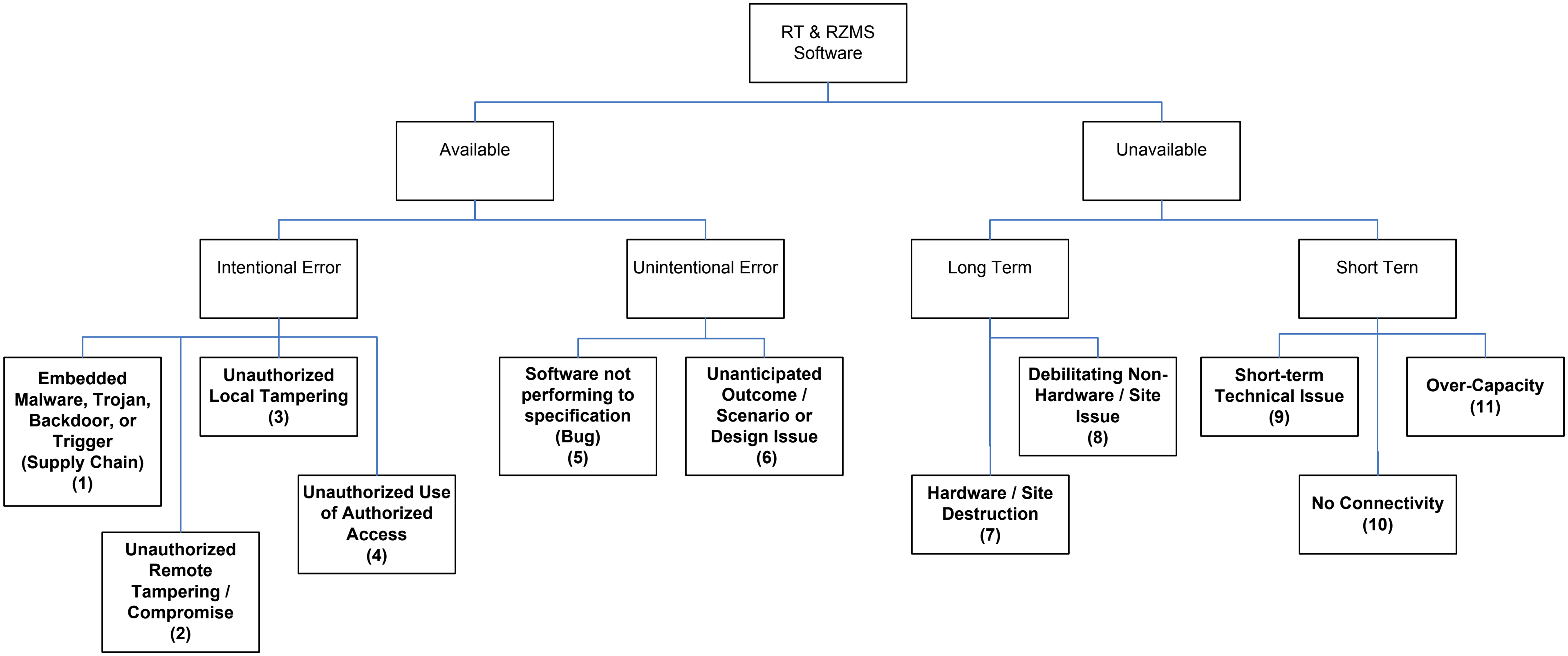


9 Appendix B: Selected Critical Resource Attack Trees

Critical Resources (1)


Key Employee
Available
Unavailable
Intentional Error
Unintentional Error
Permanent
Temporary
Political / Anti-ICANN (1)
Careless (3)
Excessive Demands / Workload (5)
Resignation (6)
Deceased (8)
Unplanned Medical (Self or Family) (9)
No Connectivity or In Transit (11)
Monetary Gain, Bribe, Extortion (2)
Training or Judgment Failure (4)
Terminated (7)
Vacation (Planned) (10)
No Access Terminal (12)

Critical Resources (2)



RT & RZMS Software

Available

Unavailable

Intentional Error

Unintentional Error

Long Term

Short Tern

Embedded Malware, Trojan, Backdoor, or Trigger (Supply Chain) (1)

Unauthorized Remote Tampering / Compromise (2)

Unauthorized Local Tampering (3)

Unauthorized Use of Authorized Access (4)

Software not performing to specification (Bug) (5)

Unanticipated Outcome / Scenario or Design Issue (6)

Hardware / Site Destruction (7)

