Second Security, Stability, and Resiliency (SSR2) Review Team Final Report

25 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

Table 1: SSR2 Recommendations Summary

#	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 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.	ICANN org	Medium-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 Board and ICANN org	High

	ICANN org should implement those mechanisms 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-	ICANN org	High

	18) for its operational responsibilities. The plan should 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	ICANN org	Medium-

	for all the systems owned by or under the ICANN org purview, based on ISO 22301 "Business Continuity Management," identifying acceptable BC and DR timelines.		High
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	ICANN org	High

	to abuse. ICANN org should update this page annually, date the latest version, and link to older versions with 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 abuse. ICANN org should include machine-readable formats of the data, in addition to the graphical data in current reports.	ICANN org	Medium
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	ICANN org	High

	Recommendation 14.1, ICANN org should investigate to confirm the veracity of the data and analysis, and 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-	ICANN org	Medium

	find information on all actions—past, present, and planned—taken on the topic of privacy and data 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	ICANN org	Low

	for the ICANN community summarizing implications of publications that are relevant to ICANN org or 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	ICANN org	Medium

	follow the root KSK rollover process.		
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	PTI	Medium

	develop a consensus plan for future root DNSKEY algorithm rollovers, taking into consideration the 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.

C. SSR1 Implementation and Intended Effects

[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/.

In 2012, the ICANN Board found *"that the 28 Recommendations in the [SSR1] Final Report are feasible and implementable,"* and unanimously accepted and instructed staff to implement all 28 SSR1 recommendations.[8] One of the SSR2 Review Team's tasks was assessing "*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."*

The process and methodology used by the SSR2 Review Team to evaluate the implementations and their effects are summarized in Appendix C: Process and Methodology. That section outlines the assessment process, the types of evidence and data used, and the methodology adopted in reaching a conclusion on the level of implementation of the recommendations. The conclusions and supporting rationale from the SSR2 Review Team for each of the SSR1 recommendations are provided in Appendix D: Findings Related to SSR1 Recommendations.

Each review is a learning opportunity, and having assessed the SSR1 recommendations, the SSR2 Review Team notes the importance and the necessity to provide recommendations that are metric-based with measurable performance indicators, something that was often missing from SSR1 recommendations. This observation is underpinned by the need to ensure effective implementation and assessment of any future review team's recommendations.

1. Summary: SSR1 Review

The SSR2 Review Team reviewed all 28 SSR1 recommendations and found that out of 28 recommendations, all remain relevant as of the publication of this report (see Table 2).[9] The team considers no recommendation to be fully implemented, for the reasons as outlined in Appendix D: Findings Related to SSR1 Recommendations.

Table 2: SSR1 Recommendation Overview

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Relevant	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Implemented	P	P	P	P	P	N	P	P	-	P	P	P	N	N	P	P	-	N	-	P	P	P	P	P	P	P	P	P
Effective	N	N	N	Y	-	N	N	N	-	N	-	N	N	N	-	N	-	-	N	N	N	N	-	N	N	-	N	N

Key: Y = Yes N = No P = Partial - = Unable to Determine

The SSR2 Review Team notes the following reappearing issues:

[8] ICANN, "Regular Meeting of the ICANN Board of Directors," last updated 18 October 2012, https://www.icann.org/resources/board-material/minutes-2012-10-18-en and "Final Report of the Security, Stability and Resiliency of the DNS Review Team," SSR Review Team, 20 June 2012, https://www.icann.org/en/system/files/files/final-report-20jun12-en.pdf.

[9] ICANN, SSR Review Implementation Report, June 2015, https://www.icann.org/en/system/files/files/ssr-review-implementation-30jun15-en.pdf.

1. There is generally a lack of indicators, measurement, and goalposts in the SSR1 recommendations and associated implementation plans that would allow the community and ICANN org to track and understand the security space and their own activities.

2. There is a lack of publicly available evidence, definitions, and procedures, which inhibits independent observation of SSR activities. This scarcity of information results in a lack of clarity regarding if or how ICANN org has implemented the recommendations from SSR1.

3. There is a lack of community review and accountability against the various implementation plans, denying the ICANN community opportunities to provide input on SSR matters.

4. ICANN org does not currently have an overarching strategy, identifiable goals, or a clear and comprehensive SSR policy. Without a functional SSR strategy and integrated security and risk management (e.g., policies, procedures, standards, baselines, guidelines), SSR-related responsibilities are not assigned, measured, and tracked, leading to a lack of transparency, accountability, and apparent gaps in ICANN org's SSR-related responsibilities.

