Second Security, Stability, and Resiliency (SSR2) Review Team Final Report – Executive Summary & Recommendations

Excerpted from the SSR2 Review Team Final Report

22 January 2021

TABLE OF CONTENTS

A. Executive Summary

Under the Internet Corporation for Assigned Names and Numbers (ICANN) Bylaws (Section 4.6(c)):

"*The Board shall cause a periodic review of ICANN's execution of its commitment to enhance the operational stability, reliability, resiliency, security, and global interoperability of the systems and processes, both internal and external, that directly affect and/or are affected by the Internet's system of unique identifiers that ICANN coordinates ("SSR Review").*"[1]

These SSR reviews are a critical part of the ICANN organization's mandate[2] to "operate to the maximum extent feasible in an open and transparent manner and consistent with procedures designed to ensure fairness." This is the second SSR review conducted and per the Bylaws' direction includes a review of ICANN org's handling of the first SSR review's recommendations as well as new recommendations for ICANN org to consider.

The SSR2 Review Team offers 24 groups of recommendations, resulting in 63 specific recommendations, starting with the evaluation of ICANN org's response to the SSR1 recommendations. We took the approach of breaking these into very specific recommendations in response to the lack of specificity in the SSR1 recommendations. The recommendations are then structured to offer insight on internal ICANN org operations, ICANN org's engagement (particularly contracts and complaint handling), and how ICANN org can take steps to improve both its own SSR actions and help others understand how to improve theirs. Recommendations throughout the document often influence each other and include dependencies between them. The ICANN org and Board should take this into account when developing implementation plans. The review team reached full consensus on every recommendation.

To support more efficient evaluations by future SSR review teams, the SSR2 Review Team attempted to phrase its own recommendations according to the SMART criteria: *specific, measurable, assignable, relevant, and trackable*. In many cases, the detail required to make each recommendation fully SMART, including assigning appropriate timelines, will require thought and action from the implementation team and should be included in the final implementation plan. The review team also offered several suggestions for consideration regarding how future reviews might be handled, recognizing that these fall outside the direct mandate of the SSR review itself. Additional information on the process and methodology used by the SSR2 Review Team to fulfill their mandate is available in Appendix C: Process and Methodology.

1. Background

As noted in Section A.2. Objectives of the SSR Review, the ICANN Bylaws require a periodic assessment of the Security, Stability, and Resiliency of the Domain Name System (DNS). The ICANN Board formally received the first SSR review report on 13 September 2012. Five years later, the second review began with the SSR2 Review Team's initial meeting, held on 2 March

[1] ICANN, "Bylaws for Internet Corporation for Assigned Names and Numbers: Section 4.6(c): Specific Reviews: Security, Stability, and Resiliency Review" amended 28 November 2019, https://www.icann.org/resources/pages/governance/bylaws-en/#article4.

[2] ICANN Bylaws, Section 3.1: https://www.icann.org/resources/pages/governance/bylaws-en/.

2017. Since its inception, however, the SSR2 Review Team encountered several challenges that extended the review's duration far beyond what anyone expected. The SSR2 Review Team regularly met until October 2017, when the Board paused the team's activities.[3] Meetings began again with a reconstituted membership on 19 June 2018.[4]

The landscape of the global unique identifier ecosystem continued to evolve during the extended timeframe of the review process. Despite the global disruption of business and travel resulting from the COVID-19 pandemic that introduced additional delays in the SSR2 review process, the SSR2 Review Team was able to complete the review. In the last year of the review process, the team chose not to restart the evaluation of their original recommendations but rather to preserve their foundational and historical contributions. The review team believes these recommendations remain largely relevant to ICANN org and in support of the security, stability, and resiliency of the global DNS.