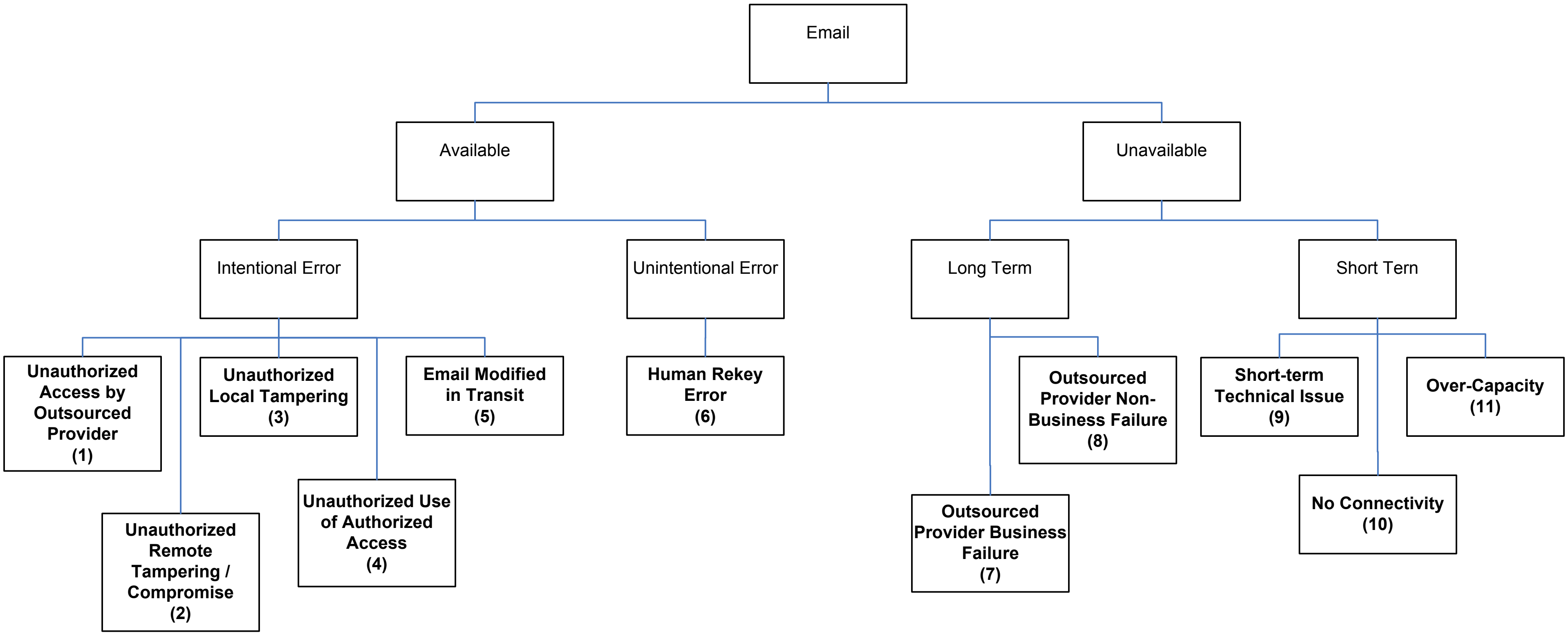
Debilitating Non-Hardware / Site Issue (8)

Short-term Technical Issue (9)

No Connectivity (10)

Over-Capacity (11)

Critical Resources (3)


Email
Available
Unavailable
Intentional Error
Unintentional Error
Long Term
Short Tern
Unauthorized Access by Outsourced Provider (1)
Unauthorized Remote Tampering / Compromise (2)
Unauthorized Local Tampering (3)
Unauthorized Use of Authorized Access (4)
Email Modified in Transit (5)
Human Rekey Error (6)
Outsourced Provider Business Failure (7)
Outsourced Provider Non-Business Failure (8)
Short-term Technical Issue (9)
No Connectivity (10)
Over-Capacity (11)

10 Appendix C: Path Enumeration

This appendix provides an enumeration of each possible path through the process activity diagram in Appendix A. The paths are probability weighted at each gate, and an overall path probability is calculated, which shows the probability of that path being followed all the way through. Probability weightings for each node exit gate were provided by ICANN/IANA.

For each node "visit" in this enumeration, a section appears similar to the following: "Receive_Request(0.99, Success) ->". Referring to the diagram in Appendix A, this indicates that the enumeration is currently visiting the Receive_Request node and has followed the "Success" gate out, which has probability of 99%.

There are 124 paths and 372 activity visits for 1.00000 total probability.

1: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.283]

2: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.00286]

3: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.0311]

4: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.000314]

5: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.01, Denied) -> Admin_Close(END) [Path Probability=0.000318]

6: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.0896]

7: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.000905]

8: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.00986]

9: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=9.96e-05]

10: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.01, Denied) -> Admin_Close(END) [Path Probability=0.000101]

11: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.05, Timeout) -> Admin_Close(END) [Path Probability=0.00529]

12: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.01, Fail) -> Admin_Close(END) [Path Probability=0.00441]

13: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.03, Exception) -> Delegation_Evaluation(1.0, ALL) -> Admin_Close(END) [Path Probability=0.0132]

14: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.01, Fail) -> Admin_Close(END) [Path Probability=0.00446]

15: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.0265]

16: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.000268]

17: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.00292]

18: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=2.95e-05]

19: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.01, Denied) -> Admin_Close(END) [Path Probability=2.98e-05]

20: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.00840]

21: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=8.48e-05]

22: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.000924]

23: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=9.33e-06]

24: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.01, Denied) -> Admin_Close(END) [Path Probability=9.43e-06]