The SSR2 Review Team recognizes that the original guidance provided by the SSR1 Review Team was not in all cases sufficiently measurable, and while ICANN org has indicated that they believe all recommendations were addressed, the implementation plans for those recommendations were also often unclear and insufficiently measurable. The SSR2 Review Team, therefore, was unable to find the implementation of SSR1 recommendations to be complete. ICANN org should perform a further comprehensive review of the implementation of the SSR1 recommendations, taking into account the findings offered by the SSR2 Review Team.

This report also offers suggestions that fall outside of the direct scope of the SSR2 review (see Appendix A - Further Suggestions) as a way for future review teams to avoid some of the challenges encountered by the SSR2 Review Team.

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).

D. Key Stability Issues within ICANN

The focus of this section is on areas as they relate to the ICANN Bylaws sections 4.6(c) (ii) A, 4.6(c) (ii) B, and 4.6(c) (iii).[10] These areas include security, operational stability, and resiliency matters, both physical and network, relating to the coordination of the Internet's system of unique identifiers; security contingency planning framework for the Internet's system of unique

[10] See Appendix H - Bylaws and Strategic Plan sections most relevant to SSR2 Recommendations of this report for a copy of the sections of the ICANN Bylaws and Strategic Plan 2021-2025 that are most relevant to SSR.

identifiers; and completeness and effectiveness of ICANN org's internal security processes and the ICANN security framework.

The fundamental issue that informs this section's recommendations is the lack of evidence available to the SSR2 Review Team demonstrating an efficient, comprehensive, and transparent SSR program for ICANN org. During the team's review of ICANN org's internal security, it was apparent that ICANN org was undertaking various security-relevant projects and measures. The review team did not, however, see sufficiently comprehensive evidence of an appropriately managed and documented information management and security program (see Section D.3. Risk and Security Management), of business continuity and disaster recovery processes (see Section D.4. Business Continuity Management), or of a largely independent security structure appropriate to an organization that supports a system critical to the functioning of the Internet (see Section D.1. Organization Structure Improvements).

ICANN org, according to its Bylaws, must "*operate to the maximum extent feasible in an open and transparent manner and consistent with procedures designed to ensure fairness.*"[11] The recommendations in this section are offered to help ICANN org improve SSR disclosure and transparency in all aspects of the organization to the greatest extent possible considering security objectives. By following these recommendations, ICANN org will efficiently and effectively resolve the fundamental issue of information transparency and the lack of clear, demonstrable security leadership and organization.

1. Organization Structure Improvements - C-Suite Security Position

Currently, ICANN org splits SSR-related activities across the organization. The SSR2 Review Team recognizes the roles of the Office of the Chief Technology Officer (OCTO), which has responsibilities including but not limited to:

Researching issues related to the Internet's system of unique identifiers (domain names, IP addresses/AS numbers, protocol parameters, etc.)

Supporting improving the Security, Stability, and Resiliency of those identifiers.[12]

And the Chief Information Officer, who is generally responsible for the *"monitoring and maintenance of ICANN systems and technical operations, corporate security, and Information Technology, and the ICANN DNS Engineering Team (http://www.dns.icann.org/), which administers L-root and ICANN's DNS network services,"*[13] as well as securing, monitoring, and managing data-assets, such as private data from contracted parties.

[11] ICANN Bylaws, Section 3.1, https://www.icann.org/resources/pages/governance/bylaws-en/#article3

[12] Office of the Chief Technology Officer (OCTO), ICANN, accessed 27 December 2019, https://www.icann.org/octo.

[13] ICANN, "Information Systems and Innovation," accessed 21 January 2020, https://www.icann.org/resources/pages/technical-functions-cio.

ICANN org should create an Executive C-Suite position responsible for all security-related matters, including setting strategic objectives, managing regulatory compliance and budgeting, securing the organization's assets.[14]

Several mandates in ICANN's Bylaws and commitments in ICANN's Strategic Plan FY21-25 would come under this position's purview. In addition, SSR1 Recommendation 24 called for the creation of a Chief Security Office Team.[15] The current structure distributes these responsibilities across two separate units within ICANN org. Centralized management would more efficiently drive the strategic alignment of all related activities by consolidating the work under one role, with a commensurate budget.[16] This will support efforts to make coherent, consistent documentation available to the community and future review teams.

SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management

The SSR2 Review Team considers it necessary for ICANN org to have an officer at the Executive C-Suite level to coordinate and strategically manage ICANN org's security and security risk activities and implement ICANN org's mission and strategic security objectives.[17]

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.

2.2. ICANN org should include as part of this role's 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.

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 SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures) across the internal security domain of the organization,

[14] The Institute of Education Sciences (IES): National Center for Education Statistics, "CHAPTER 3 - Security Policy: Development and Implementation," accessed 9 December 2020, https://nces.ed.gov/pubs98/safetech/chapter3.asp.