2. Objectives of the SSR Review

Under the ICANN Bylaws (Section 4.6(c)): "*The Board shall cause a periodic review of ICANN's execution of its commitment to enhance the operational stability, reliability, resiliency, security, and global interoperability of the systems and processes, both internal and external, that directly affect and/or are affected by the Internet's system of unique identifiers that ICANN coordinates ("SSR Review").*"[5]

Specifically it states that:

"ii. The issues that the review team for the SSR Review ("SSR Review Team") may assess are the following:

1. *security, operational stability and resiliency matters, both physical and network, relating to the coordination of the Internet's system of unique identifiers;*
2. *conformance with appropriate security contingency planning framework for the Internet's system of unique identifiers;*
3. *maintaining clear and globally interoperable security processes for those portions of the Internet's system of unique identifiers that ICANN coordinates.*

iii. The SSR Review Team shall also assess the extent to which ICANN org has successfully implemented its security efforts, the effectiveness of the security efforts to deal with actual and potential challenges and threats to the security and stability of the DNS, and the extent to which the security efforts are sufficiently robust to meet future challenges and threats to the security, stability, and resiliency of the DNS, consistent with ICANN's Mission.

iv. The SSR Review Team shall also assess the extent to which prior SSR Review recommendations have been implemented and the extent to which implementation of such recommendations has resulted in the intended effect.

v. The SSR Review shall be conducted no less frequently than every five years, measured from the date the previous SSR Review Team was convened."

[3] Letter to the SSR2 Review Team from Dr. Stephen D. Crocker, Chairman, ICANN Board of Directors, 28 October 2017, https://www.icann.org/en/system/files/correspondence/crocker-to-ssr2-28oct17-en.pdf.

[4] ICANN, "Second Security, Stability, and Resiliency of the DNS Review (SSR2) Restarts," blog, 7 June 2018, https://www.icann.org/news/announcement-2-2018-06-07-en. four

[5] ICANN Bylaws, Section 4.6(c), https://www.icann.org/resources/pages/governance/bylaws-en.

3. Influence of Other Review Teams and Advisory Committees

ICANN org must engage with several review teams and Advisory Committees (ACs), as required by the ICANN Bylaws. While each of those teams and committees have specific mandates, the recommendations developed from those groups can and do overlap the work areas of other review teams and committees. The SSR2 Review Team evaluated recommendations from other review teams and ACs to determine where their published recommendations impacted the SSR of ICANN org and the global DNS. In several instances, the SSR2 Review Team found it necessary to incorporate and build on those recommendations to develop the necessary SSR-related guidance for ICANN org (see in particular Section E.1. Unachieved Safeguards for the New gTLD Program and Section E.3. PDP Alternatives). The SSR2 Review Team viewed these overlaps in recommendations as tacit corroboration of the merits of the corresponding issues and further viewed agreements between the review team's recommendations and those of other groups as empirical support for their necessity. The SSR2 recommendations are meant to complement the recommendations of those other review teams.

B. SSR2 Recommendations

The SSR2 Review Team reached full consensus on every recommendation.

1. Summary Table

#	Recommendation	Owner	Priority
SSR2 Recommendation 1: Further Review of SSR1			
1.1	The ICANN Board and ICANN org should perform a further comprehensive review of the SSR1 Recommendations and execute a new plan to complete the implementation of the SSR1 Recommendations (see Appendix D: Findings Related to SSR1 Recommendations).	ICANN Board and ICANN org	Low
SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management			
2.1	ICANN org should create a position of a Chief Security Officer (CSO) or Chief Information Security Officer (CISO) at the Executive C-Suite level of ICANN org and hire an appropriately qualified individual for that position and allocate a specific budget sufficient to execute this role's functions.	ICANN org	Medium-High
2.2	ICANN org should include as part of this role's	ICANN org	Medium-