25: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.05, Timeout) -> Admin_Close(END) [Path Probability=0.000496]

26: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.01, Fail) -> Admin_Close(END) [Path Probability=0.000413]

27: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.03, Exception) -> Delegation_Evaluation(1.0, ALL) -> Admin_Close(END) [Path Probability=0.00124]

28: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.01, Fail) -> Admin_Close(END) [Path Probability=0.000418]

29: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.25, Fail) -> Admin_Close(END) [Path Probability=0.0139]

30: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Fail) -> Admin_Close(END) [Path Probability=0.0557]

31: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.0896]

32: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.000905]

33: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.00986]

34: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=9.96e-05]

35: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.01, Denied) -> Admin_Close(END) [Path Probability=0.000101]

36: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.0284]

37: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.000287]

38: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.00312]

39: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=3.15e-05]

40: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.01, Denied) -> Admin_Close(END) [Path Probability=3.18e-05]

41: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.05, Timeout) -> Admin_Close(END) [Path Probability=0.00168]

42: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.01, Fail) -> Admin_Close(END) [Path Probability=0.00140]

43: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.03, Exception) -> Delegation_Evaluation(1.0, ALL) -> Admin_Close(END) [Path Probability=0.00419]

44: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.01, Fail) -> Admin_Close(END) [Path Probability=0.00141]

45: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.00840]

46: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=8.48e-05]

47: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.000924]

48: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=9.33e-06]

49: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.01, Denied) -> Admin_Close(END) [Path Probability=9.43e-06]

50: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.00266]

51: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=2.69e-05]

52: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.000293]

53: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=2.96e-06]

54: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.01, Denied) -> Admin_Close(END) [Path Probability=2.99e-06]

55: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.05, Timeout) -> Admin_Close(END) [Path Probability=0.000157]

56: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.01, Fail) -> Admin_Close(END) [Path Probability=0.000131]

57: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.03, Exception) -> Delegation_Evaluation(1.0, ALL) -> Admin_Close(END) [Path Probability=0.000393]

58: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.01, Fail) -> Admin_Close(END) [Path Probability=0.000132]

59: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.25, Fail) -> Admin_Close(END) [Path Probability=0.00441]

60: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Fail) -> Admin_Close(END) [Path Probability=0.0176]

61: Receive_Request(0.99, Success) -> Pre_Review(0.75, Pass) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.05, Timeout) -> Admin_Close(END) [Path Probability=0.00928]

62: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.0849]

63: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.000857]

64: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.00934]

65: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=9.43e-05]

66: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.01, Denied) -> Admin_Close(END) [Path Probability=9.53e-05]

67: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.0269]

68: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.000272]

69: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.00296]

70: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=2.99e-05]

71: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.01, Denied) -> Admin_Close(END) [Path Probability=3.02e-05]

72: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.05, Timeout) -> Admin_Close(END) [Path Probability=0.00159]

73: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.01, Fail) -> Admin_Close(END) [Path Probability=0.00132]

74: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.03, Exception) -> Delegation_Evaluation(1.0, ALL) -> Admin_Close(END) [Path Probability=0.00397]

75: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.01, Fail) -> Admin_Close(END) [Path Probability=0.00134]

76: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.00796]

77: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=8.04e-05]

78: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.000875]

79: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=8.84e-06]

80: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.01, Denied) -> Admin_Close(END) [Path Probability=8.93e-06]

81: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.00252]

82: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=2.55e-05]

83: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.000277]

84: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=2.80e-06]

85: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.01, Denied) -> Admin_Close(END) [Path Probability=2.83e-06]

86: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.05, Timeout) -> Admin_Close(END) [Path Probability=0.000149]

87: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.01, Fail) -> Admin_Close(END) [Path Probability=0.000124]

88: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.03, Exception) -> Delegation_Evaluation(1.0, ALL) -> Admin_Close(END) [Path Probability=0.000372]

89: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.01, Fail) -> Admin_Close(END) [Path Probability=0.000125]

90: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.25, Fail) -> Admin_Close(END) [Path Probability=0.00418]

91: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.75, Pass) -> Contact_Confirmation(0.1, Fail) -> Admin_Close(END) [Path Probability=0.0167]

92: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.0269]

93: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.000272]

94: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.00296]

95: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=2.99e-05]

96: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.01, Denied) -> Admin_Close(END) [Path Probability=3.02e-05]

97: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.00851]

98: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=8.60e-05]

99: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.000936]

100: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=9.46e-06]

101: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.01, Denied) -> Admin_Close(END) [Path Probability=9.55e-06]

102: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.05, Timeout) -> Admin_Close(END) [Path Probability=0.000503]

103: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.01, Fail) -> Admin_Close(END) [Path Probability=0.000419]

104: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.03, Exception) -> Delegation_Evaluation(1.0, ALL) -> Admin_Close(END) [Path Probability=0.00126]

105: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.8, Pass) -> Confirm_Impacted_Parties(0.01, Fail) -> Admin_Close(END) [Path Probability=0.000423]

106: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.00252]

107: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=2.55e-05]

108: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.000277]

109: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=2.80e-06]