[15] See Appendix D: Findings Related to SSR1 Recommendations.

[16] See Clause 5.1 in International Organization for Standardization standards and standard suites ISO 27001, ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, which also maps to the SSAE18 2017 Trust Services Criteria CC1.3/COSO Principle 3, https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/othermapping/trust-services-map-to-iso-27001.xlsx.

[17] The ICANN Board can be guided by resources such as the Cybersecurity Risk Handbook: National Association of Corporate Directors, "NACD Director's Handbook on Cyber-Risk Oversight," 2017, http://boardleadership.nacdonline.org/Cyber-Risk-Handbook-GCNews.html.

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.

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.

This recommendation can be considered implemented when ICANN org has created and filled the role of Chief Security Officer with responsibilities as defined in the recommendations.

This recommendation can be considered effective when ICANN org centralizes security responsibilities such that ICANN org can demonstrably coordinate SSR activities and budget and speak to security issues at the appropriate management level.

2. SSR-related Budgets and Reporting

While ICANN org may cover SSR-related activities under various items within its annual budget, it is unclear how ICANN org currently allocates funds to specific SSR-related functions. This section of the SSR2 report examines the intent and results (where discoverable and measurable) of the SSR1 recommendations related to SSR budgeting and reporting.

SSR1 Recommendations 20, 21, and 22 touched on various aspects of the need for a more granular and transparent set of budgeting and reporting processes for SSR-related budget items. For example, SSR1 Recommendation 20 intended a greater degree of granularity for examination and public comment of SSR-related budget items as well as regular review.[18] [19] Recommendation 21 of SSR1 indicated that ICANN org should establish a more structured internal process for showing how organizational and budget decisions relate to the IS-SSR Framework, including the underlying cost-benefit analysis. Recommendation 22 of SSR1 advised ICANN org to publish, monitor, and update documentation on the organization and budget resources needed to manage SSR issues in conjunction with the introduction of new gTLDs.

The SSR2 Review Team assessed the extent of ICANN org's implementation of these recommendations by exploring publicly available documents, documents made available to the review team by ICANN org, the SSR1 implementation report, and through the answers received regarding many questions sent to the ICANN org staff.[20] ICANN org did not provide the SSR2 Review Team with any additional information beyond the granularity of what staff shared with SSR1, which resulted in those initial recommendations (SSR1 Recommendations 20, 21, and 22). The review team found that while annual reporting on SSR-related activities did occur via the IS-SSR Framework documents and Annual Reports, most of the information related to the

[18] See Appendix D - SSR1 Recommendation 20 and SSR1 Recommendation 22 for more detail on the findings and conclusions made by the SSR2 Review Team against these recommendations.
[19] ICANN, "Identifier Systems Security, Stability, and Resiliency Framework – FY 15-16," 15 September 2016, https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf.
[20] ICANN SSR2 Review Team wiki, Background Materials, accessed 10 December 2020, https://community.icann.org/display/SSR/Background+Materials.

budgeting matters of SSR was at too high a level, which is not in line with the recommendations made by the SSR1 review. ICANN org's annual budget does not provide fine-grained information regarding SSR-related activities, and the IS-SSR Framework documents are no longer produced.[21]

Looking specifically at ICANN org's New gTLD Program, the new program's structure and budget reflected at a high level the SSR issues related to the New gTLD Program (e.g., DNS Stability Panel, EBERO).[22] However, ICANN org did not achieve the desired outcomes of more detailed data and improved clarity of information regarding the organization and budget for implementing the IS-SSR Framework and performing SSR-related functions related to the New gTLD Program. Notably, there is no document in the ICANN Identifier Systems Security, Stability, and Resiliency (IS-SSR) Document Archive specific to the New gTLD Program.[23] When examining the 2016 IS-SSR Framework documents and annual reports, gTLDs are mentioned twice, once in Module A as a trend in the Internet ecosystem and again in Module B as part of the overall ICANN Strategic Plan.[24] In the previous framework, published in March 2013, ICANN org mentions the New gTLD Program as a 'trend,' and a policy driver for the Generic Names Supporting Organization (GNSO).[25] The only remaining mentions of the New gTLD Program are in the section reporting on the implementation of the SSR1 recommendations. While ICANN org has published an annual report that includes direct costs of shared resources and the costs of support functions allocated to SSR, this report does not provide a breakdown of funding, resources, or other activities related to the New gTLD Program.[26]

To summarize the review team's concerns in this area, while ICANN org may cover SSR-related activities under various items within its annual budget, it remains unclear how ICANN org allocates funds to specific SSR-related functions. The review team was unable to find any evidence of any reporting on budget and associated resource impacts of SSR events by ICANN org; if such material exists, it is not readily available.