	description that this position will manage ICANN org's security function and oversee staff interactions in all relevant areas that impact security. This position should be responsible for providing regular reports to the ICANN Board and community on all SSR-related activities within ICANN org. Existing security functions should be restructured and moved organizationally to report to this new position.		High
2.3	ICANN org should include as part of this role's description that this position will be responsible for both strategic and tactical security and risk management. These areas of responsibility include being in charge of and strategically coordinating a centralized risk assessment function, business continuity (BC), and disaster recovery (DR) planning (see also SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures) across the internal security domain of the organization, including the ICANN Managed Root Server (IMRS, commonly known as L-Root), and coordinate with other stakeholders involved in the external global identifier system, as well as publishing a risk assessment methodology and approach.	ICANN org	Medium-High
2.4	ICANN org should include as part of this role's description that this role will be responsible for all security-relevant budget items and responsibilities and take part in all security-relevant contractual negotiations (e.g., registry and registrar agreements, supply chains for hardware and software, and associated service level agreements) undertaken by ICANN org, signing off on all security-related contractual terms.	ICANN org	Medium-High
SSR2 Recommendation 3: Improve SSR-related Budget Transparency			
3.1	The Executive C-Suite Security Officer (see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management) should brief the community on behalf of ICANN org regarding ICANN org's SSR strategy, projects, and budget twice per year and update and publish budget overviews annually.	ICANN org	High
3.2	The ICANN Board and ICANN org should ensure specific budget items relating to ICANN org's performance of SSR-related functions are linked to specific ICANN strategic plan goals and objectives. ICANN org should implement those mechanisms	ICANN Board and ICANN org	High

	through a consistent, detailed, annual budgeting and reporting process.		
3.3	The ICANN Board and ICANN org should create, publish, and request public comment on detailed reports regarding the costs and SSR-related budgeting as part of the strategic planning cycle.	ICANN Board and ICANN org	High
SSR2 Recommendation 4: Improve Risk Management Processes and Procedures			
4.1	ICANN org should continue centralizing its risk management and clearly articulate its Security Risk Management Framework and ensure that it aligns strategically with the organization's requirements and objectives. ICANN org should describe relevant measures of success and how to assess them.	ICANN org	High
4.2	ICANN org should adopt and implement ISO 31000 "Risk Management" and validate its implementation with appropriate independent audits. ICANN org should make audit reports, potentially in redacted form, available to the community. Risk management efforts should feed into BC and DR plans and procedures (see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures).	ICANN org	High
4.3	ICANN org should name or appoint a dedicated, responsible person in charge of security risk management that will report to the C-Suite Security role (see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management). This function should regularly update, and report on, a register of security risks and guide ICANN org's activities. Findings should feed into BC and DR plans and procedures (see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures) and the Information Security Management System (ISMS) (see SSR2 Recommendation 6: Comply with Appropriate Information Security Management Systems and Security Certifications).	ICANN org	High
SSR2 Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications			
5.1	ICANN org should implement an ISMS and be audited and certified by a third party along the lines of industry security standards (e.g., ITIL, ISO 27000 family, SSAE-18) for its operational responsibilities. The plan should	ICANN org	High

	include a road map and milestone dates for obtaining certifications and noting areas that will be the target of continuous improvement.		
5.2	Based on the ISMS, ICANN org should put together a plan for certifications and training requirements for roles in the organization, track completion rates, provide rationale for their choices, and document how the certifications fit into ICANN org's security and risk management strategies.	ICANN org	High
5.3	ICANN org should require external parties that provide services to ICANN org to be compliant with relevant security standards and document their due diligence regarding vendors and service providers.	ICANN org	High
5.4	ICANN org should reach out to the community and beyond with clear reports demonstrating what ICANN org is doing and achieving in the security space. These reports would be most beneficial if they provided information describing how ICANN org follows best practices and mature, continually-improving processes to manage risk, security, and vulnerabilities.	ICANN org	High
SSR2 Recommendation 6: SSR Vulnerability Disclosure and Transparency			
6.1	ICANN org should proactively promote the voluntary adoption of SSR best practices and objectives for vulnerability disclosure by the contracted parties. If voluntary measures prove insufficient to achieve the adoption of such best practices and objectives, ICANN org should implement the best practices and objectives in contracts, agreements, and MOUs.	ICANN org	High
6.2	ICANN org should implement coordinated vulnerability disclosure reporting. Disclosures and information regarding SSR-related issues, such as breaches at any contracted party and in cases of critical vulnerabilities discovered and reported to ICANN org, should be communicated promptly to trusted and relevant parties (e.g., those affected or required to fix the given issue). ICANN org should regularly report on vulnerabilities (at least annually), including anonymized metrics and using responsible disclosure.	ICANN org	High
SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures			
7.1	ICANN org should establish a Business Continuity Plan for all the systems owned by or under the ICANN org	ICANN org	Medium-High