110: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.75, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.01, Denied) -> Admin_Close(END) [Path Probability=2.83e-06]

111: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=0.000798]

112: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.9, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=8.06e-06]

113: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.99, Pass) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=8.78e-05]

114: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.99, Pass) -> Implementation(1.0, ALL) -> Verification(0.01, Fail) -> Troubleshooting(1.0, ALL) -> Completion(1.0, ALL) -> Admin_Close(END) [Path Probability=8.87e-07]

115: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.95, Pass) -> USG_Authorization(0.1, Requires_Clarification) -> NTIA_Clarification(0.01, Denied) -> Admin_Close(END) [Path Probability=8.96e-07]

116: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.96, Pass) -> Supplemental_Techncal_Check(0.25, Fail) -> Supplemental_Techncal_Check_Remedy(0.05, Timeout) -> Admin_Close(END) [Path Probability=4.71e-05]

117: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.01, Fail) -> Admin_Close(END) [Path Probability=3.93e-05]

118: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.99, Pass) -> Manual_Review(0.03, Exception) -> Delegation_Evaluation(1.0, ALL) -> Admin_Close(END) [Path Probability=0.000118]

119: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.75, Pass) -> Confirm_Impacted_Parties(0.01, Fail) -> Admin_Close(END) [Path Probability=3.97e-05]

120: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Timeout_Unreachable) -> Sponsor_Endorsement(0.25, Fail) -> Admin_Close(END) [Path Probability=0.00132]

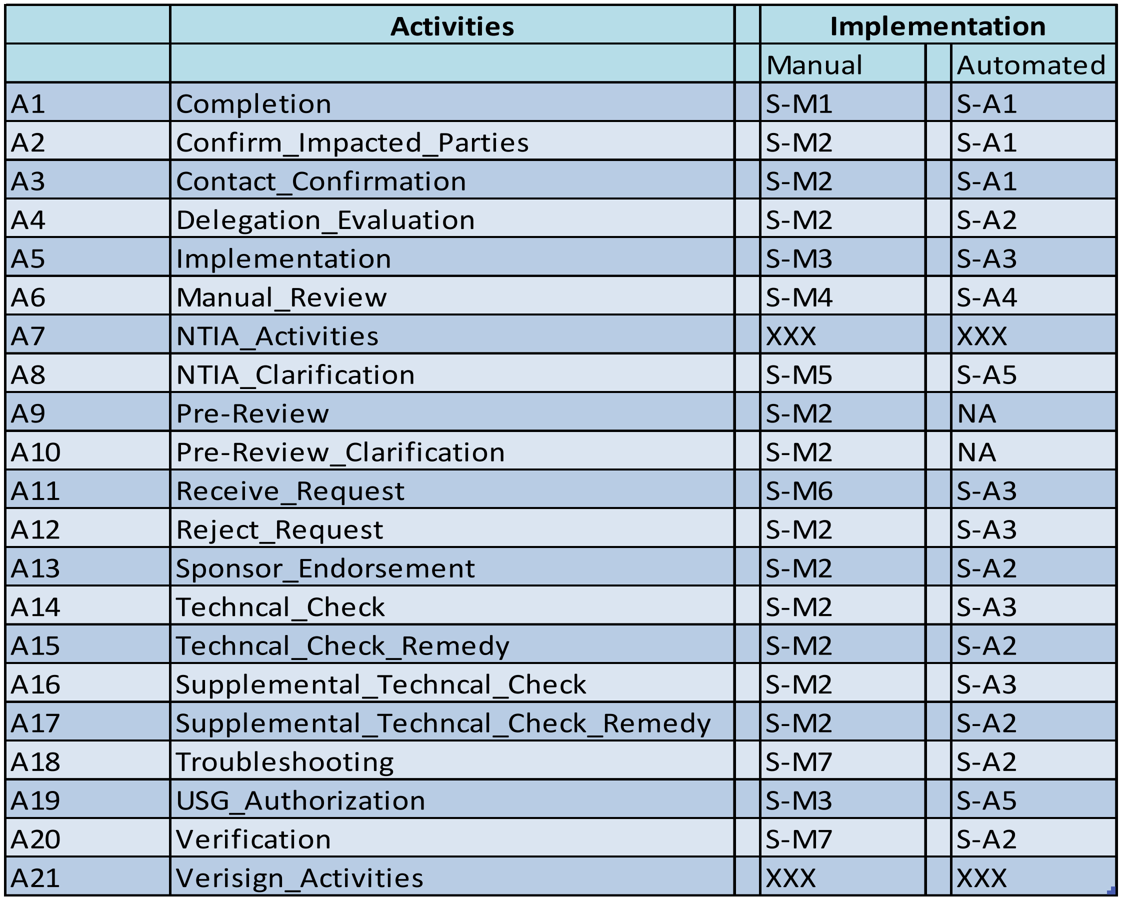
121: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.95, Pass) -> Contact_Confirmation(0.1, Fail) -> Admin_Close(END) [Path Probability=0.00529]