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.

---

[21] ICANN, "ICANN Current Financial Information (FY20 and FY21)," n.d., https://www.icann.org/resources/pages/governance/current-en, and ICANN, "IS-SSR Document Archive," n.d., https://www.icann.org/ssr-document-archive. Note: The ICANN budget does not report out on any specific SSR-related spending. The IS-SSR Document Archive does not show any IS-SSR Framework documents after FY 15-16.

[22] ICANN, "Internet Corporation for Assigned Names and Numbers (ICANN) FY21 Adopted Budget," 7 May 2020, 26-28, https://www.icann.org/en/system/files/files/adopted-budget-fy21-07may20-en.pdf.

[23] IS-SSR Document Archive, https://www.icann.org/ssr-document-archive

[24] ICANN, IS-SSR Framework – FY15-16, https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf.

[25] ICANN, "Security, Stability and Resiliency Framework," March 2013, 8, https://www.icann.org/en/system/files/files/ssr-plan-fy14-06mar13-en.pdf.

[26] ICANN, "Operating Plan of SSR Related Activities - FY18," n.d., https://community.icann.org/x/DqNYAw.

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 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.

This recommendation can be considered implemented when ICANN org moves all relevant functions and budget items under the new C-Suite position.

This recommendation can be considered effective when the ICANN community has a transparent view of the SSR-related budget.

3. Risk and Security Management

Security risk management is an ongoing process that allows an organization to identify security risks and implement strategies to mitigate those risks. The review team found that while ICANN org initiated comprehensive and appropriate activities in the security risk management area, resulting in the DNS Risk Framework Working Group's report and the IS-SSR Framework for FY15-16, the outputs of those activities have not been kept up to date.[27] This lack of action puts the maturity of the security risk management efforts, specifically repeatability and definition of processes, in question.

Without current documentation available, the review team could not find evidence demonstrating ICANN org's compliance with industry standards and best practices.[28] The absence of current documentation includes a crucial lack of third-party audits on ICANN org's approach and implementation. In contrast, the review team notes that various contracted parties and ccTLDs are compliant with relevant security and industry standards, underlining that these standards are applicable in and for the DNS space.[29] Ultimately, the review team was unable to determine if the work undertaken by ICANN org in the area of security risk management is sufficient or not.

In the absence of current, publicly available information, members of the community and other parties (e.g., governments, registrants) are also unlikely to be able to assess ICANN org's work. This absence results in a lack of transparency that impacts ICANN org's core values and global

[27] ICANN, "DNS Risk Management Framework Report," DNS Risk Management Framework Working Group, last modified 4 October 2013, https://www.icann.org/public-comments/dns-rmf-final-2013-08-23-en and ICANN, IS-SSR Framework – FY15-16.

[28] See SSR2 Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications, SSR2 Recommendation 6: SSR Vulnerability Disclosure and Transparency, and SSR2 Recommendation 7: SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures.

[29] Examples of various ccTLD's that are certified in accordance to ISO/IEC 27001:2013 and/or ISO 22301:2012: DENIC https://www.denic.de/en/content-pool/information-security-master/, IIS https://internetstiftelsen.se/docs/27001-eng-Certificate.pdf, nic.at https://www.nic.at/en/the-company/certificates-and-awards, Nominet https://www.nominet.uk/security-at-nominet/.

trust in ICANN org and the DNS ecosystem. Proper management of risk and security requires clear processes that follow known international standards and best practice guidelines, as well as clear and publicly accessible responsibilities and structures. Third-party audits, if done according to accepted standards and followed by publicly available audit reports, will provide a different perspective, confirm that measures are appropriate, and build stronger trust between the community and ICANN org. Creating and maintaining security management structures and procedures will help ICANN org maintain its security stance more completely and independently of individual staff members.

The SSR2 Review Team is acutely aware that oversharing certain operational information can be problematic, particularly in security. Nevertheless, ICANN org manages a critical system with global impact and should provide security-relevant information and associated data to the community. Oversight for the disclosure processes (risk, security, and vulnerabilities), including determining moratorium timing and public disclosure, should fall within the C-Suite role mandate (see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management).

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.

4.2. ICANN org should adopt and implement ISO 31000 "Risk Management" and validate its implementation with appropriate independent audits.[30] 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).

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).

This recommendation can be considered implemented when ICANN org's risk management processes are sufficiently documented as per international standards (e.g., ISO 31000), and the organization has established a cycle of regular audits for this program that include the publication of audit summary reports.