	purview, based on ISO 22301 "Business Continuity Management," identifying acceptable BC and DR timelines.		
7.2	ICANN org should ensure that the DR plan for Public Technical Identifiers (PTI) operations (i.e., IANA functions) includes all relevant systems that contribute to the security and stability of the DNS and also includes Root Zone Management and is in line with ISO 27031. ICANN org should develop this plan in close cooperation with the Root Server System Advisory Committee (RSSAC) and the Root Server Operators (RSO).	ICANN org	Medium-High
7.3	ICANN org should also establish a DR plan for all the systems owned by or under the ICANN org purview, again in line with ISO 27031.	ICANN org	Medium-High
7.4	ICANN org should establish a new site for DR for all the systems owned by or under the ICANN org purview with the goal of replacing either the Los Angeles or Culpeper sites or adding a permanent third site. ICANN org should locate this site outside of the North American region and any United States territories. If ICANN org chooses to replace one of the existing sites, whichever site ICANN org replaces should not be closed until the organization has verified that the new site is fully operational and capable of handling DR of these systems for ICANN org.	ICANN org	Medium-High
7.5	ICANN org should publish a summary of their overall BC and DR plans and procedures. Doing so would improve transparency and trustworthiness beyond addressing ICANN org's strategic goals and objectives. ICANN org should engage an external auditor to verify compliance with these BC and DR plans.	ICANN org	Medium-High
SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties			
8.1	ICANN org should commission a negotiating team that includes abuse and security experts not affiliated with or paid by contracted parties to represent the interests of non-contracted entities and work with ICANN org to renegotiate contracted party contracts in good faith, with public transparency, and with the objective of improving the SSR of the DNS for end-users, businesses, and governments.	ICANN org	Medium
SSR2 Recommendation 9: Monitor and Enforce Compliance			

9.1	The ICANN Board should direct the compliance team to monitor and strictly enforce the compliance of contracted parties to current and future SSR and abuse-related obligations in contracts, baseline agreements, temporary specifications, and community policies.	ICANN Board	High
9.2	ICANN org should proactively monitor and enforce registry and registrar contractual obligations to improve the accuracy of registration data. This monitoring and enforcement should include the validation of address fields and conducting periodic audits of the accuracy of registration data. ICANN org should focus their enforcement efforts on those registrars and registries that have been the subject of over 50 complaints or reports per year regarding their inclusion of inaccurate data to ICANN org.	ICANN org	High
9.3	ICANN org should have compliance activities audited externally at least annually and publish the audit reports and ICANN org response to audit recommendations, including implementation plans.	ICANN org	High
9.4	ICANN org should task the compliance function with publishing regular reports that enumerate tools they are missing that would help them support ICANN org as a whole to effectively use contractual levers to address security threats in the DNS, including measures that would require changes to the contracts.	ICANN org	High
SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms			
10.1	ICANN org should post a web page that includes their working definition of DNS abuse, i.e., what it uses for projects, documents, and contracts. The definition should explicitly note what types of security threats ICANN org currently considers within its remit to address through contractual and compliance mechanisms, as well as those ICANN org understands to be outside its remit. If ICANN org uses other similar terminology—e.g., security threat, malicious conduct—ICANN org should include both its working definition of those terms and precisely how ICANN org is distinguishing those terms from DNS abuse. This page should include links to excerpts of all current abuse-related obligations in contracts with contracted parties, including any procedures and protocols for responding to abuse. ICANN org should update this page annually, date the latest version, and link to older versions with	ICANN org	High