122: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.9, Success) -> Techncal_Check(0.25, Fail) -> Techncal_Check_Remedy(0.05, Timeout) -> Admin_Close(END) [Path Probability=0.00278]

123: Receive_Request(0.99, Success) -> Pre_Review(0.25, Fail) -> Pre_Review_Clarification(0.1, Timeout) -> Admin_Close(END) [Path Probability=0.0248]

124: Receive_Request(0.01, Exception) -> Reject_Request(1.0, ALL) -> Admin_Close(END) [Path Probability=0.0100]

11 Appendix D: Resource Tables and Dependency Equations



	Activities		Implementation		
			Manual		Automated
A1	Completion		S-M1		S-A1
A2	Confirm_Impacted_Parties		S-M2		S-A1
A3	Contact_Confirmation		S-M2		S-A1
A4	Delegation_Evaluation		S-M2		S-A2
A5	Implementation		S-M3		S-A3
A6	Manual_Review		S-M4		S-A4
A7	NTIA_Activities		XXX		XXX
A8	NTIA_Clarification		S-M5		S-A5
A9	Pre-Review		S-M2		NA
A10	Pre-Review_Clarification		S-M2		NA
A11	Receive_Request		S-M6		S-A3
A12	Reject_Request		S-M2		S-A3
A13	Sponsor_Endorsement		S-M2		S-A2
A14	Techncal_Check		S-M2		S-A3
A15	Techncal_Check_Remedy		S-M2		S-A2
A16	Supplemental_Techncal_Check		S-M2		S-A3
A17	Supplemental_Techncal_Check_Remedy		S-M2		S-A2
A18	Troubleshooting		S-M7		S-A2
A19	USG_Authorization		S-M3		S-A5
A20	Verification		S-M7		S-A2
A21	Verisign_Activities		XXX		XXX

Automated Process Implementation

S_A1 = "((RZMS && RT) && Internet_large_scale && (Exchange_Email && Email_MX))"

S_A2 = "((Keyman_1 || Keyman_2 || Keyman_3 || Keyman_4 || Keyman_5) && (RZMS && RT) && Internet_large_scale && (Exchange_Email && Email_MX) && Human_Judgement)"

S_A3 = "((RZMS && RT) && Internet_large_scale)"

S_A4 = "((Keyman_1 || Keyman_2 || Keyman_3 || Keyman_4 || Keyman_5) && Keyman_10 && (Exchange_Email && Email_MX) && Human_Judgement && (RZMS && RT))"

S_A5 = "((Keyman_1 || Keyman_2 || Keyman_3 || Keyman_4 || Keyman_5) && (RZMS && RT) && Internet_large_scale && (Exchange_Email && Email_MX) && Human_Judgement && Authorized_PGP_Key)"

Manual Process Implementation

S_M1 = "((Keyman_1 || Keyman_2 || Keyman_3 || Keyman_4 || Keyman_5) && (Exchange_Email && Email_MX) && RT)"

S_M2 = "((Keyman_1 || Keyman_2 || Keyman_3 || Keyman_4 || Keyman_5) && (Exchange_Email && Email_MX) && RT && Human_Rekey && Human_Judgement)"

S_M3 = "((Keyman_1 || Keyman_2 || Keyman_3 || Keyman_4 || Keyman_5) && (Exchange_Email && Email_MX) && RT && Authorized_PGP_Key && Human_Rekey)"

S_M4 = "((Keyman_1 || Keyman_2 || Keyman_3 || Keyman_4 || Keyman_5) && Keyman_10 && (Exchange_Email && Email_MX) && RT && Human_Rekey && Human_Judgement)"

S_M5 = "((Keyman_1 || Keyman_2 || Keyman_3 || Keyman_4 || Keyman_5) && (Exchange_Email && Email_MX) && RT && Human_Rekey && Human_Judgement && Authorized_PGP_Key)"

S_M6 = "((HQ_Phone_Fax_System || (Email_MX && RT) || (Paging_Service_UK && HQ_Phone_Fax_System) || (Paging_Service_UK && Mobile_Phone_Network) || HQ) && RT)"

S_M7 = "((Keyman_1 || Keyman_2 || Keyman_3 || Keyman_4 || Keyman_5) && (Exchange_Email && Email_MX) && RT && Human_Rekey && Human_Judgement && Authorized_PGP_Key && Any_SSH_Host)"

12 Appendix E: Process Dependency Analysis and Determination of Critical Resources

Through documentation review and structured interview sessions, JAS received from ICANN/IANA data sufficient to generate the artifacts in Appendices A - D and F. Dependency analysis and determination of critical Resources is accomplished through analysis of the paths through the UML Activity Diagram (Appendix A; path enumeration in Appendix C) and application of the resource availability formulas (Appendix D) at each node. Boolean Algebra determines the availability of the Activity at a specific node given one or more Resource failures. The result is a quantitative model of the business process.