[30] International Organization for Standardization, *ISO 31000 Risk Management*, https://www.iso.org/iso-31000-risk-management.html.

This recommendation can be considered effective when ICANN org has a strong, clearly documented risk management program.

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 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.

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.

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.

This recommendation can be considered implemented when ICANN org has an ISMS oriented alongside accepted standards (e.g., ITIL, ISO 27000 family, SSAE-18), with regular audits that validate the appropriate security management and management procedures.

This recommendation can be considered effective when ICANN org has an Information Security Management System that is thoroughly documented and adequately addresses current security threats and offers plans to address potential future security threats.

SSR2 Recommendation 6: SSR Vulnerability Disclosure and Transparency

The SSR2 Review Team recommends that ICANN org improve their internal processes in support of managing and reporting on SSR-related vulnerabilities through the following actions:

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.

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.

This recommendation can be considered implemented when ICANN org promotes the voluntary adoption of SSR best practices for vulnerability disclosures by contracted parties and implements associated vulnerability disclosure reporting.

These recommendations can be considered effective when ICANN org and the contracted parties have adopted SSR best practices and objectives for vulnerability disclosure.

4. Business Continuity Management and Disaster Recovery Planning

Given the criticality of the functions ICANN org operates, from the DNS to IANA registries (including the management and maintenance of critical registries like the root zone, IP and AS numbers, and protocol registries), ICANN org needs to engage in well planned, executed, and documented BC management as well as DR planning. Based on this critical role, the SSR2 Review Team believes ICANN org should have more robust, better-organized BC and DR programs. ICANN would benefit from following industry best practices, particularly the implementation and documentation of compliance with applicable international standards (e.g., ISO/IEC 27001, NIST 800-53). Independent audits should follow these actions to confirm the appropriateness of procedures.

The team reviewed available documentation regarding BC and DR. The most up-to-date documentation was from 2017.[31] As defined by ISO 22301 and 22730, best practice requires annual reviews of these policies and procedures. Independent audits are necessary to ensure that BC and DR plans are up to date and in line with the best practices appropriate for the criticality of the DNS. Overall, the SSR2 Review Team and ICANN org staff members were unable to find and present sufficiently detailed documentation that would allow for a proper assessment of ICANN org's implementation of their BC and DR plans. ICANN org has room for significant improvements in how it handles BC and DR for the essential functions it provides.[32]

Compliance with well-established international standards, as confirmed by external, third-party audits, is crucial for any organization that runs critical infrastructure for the Internet, even if that compliance is not legally required. External experts would contribute to the transparency and legitimacy of ICANN org's BC and DR plans and procedures through a public tender for auditors, along with the subsequent publication of the final audit (and, if necessary, redacted)

[31] SSR2 wiki, Review Team Review Team Documents & Drafts, "SSR2 questions and answers," n.d., 2, https://community.icann.org/pages/viewpage.action?pageId=64076120. Note: As per interviews with ICANN staff, "These documents are confidential and not published publicly for security reasons. There is an established Disaster Recovery plan for systems, a Continuity Plan for the IANA Functions, and a broader Continuity Plan under development for the wider ICANN organization to be delivered in 2019."

[32] The team is aware that ISMS, BC, DR, and ISO-compliant risk management interact and are interdependent. Nevertheless, the team considered it appropriate to give details on identified needs, implementation, and necessary steps.

reports. In particular, ISO 31000 “Risk Management,” the ISO/IEC 27000 family “Information Security Management Systems,” and ISO 22301 "Business Continuity Management" would be useful as guidance and, more importantly, serve as target standards for third-party, independent audits.[33] While ICANN org is unique in its organizational structure and mission, ISO standards are flexible and applicable to ICANN org, particularly when it comes to ICANN org and the IANA functions. The review team also considers the use of NIST standards appropriate, as long as ICANN org thoroughly documents the process and is audited independently by a respected third party.[34]

Evaluating appropriate BC and DR processes and procedures is work that builds on more general risk assessment activities, as described above Section D.3. Risk and Security Management. ICANN supports a system critical to the functioning of the Internet and therefore is one level above normal BC and DR requirements. A suspected compromise of key signing key (KSK) related procedures, particularly during a crisis, would constitute a considerable problem and must be avoided. The turbulent global issues of 2020, from the COVID-19 pandemic to significant societal unrest, demonstrate how having two sites in the same country (in this case, the United States) is insufficient and has resulted in unexpectedly high levels of risk to the BC and DR function within ICANN org. Travel bans equally impact different sites within the United States, and violent events also occurred in most of the major cities in the country at the same time. Furthermore, while extremely unlikely, both sites could be affected by other adverse events, such as earthquakes, fires, or other natural disasters. The types of risks that may impact ICANN org operations will evolve and ICANN org must respond accordingly through regular and documented evaluation of the BC and DR plans, including appropriate and timely planning and execution where changes are necessary.