	associated dates of publication.		
10.2	Establish a staff-supported, cross-community working group (CCWG) to establish a process for evolving the definitions of prohibited DNS abuse, at least once every two years, on a predictable schedule (e.g., every other January), that will not take more than 30 business days to complete. This group should involve stakeholders from consumer protection, operational cybersecurity, academic or independent cybersecurity research, law enforcement, and e-commerce.	ICANN org	High
10.3	Both the ICANN Board and ICANN org should use the consensus definitions consistently in public documents, contracts, review team implementation plans, and other activities, and have such uses reference this web page.	ICANN org	High
SSR2 Recommendation 11: Resolve CZDS Data Access Problems			
11.1	The ICANN community and ICANN org should take steps to ensure that access to Centralized Zone Data Service (CZDS) data is available, in a timely manner and without unnecessary hurdles to requesters, e.g., lack of auto-renewal of access credentials.	ICANN community and ICANN org	Medium
SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review			
12.1	ICANN org should create a DNS Abuse Analysis advisory team composed of independent experts (i.e., experts without financial conflicts of interest) to recommend an overhaul of the DNS Abuse Reporting activity with actionable data, validation, transparency, and independent reproducibility of analyses as its highest priorities.	ICANN org	Medium
12.2	ICANN org should structure its agreements with data providers to allow further sharing of the data for non-commercial use, specifically for validation or peer-reviewed scientific research. This special no-fee non-commercial license to use the data may involve a time-delay so as not to interfere with commercial revenue opportunities of the data provider. ICANN org should publish all data-sharing contract terms on the ICANN website. ICANN org should terminate any contracts that do not allow independent verification of methodology behind blocklisting.	ICANN org	Medium
12.3	ICANN org should publish reports that identify registries and registrars whose domains most contribute to	ICANN org	Medium

	abuse. ICANN org should include machine-readable formats of the data, in addition to the graphical data in current reports.		
12.4	ICANN org should collate and publish reports of the actions that registries and registrars have taken, both voluntary and in response to legal obligations, to respond to complaints of illegal and/or malicious conduct based on applicable laws in connection with the use of the DNS.	ICANN org	Medium
SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting			
13.1	ICANN org should establish and maintain a central DNS abuse complaint portal that automatically directs all abuse reports to relevant parties. The system would purely act as an inflow, with ICANN org collecting and processing only summary and metadata, including timestamps and types of complaint (categorical). Use of the system should become mandatory for all generic top-level domains (gTLDs); the participation of each country code top-level domain (ccTLD) would be voluntary. In addition, ICANN org should share abuse reports (e.g., via email) with all ccTLDs.	ICANN org	High
13.2	ICANN org should publish the number of complaints made in a form that allows independent third parties to analyze the types of complaints on the DNS.	ICANN org	High
SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements			
14.1	ICANN org should create a Temporary Specification that requires all contracted parties to keep the percentage of domains identified by the revised DNS Abuse Reporting (see SSR2 Recommendation 13.1) activity as abusive below a reasonable and published threshold.	ICANN org	High
14.2	To enable anti-abuse action, ICANN org should provide contracted parties with lists of domains in their portfolios identified as abusive, in accordance with SSR2 Recommendation 12.2 regarding independent review of data and methods for blocklisting domains.	ICANN org	High
14.3	Should the number of domains linked to abusive activity reach the published threshold described in SSR2 Recommendation 14.1, ICANN org should investigate to confirm the veracity of the data and analysis, and	ICANN org	High