In general, we analyze the model by failing resources and observing the impact on the ability to complete the process along the identified paths. Ability to complete a path with available resources is weighted by the probability of occurrence of that specific path. Additionally, resource failures may or may not cascade through resource dependencies. For example, a large-scale disruption in Los Angeles could affect several additional resources in that physical geography. In the JAS model, cascading failures are either absolute or follow a Gaussian distribution anchored with industry norms and various other data points. For example, assumptions regarding availability of telecommunications infrastructure, office space, human error rates, and compromise of insiders in various demographics appear in several places in this document. In addition, the Attack Trees in Appendix B factor into the quantitative model as well as our textual analysis of potential attack methodologies. Typically, a 1,000 iteration Monte Carlo analysis is sufficient to reveal the behavior of the model.

Factoring in the probability weighting of each path through the process and complex relationships between resource dependencies and individual business activities, this analysis permits a quantitative determination of the level of dependency on each given resource. The high level result is an ordering of resources by the level of dependency as shown in Table 1.

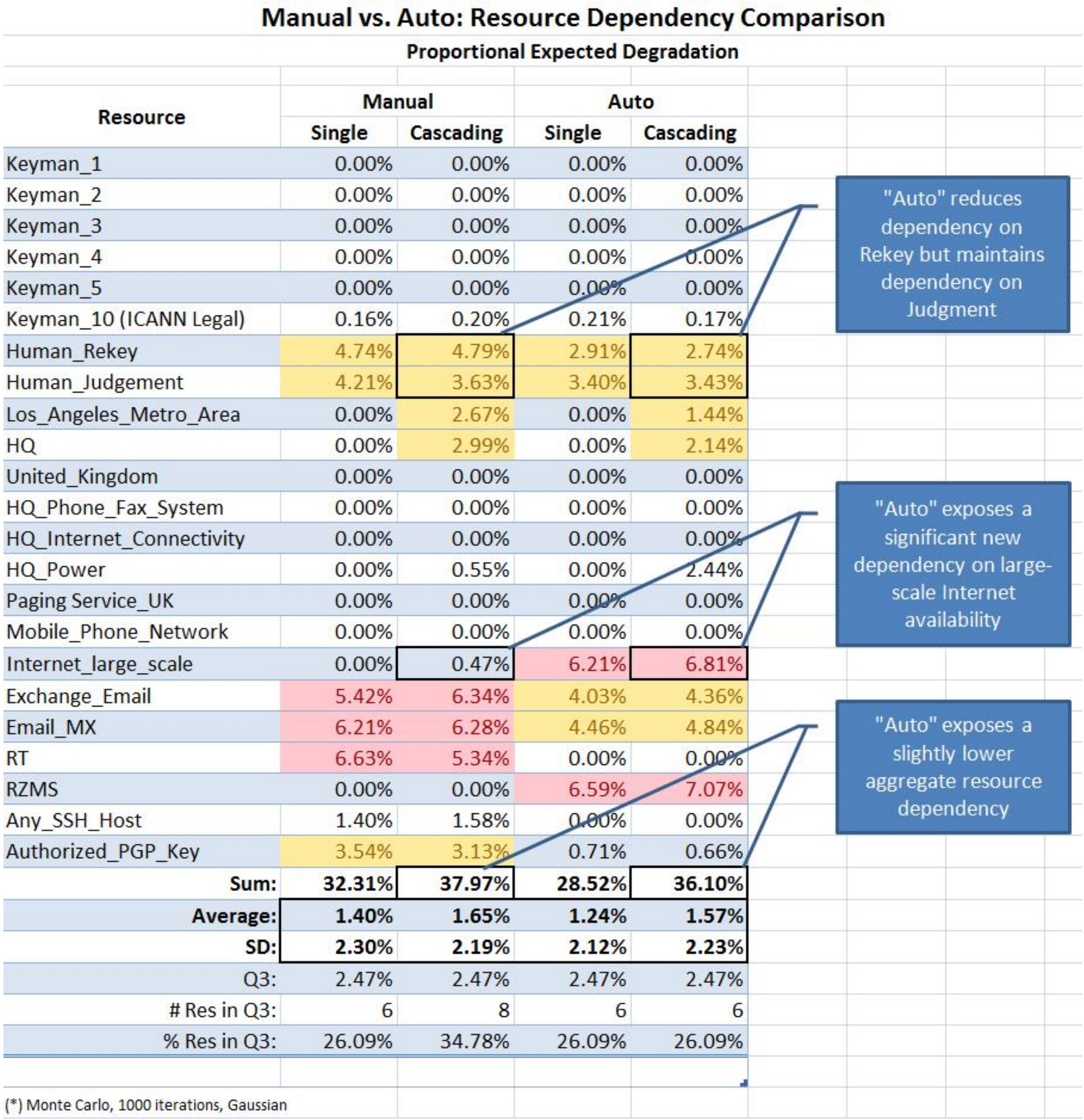
JAS ran the analysis for both the current "manual" process implementation and the anticipated "automated" process implementation. The activity diagram and path enumeration is identical for both processes; only the resource dependencies (expressed in Boolean Algebra equations) change between the implementations. The result is a quantitative comparison between process implementations.