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 purview, based on ISO 22301 "Business Continuity Management," identifying acceptable BC and DR timelines.[35]

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

[33] International Organization for Standardization standards and standard suites *ISO 31000, ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary,* and *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements.*

[34] U.S. Department of Commerce, National Institute of Standards and Technology. *NIST Special Publication (SP) 800-30 Rev. 1, Guide for Conducting Risk Assessments*. Gaithersburg, MD: U.S. Department of Commerce, 2012. https://doi.org/10.6028/NIST.SP.800-30r1 and U.S. Department of Commerce, National Institute of Standards and Technology, Computer Security Resource Center. *SP 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations*. Gaithersburg, MD: U.S. Department of Commerce, 2020. https://doi.org/10.6028/NIST.SP.800-53r5.

[35] ISO 22301:2019

with ISO 27031.[36] ICANN org should develop this plan in close cooperation with the Root Server System Advisory Committee (RSSAC) and the Root Server Operators (RSO).

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.

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.

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.

This recommendation can be considered implemented when ICANN org's BC and DR plans and processes are thoroughly documented according to accepted industry standards, including regular audits that those processes are being followed, and when a non-U.S., non-North American site is operational.

This recommendation can be considered effective when ICANN org can demonstrate how they can handle incidents that impact the whole U.S. or North America.

E. Contracts, Compliance, and Transparency around DNS Abuse

Since its founding, ICANN's mission has included "*coordinat[ing] the development and implementation of policies that are developed through a bottom-up consensus-based multistakeholder process and designed to ensure the stable and secure operation of the Internet's unique names systems*."[37] The SSR2 Review Team concludes that despite the above commitment, the current ICANN-coordinated system does not sufficiently address DNS abuse and its associated harms. Groups within and outside the ICANN community have noted this gap for many years.[38] Some of the most pointed communications on this topic have come from

[36] International Organization for Standardization standards and standard suites *ISO 27031*, *ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity.*

[37] ICANN Bylaws, Section 1.1(a), https://www.icann.org/resources/pages/governance/bylaws-en/#article1.

[38] Examples: "Open Letter to the ICANN Community from the Registries Stakeholder Group," 19 August 2020, https://docs.wixstatic.com/ugd/ec8e4c_00d2dbac27b24330b8342686e9c2e53a.pdf, and a Letter from the ICANN Business Constituency to the ICANN Board of Directors, Göran Marby, ICANN President and CEO, Keith Drazek, GNSO Council Chair, and the ICANN Community, 28 October 2019,

representatives of the world's governments via the Governmental Advisory Committee (GAC), who have asserted for over a decade that they do not find ICANN processes and procedures sufficient to address public safety interests.[39]

Abuse of the DNS for fraudulent or criminal purposes has existed before ICANN org.[40] The threat landscape, which used to revolve around spam, phishing, and fraud, has expanded to include more sophisticated attacks, e.g., malware, ransomware, and Business Email Compromise (BEC), that target businesses, governments, and the Internet of Things (IoT).[41] Malicious actors now include state-sponsored and commercial actors who develop industrial platforms to support abuse. The COVID-19 pandemic and associated quarantines have provided an expanded attack surface for opportunistic criminals.[42]

As noted below in Section E.1. Unachieved Safeguards for the New gTLD Program, DNS abuse was a key concern of all stakeholders at the time, and ICANN org had several opportunities to develop policies designed to ensure the stable and secure operation of the Internet's unique name system during that expansion of the global namespace. ICANN org also had an opportunity to serve as a leader in guiding the entire DNS and security communities towards a common set of terms, definitions, and data that would facilitate communication and collaboration, as noted in Section E.2. Challenges: Definitions and Data.

These opportunities still exist for ICANN org. The recommendations in this section offer ICANN org specific suggestions on where and how to improve the fulfillment of their own mission and to serve as a stronger leader in the DNS and security communities.

1. Unachieved Safeguards for the New gTLD Program

DNS abuse was a key concern in the launch of the New gTLD Program in 2010. Law enforcement, governments, security communities, and commercial and user interest groups all argued for contractual abuse-mitigation obligations in both the base New gTLD Registry Agreement and the 2013 Registrar Accreditation Agreement (RAA). As part of these deliberations, the ICANN community prepared a memorandum in 2009 proposing measures to mitigate malicious conduct in the New gTLD Program.[43] The memorandum included recommendations for vetting registry operators, defining registry-level abuse contacts and procedures, and centralized access to zone files. Unfortunately, there was a gap between the measures outlined in this memorandum and what emerged from the closed negotiations between ICANN org and registries. Later attempts to improve security practices through

https://www.bizconst.org/assets/docs/positions-statements/2019/2019_10October_28%20BC%20Statement%20on%20DNS%20Abuse.pdf.