	then issue a notice to the relevant party.		
14.4	ICANN org should provide contracted parties 30 days to reduce the fraction of abusive domains below the threshold or to demonstrate that ICANN org's conclusions or data are flawed. Should a contracted party fail to rectify for 60 days, ICANN Contractual Compliance should move to the de-accreditation process.	ICANN org	High
14.5	ICANN org should consider offering financial incentives: contracted parties with portfolios with less than a specific percentage of abusive domain names should receive a fee reduction on chargeable transactions up to an appropriate threshold.	ICANN org	High
SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements			
15.1	After creating the Temporary Specification (see SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements), ICANN org should establish a staff-supported Expedited Policy Development Process (EPDP) to create an anti-abuse policy. The EPDP volunteers should represent the ICANN community, using the numbers and distribution from the Temporary Specification for gTLD Registration Data EPDP team charter as a template.	ICANN org	High
15.2	The EPDP should draw from the definition groundwork of the CCWG proposed in SSR2 Recommendation 10.2. This policy framework should define appropriate countermeasures and remediation actions for different types of abuse, time-frames for contracted party actions like abuse report/response report timelines, and ICANN Contractual Compliance enforcement actions in case of policy violations. ICANN org should insist on the power to terminate contracts in the case of a pattern and practice of harboring abuse by any contracted party. The outcome should include a mechanism to update benchmarks and contractual obligations related to abuse every two years, using a process that will not take more than 45 business days.	ICANN org	High
SSR2 Recommendation 16: Privacy Requirements and RDS			
16.1	ICANN org should provide consistent cross-references across their website to provide cohesive and easy-to-find information on all actions—past, present, and planned—taken on the topic of privacy and data	ICANN org	Medium

	stewardship, with particular attention to the information around the Registration Directory Service (RDS).		
16.2	ICANN org should create specialized groups within the Contractual Compliance function that understand privacy requirements and principles (such as collection limitation, data qualification, purpose specification, and security safeguards for disclosure) and that can facilitate law enforcement needs under the RDS framework as that framework is amended and adopted by the community (see also SSR2 Recommendation 11: Resolve CZDS Data Access Problems).	ICANN org	Medium
16.3	ICANN org should conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they have procedures in place to address privacy breaches.	ICANN org	Medium
SSR2 Recommendation 17: Measuring Name Collisions			
17.1	ICANN org should create a framework to characterize the nature and frequency of name collisions and resulting concerns. This framework should include metrics and mechanisms to measure the extent to which controlled interruption is successful in identifying and eliminating name collisions. This could be supported by a mechanism to enable protected disclosure of name collision instances. This framework should allow the appropriate handling of sensitive data and security threats.	ICANN org	Medium
17.2	The ICANN community should develop a clear policy for avoiding and handling new gTLD-related name collisions and implement this policy before the next round of gTLDs. ICANN org should ensure that the evaluation of this policy is undertaken by parties that have no financial interest in gTLD expansion.	ICANN community and ICANN org	Medium
SSR2 Recommendation 18: Informing Policy Debates			
18.1	ICANN org should track developments in the peer-reviewed research community, focusing on networking and security research conferences, including at least ACM CCS, ACM Internet Measurement Conference, Usenix Security, CCR, SIGCOMM, IEEE Symposium on Security and Privacy, as well as the operational security conferences and FIRST, and publish a report for the ICANN community summarizing implications of publications that are relevant to ICANN org or	ICANN org	Low

	contracted party behavior.		
18.2	ICANN org should ensure that these reports include relevant observations that may pertain to recommendations for actions, including changes to contracts with registries and registrars, that could mitigate, prevent, or remedy SSR harms to consumers and infrastructure identified in the peer-reviewed literature.	ICANN org	Low
18.3	ICANN org should ensure that these reports also include recommendations for additional studies to confirm peer-reviewed findings, a description of what data would be required by the community to execute additional studies, and how ICANN org can offer to help broker access to such data, e.g., via the CZDS.	ICANN org	Low
SSR2 Recommendation 19: Complete Development of the DNS Regression Test Suite			
19.1	ICANN org should complete the development of a suite for DNS resolver behavior testing.	ICANN org	Low
19.2	ICANN org should ensure that the capability to continue to perform functional testing of different configurations and software versions is implemented and maintained.	ICANN org	Low
SSR2 Recommendation 20: Formal Procedures for Key Rollovers			
20.1	ICANN org should establish a formal procedure, supported by a formal process modeling tool and language to specify the details of future key rollovers, including decision points, exception legs, the full control-flow, etc. Verification of the key rollover process should include posting the programmatic procedure (e.g., program, finite-state machine (FSM)) for Public Comment, and ICANN org should incorporate community feedback. The process should have empirically verifiable acceptance criteria at each stage, which should be fulfilled for the process to continue. This process should be reassessed at least as often as the rollover itself (i.e., the same periodicity) so that ICANN org can use the lessons learned to adjust the process.	ICANN org	Medium
20.2	ICANN org should create a group of stakeholders involving relevant personnel (from ICANN org or the community) to periodically run table-top exercises that follow the root KSK rollover process.	ICANN org	Medium