At a lower level, the quantitative analysis outputs several datasets. The most instructive is a *Proportional Expected Degradation* analysis, which reveals the proportional contribution of a specific resource to an overall failure rate. This table can be seen in Appendix F. For the purpose of illustration, consider the Manual process implementation in a Cascading resource failure model (column 3). This column tells us that, if the overall failure rate were 37.97%, then failure of Exchange email would be responsible for 6.34% of that 37.97%. Refactoring, if the failure rate were 1%, the contribution of failures in Exchange email would be responsible for contributing 0.167% to that 1% overall rate.

This analysis quickly identifies critical resources, and allows a quantitative comparison between the process implementations. Note that individual personnel do not appear as critical in this analysis; while possibly counter-intuitive, this accurately reflects the depth of cross-trained personnel available to perform the tasks, and the fact that personnel are geographically distributed such that cascading resource failures do not affect all personnel simultaneously. For example, an event affecting Los Angeles does not affect all personnel. This behavior was confirmed during the 19-Jan-2010 continuity exercise.

The exception is Keyman 10 (ICANN Legal) who is a single point of failure, but only critically required for a very small and relatively improbable number of paths through the process.

13 Appendix F: Proportional Expected Degradation Analysis



Manual vs. Auto: Resource Dependency Comparison

Proportional Expected Degradation

Resource	**Manual**		**Auto**	
	Single	**Cascading**	**Single**	**Cascading**
Keyman_1	0.00%	0.00%	0.00%	0.00%
Keyman_2	0.00%	0.00%	0.00%	0.00%
Keyman_3	0.00%	0.00%	0.00%	0.00%
Keyman_4	0.00%	0.00%	0.00%	0.00%
Keyman_5	0.00%	0.00%	0.00%	0.00%
Keyman_10 (ICANN Legal)	0.16%	0.20%	0.21%	0.17%
Human_Rekey	4.74%	4.79%	2.91%	2.74%
Human_Judgement	4.21%	3.63%	3.40%	3.43%
Los_Angeles_Metro_Area	0.00%	2.67%	0.00%	1.44%
HQ	0.00%	2.99%	0.00%	2.14%
United_Kingdom	0.00%	0.00%	0.00%	0.00%
HQ_Phone_Fax_System	0.00%	0.00%	0.00%	0.00%
HQ_Internet_Connectivity	0.00%	0.00%	0.00%	0.00%
HQ_Power	0.00%	0.55%	0.00%	2.44%
Paging Service_UK	0.00%	0.00%	0.00%	0.00%
Mobile_Phone_Network	0.00%	0.00%	0.00%	0.00%
Internet_large_scale	0.00%	0.47%	6.21%	6.81%
Exchange_Email	5.42%	6.34%	4.03%	4.36%
Email_MX	6.21%	6.28%	4.46%	4.84%
RT	6.63%	5.34%	0.00%	0.00%
RZMS	0.00%	0.00%	6.59%	7.07%
Any_SSH_Host	1.40%	1.58%	0.00%	0.00%
Authorized_PGP_Key	3.54%	3.13%	0.71%	0.66%
Sum:	**32.31%**	**37.97%**	**28.52%**	**36.10%**
Average:	**1.40%**	**1.65%**	**1.24%**	**1.57%**
SD:	**2.30%**	**2.19%**	**2.12%**	**2.23%**
Q3:	2.47%	2.47%	2.47%	2.47%
# Res in Q3:	6	8	6	6
% Res in Q3:	26.09%	34.78%	26.09%	26.09%

(*) Monte Carlo, 1000 iterations, Gaussian

"Auto" reduces dependency on Rekey but maintains dependency on Judgment

"Auto" exposes a significant new dependency on large-scale Internet availability

"Auto" exposes a slightly lower aggregate resource dependency

14 Appendix G: 1Q 2010 UPDATE

JAS was engaged in August, 2009 to provide a risk assessment of the ICANN/IANA root zone change process. The analysis that comprises the majority of the previous pages is based on data obtained through November, 2009. However, in the months since August, ICANN/IANA has aggressively moved to improve the resiliency of the IANA departmental business processes. This Appendix provides an update based on data provided to JAS in the months following delivery of the November 2009 draft of this document.[7]

14.1 Clarification of Risk Governance

ICANN/IANA has clarified several critical questions of risk governance by clearly listing critical ICANN/IANA processes and systems in the ICANN/IANA Business Continuity plan, identifying internal and external stakeholders and communications protocols, and introducing a requirement limiting acceptable service downtime following a continuity event to a maximum of four hours. These clarifications inform the requirements for business continuity planning, technical systems, and personnel redundancy.

14.2 Creation of a Hot Datacenter in Reston, Virginia

In order to satisfy the requirement that critical ICANN/IANA services be restored in less than four hours, ICANN located hot standby systems in a datacenter in Northern Virginia; these systems stand at the ready in the event the Los Angeles facilities are unavailable for an extended period. Additionally, technical systems are in place to facilitate rapid migration of services to the Northern Virginia datacenter if needed.