[39] ICANN Governmental Advisory Committee, "GAC Statement on DNS Abuse," 18 September 2019, 1, https://gac.icann.org/file-asset/public/gac-statement-dns-abuse-final-18sep19.pdf.

[40] See Appendix F: Research Data on Reports of DNS Abuse Trends for more information on historic trends in this space.

[41] ICANN Security and Stability Advisory Committee, "SAC105: The DNS and the Internet of Things: Opportunities, Risks, and Challenges," 28 May 2019, https://www.icann.org/en/system/files/files/sac-105-en.pdf.

[42] Interpol, "Global Landscape on COVID-19 cyberthreat," April 2020, https://www.interpol.int/en/content/download/15217/file/Global%20landscape%20on%20COVID-19%20cyberthreat.pdf.

[43] ICANN, "Mitigating Malicious Conduct," New gTLD Explanatory Memorandum, 3 October 2009, https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf.

contractual amendments received criticism for lack of transparency and community engagement in the process.[44]

In 2013, ICANN's Competition, Consumer Trust, and Consumer Choice (CCT) Review Team reviewed the effectiveness of these safeguards explicitly intended to mitigate rates of abusive, malicious, and criminal activity in these new gTLDs. The CCT team commissioned an independent research study (hereafter, the SADAG report) that used public data sources to show that rates of abuse in the new gTLDs were higher than in legacy TLDs, implying the safeguards were ineffective.[45] The CCT final report concluded:

"Although abuse does not universally persist in all new gTLDs, it is endemic to many. More troubling, at present there is little recourse for the community to stop new gTLD registries and registrars associated with high levels of abuse. This in turn creates incentives for network operators to unilaterally block all traffic from specific TLDs or registrars, running counter to community goals for Universal Acceptance of new gTLDs.

The failure to prevent the spread of certain abusive activities to new gTLDs previously identified by the community is significant. The CCT Review Team recognizes the infrastructure role played by domain names in enabling abusive activities that impact the security, stability, and resiliency of the DNS, undermine consumer trust, and, ultimately, impact end-users around the globe. Accordingly, this is a high-priority topic that must be addressed before any further expansion of the DNS, and the review team offers several recommendations to remedy the deficiencies of the status quo and improve the security of the DNS."[46]

The CCT review and associated SADAG report, as well as other third-party reports, also found that after the launch of the New gTLD Program, some registries and registrars promptly established practices to quickly and substantially increase domain registrations, e.g., bulk registrations, many of which are used for abuse and criminal activities.[47] Spamhaus (among others) also publishes what they estimate as the most-abused TLDs and registrars, and certain entities appear on these lists year after year.[48] Alpnames, highlighted in the SADAG report as

---

[44] ICANN GNSO Business Constituency, "Comment on Proposed Amendments to Base New gTLD Registry Agreement," Business Constituency Submission, version 3, 20 July 2016, https://www.bizconst.org/assets/docs/positions-statements/2016/2016_07july_20%20bc%20comment%20on%20proposed%20gtld%20base%20registry%20agreement%20final.pdf.

[45] Korczyński, Maciej , Maarten Wullink, Samaneh Tajalizadehkhoob, Giovane C.M. Moura, and Cristian Hesselman, "Statistical Analysis of DNS Abuse in gTLDs Final Report," SIDN Labs and the Delft University of Technology, August 2017, accessed 3 August 2018, https://www.icann.org/public-comments/sadag-final-2017-08-09-en.

[46] Competition, Consumer Trust, and Consumer Choice Review Team, "Competition, Consumer Trust, and Consumer Choice: Final Report," ICANN, 8 September 2018, https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf, and Piscatello, Dave, "Weaponizing Domain Names: how bulk registration aids global spam campaigns," Spamhaus, 21 March 2020, https://www.spamhaus.org/news/article/795/weaponizing-domain-names-how-bulk-registration-aids-global-spam-campaigns.

[47] Ibid., and, Piscitello, Dave, "Weaponizing Domain Names: how bulk registration aids global spam campaigns," Spamhaus, 21 March 2020, https://www.spamhaus.org/news/article/795/weaponizing-domain-names-how-bulk-registration-aids-global-spam-campaigns.