SSR2 Recommendation 21: Improve the Security of Communications with TLD Operators			
21.1	ICANN org and PTI operations should accelerate the implementation of new Root Zone Management System (RZMS) security measures regarding the authentication and authorization of requested changes and offer TLD operators the opportunity to take advantage of those security measures, particularly MFA and encrypted email.	ICANN org and PTI	Medium
SSR2 Recommendation 22: Service Measurements			
22.1	For each service that ICANN org has authoritative purview over, including root zone and gTLD-related services as well as IANA registries, ICANN org should create a list of statistics and metrics that reflect the operational status (such as availability and responsiveness) of that service, and publish a directory of these services, data sets, and metrics on a single page on the icann.org website, such as under the Open Data Platform. ICANN org should produce measurements for each of these services as summaries over both the previous year and longitudinally (to illustrate baseline behavior).	ICANN org	Low
22.2	ICANN org should request community feedback annually on the measurements. That feedback should be considered, publicly summarized after each report, and incorporated into follow-on reports. The data and associated methodologies used to measure these reports' results should be archived and made publicly available to foster reproducibility.	ICANN org	Low
SSR2 Recommendation 23: Algorithm Rollover			
23.1	PTI operations should update the DNSSEC Practice Statement (DPS) to allow the transition from one digital signature algorithm to another, including an anticipated transition from the RSA digital signature algorithm to other algorithms or to future post-quantum algorithms, which provide the same or greater security and preserve or improve the resilience of the DNS.	PTI	Medium
23.2	As a root DNSKEY algorithm rollover is a very complex and sensitive process, PTI operations should work with other root zone partners and the global community to develop a consensus plan for future root DNSKEY algorithm rollovers, taking into consideration the	PTI	Medium

	lessons learned from the first root KSK rollover in 2018.		
SSR2 Recommendation 24: Improve Transparency and End-to-end Testing for the EBERO Process			
24.1	ICANN org should coordinate end-to-end testing of the full EBERO process at predetermined intervals (at least annually) using a test plan that includes datasets used for testing, progression states, and deadlines, and is coordinated with the ICANN contracted parties in advance to ensure that all exception legs are exercised and publish the results.	ICANN org	Medium
24.2	ICANN org should make the Common Transition Process Manual easier to find by providing links on the EBERO website.	ICANN org	Medium

2. Prioritization

The SSR2 Review Team has aligned all SSR2 recommendations with the 2021-2025 ICANN Strategic Plan and its goals and objectives.[6] The review team removed any recommendations from this report that did not clearly align with the strategic plan. All SSR2 RT recommendations align with ICANN org's strategic plan, and so are considered important.

The SSR2 Review Team used an online survey tool (the Internet-based solution Qualtrics) for polling all team members for their inputs on the priority of each grouping of recommendations in this report.[7] This survey allowed for the ranking of each group on a five-point scale that ranged from Very Low Priority, Low Priority, Medium Priority, High Priority, to Very High Priority.

The review team determined that of the twenty-four groups of recommendations, twenty-seven specific recommendations should be considered high priority, most of which are concerned with ICANN org's internal security management and anti-abuse actions. Nine recommendations are medium-high priority. Eighteen recommendations, predominantly from the Global DNS Sections, were ranked as medium priority, and the remaining eight recommendations were ranked at a lower priority.

[6] See Appendix G: Mapping of SSR2 Recommendations to the ICANN 2021-2025 Strategic Plan and the ICANN Bylaws.

[7] See https://www.qualtrics.com/.