14.3 Completion of a Detailed IANA Business Continuity Plan

A detailed Business Continuity plan was created that specifies policies, responsibilities, and processes during continuity events. Additionally, the plan called for procurement of GETS/WPS capabilities for critical employees, and strategic distribution of satellite phones, both of which have been accomplished. JAS has reviewed the plan and finds that it generally meets industry standards for continuity planning. Furthermore, the plan was informed by the 8-Oct-2009 tabletop exercise TTX and was directly used during the 19-Jan-2010 exercise and performed well.

14.4 8-Oct Tabletop Exercise

On 8-Oct, a TTX was conducted with participants from ICANN's IANA department, and ICANN-IT. The exercise was coordinated by staff in ICANN's Security and Business Continuity operation. An After Action Report (AAR) was published and included the following recommendations:

1. Improve documentation of processes;
2. Further define roles within a Crisis Response Team (CRT) framework;
3. Publish call/contact instructions for members of the CRT;
4. Pre-arrange shared electronic meeting spaces for respondents;
5. Procure several back-up CRT communications modalities;

[7] JAS was also directly involved in the planning and execution of the 19-Jan-2010 exercise.

6. Perform additional exercises in the future.

This exercise significantly advanced several initiatives and resulted in a draft IANA departmental Business Continuity plan approved by senior ICANN management. Additionally, progress was made on each of the above recommendations leading-up to the 19-Jan-2010 exercise.

14.5 19-Jan No-Notice Exercise

Following the 8-Oct-2009 TTX, significant effort was put into planning and executing a no-notice exercise involving production systems during the business day. The 19-Jan-2010 exercise scenario involved a massive natural disaster affecting the greater Los Angeles area, which rendered all systems and personnel in that geography unavailable for the duration of the exercise.

From an exercise perspective, literally pulling the plug on production systems and asking staff to step away from their computes, both without notice, is a decidedly nontrivial task and underscores the serious and comprehensive approach ICANN is taking to business continuity.

The primary objective of the exercise was to restore the production systems enumerated in the IANA departmental Business Continuity Plan in less than four hours leveraging remote staff and the Reston datacenter. Secondary objectives included testing communications with internal and external stakeholders, testing the ability for remote staff to detect system failures and invoke the Continuity Plan, and analyze the performance of new technical systems including the new Reston datacenter.

It is important to note that this exercise had the full and energetic support of ICANN senior management and involved ICANN's Security, IT, Legal, and Communications departments in addition to ICANN/IANA staff.

While an AAR for this exercise is forthcoming, the exercise was a success in that critical systems were restored well within the four hour timeframe, and early reports from stakeholders indicate that internal and external communications were appropriate and well received.

14.6 Updated Analysis

Based on the risk governance thesis provided in Section 6 and the additional data obtained since the November draft, JAS re-ran the business process model analysis and has updated Table 2 as follows (changes noted in red and annotated with **):

Risk Grouping	Overall Adequacy of Risk Management	Mitigating Factors
Unintentional human error	Properly managed	Expert staff, low turnover, workload, RZMS
Intentional human error / Insider Threat	Under-managed	High loyalty, strong culture, low turnover, three party approval process, RZMS
IT Systems	**Properly managed**	Expert staff, low turnover
Resource disruption / destruction	**Properly managed**	Expert staff, process flexibility, workload
RZMS Project management / governance	Under-managed	Good working relationship with outsourced development firm

Table 3: Updated Risk Management and Mitigation by Risk Grouping

14.7 Discussion of Improvements

Through business continuity planning and subsequent exercises, ICANN/IANA has both set objectives for performance during continuity operations, and demonstrated that processes and systems are in place to meet those requirements. Primary IT systems in Los Angeles are fully replicated 2,000 miles away in Northern Virginia, and the technical and procedural systems are in place to restore operations at the hot-site well within the allotted timeframe. Similarly, personnel are sufficiently cross-trained and distributed to provide continuity even when faced with a widespread regional event. These assertions are supported by a re-run of the JAS model as well as observations during the 19-Jan-2010 exercise.

Finally, the planning and execution of a complex "live-fire" exercise affecting production systems demonstrated a high level of communication and coordination between ICANN's IANA department, and ICANN-IT. JAS believes the increased level of communication and documentation of business continuity requirements is demonstrative of an effective working relationship between ICANN's IANA department and ICANN-IT, which reduces the risks associated with IANA's reliance on IT systems.

14.8 Remaining Under-Managed Risks

The focus of ICANN/IANA's recent activity has been on business continuity. JAS sees no grounds on which to amend our previous analysis regarding intentional and unintentional human errors, and the risks associated with RT/RZMS governance and implementation. In fact, the 19-Jan-2010 exercise raised questions about the technical capabilities of the RT ticketing system and MySQL database in complex multi-site failover scenarios. JAS recommends ICANN's IANA department and ICANN-IT continue to evaluate the applicability and viability of these systems given the new requirement to perform in a multi-site failover architecture. Based on JAS' previous experience with similar ticketing environments, complex technical architectures involving multiple database instances typically leverage mature commercial products including Oracle and Remedy.

Additionally, while the recent exercises have demonstrated depth and geographic diversity of ICANN/IANA staff, JAS remains concerned that ICANN/IANA staff often travel together and may be vulnerable to a single event in that capacity.