[48] Spamhaus, "The World's Most Abused TLDs," accessed 5 December 2020, https://www.spamhaus.org/statistics/tlds/, and Spamhaus, "The World's Most Abused Domain Registrars,"

one of the most egregious registrars involved in DNS abuse, offered cheap bulk registrations and "*has acted as the sponsoring registrar for 53.97%(59,044) of the new gTLD domains that have been blacklisted by Spamhaus.*"[49] ICANN Contractual Compliance did not sufficiently address this ongoing, systemic abuse even after many organizations repeatedly called their attention to it.[50] ICANN Contractual Compliance did not de-accredit Alpnames until after they became aware that Alpnames had ceased operations.[51] Our hope is that ICANN org and the DNS industry can demonstrate measurable progress on DNS abuse prevention and mitigation. Otherwise, governments will likely conclude the ICANN model of industry self-governance is no longer fit for purpose.

As noted in the WHOIS2/RDS Review, ICANN Contractual Compliance has an opportunity to be proactive in addressing "*suspected systemic issues, inaccuracy complaints reported, RDS accuracy studies or reviews or DAAR reports to, research, analyze and enforce against inaccuracy in the registration data*."[52]

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 domain name system for end-users, businesses, and governments.

This recommendation can be considered implemented when ICANN org has included abuse and security specialists in these negotiations and the management of the domain name system aligns with public safety and consumer interests, and not just those of the domain name industry.

---

accessed 5 December 2020, https://www.spamhaus.org/statistics/registrars/. Note: the supporting material on the Spamhaus pages offers insight into how they determine "bad" domains and registrars.

[49] SADAG Report, 19, https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf.

[50] Letter from Adobe Systems, DomainTools, eBay, Facebook, Microsoft, and Time Warner (aka, Independent Compliance Working Party) to Jamie Hedlund, SVP, ICANN Contractual Compliance & Consumer Safeguards and Managing Director, Washington D.C. Office, 27 February 2018, https://www.icann.org/en/system/files/correspondence/vayra-to-hedlund-27feb18-en.pdf.

[51] Letter from Jamie Hedlund, SVP, ICANN Contractual Compliance & Consumer Safeguards and Managing Director, Washington, DC Office to Iain Roache, Alpnames Limited, "RE: NOTICE OF TERMINATION OF REGISTRAR ACCREDITATION AGREEMENT", 15 March 2019, https://www.icann.org/uploads/compliance_notice/attachment/1113/hedlund-to-roache-15mar19.pdf.

[52] RDS-WHOIS2 Review Team, "Registration Directory Service (RDS)-WHOIS2 Review Final Report," 3 September 2019, https://www.icann.org/en/system/files/files/rds-whois2-review-03sep19-en.pdf, 46. Note: see Recommendation R4.1: "*The ICANN Board should initiate action to ensure ICANN Contractual Compliance is directed to proactively monitor and enforce registrar obligations with regard to RDS (WHOIS) data accuracy using data from incoming inaccuracy complaints and RDS accuracy studies or reviews to look for and address systemic issues. A risk-based approach should be executed to assess and understand inaccuracy issues and then take the appropriate actions to mitigate them.*"

This recommendation can be considered effective when a broader and more balanced set of stakeholders are able to have direct input into the contracts negotiated with contracted parties.

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.

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.

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.

9.4. ICANN org should task the Contractual 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.

This recommendation can be considered implemented when audits are happening regularly, and summaries published.

This recommendation can be considered effective when ICANN org has completed an audit successfully and reported out to the community.

This recommendation requires action from the ICANN Board and ICANN org. The Board might have to update its stance and instructions after completion of the anti-abuse Expedited Policy Development Process (EPDP) (see SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements).

2. Challenges: Definitions and Data Access

The SSR2 Review Team found two classes of persistent challenges to progress: one related to definitions and scope of abuse that ICANN contractual obligations can manage, and the other related to access to data that can inform detection, mitigation, prevention, and response to abuse. SSR2 Recommendations 11 through 14 target improved transparency and accountability in both areas.

A. Definitions of Abuse

During an April 2018 dialogue with the SSR2 Review Team, ICANN Contractual Compliance asserted that the current contracts with registries and registrars do not authorize ICANN org to require registries to suspend or delete potentially abusive domain names and are thus

ineffective in allowing them to pursue those engaged in systemic DNS abuse.[53] This point was also publicly asserted in the letter from ICANN Contractual Compliance to the Independent Compliance Working Party.[54]

A year later, in April 2019, ICANN Contractual Compliance reported to the SSR2 Review Team that lack of a contractual prohibition on "systematic DNS abuse" prevents ICANN Contractual Compliance from effectively addressing it until there is a community consensus policy defining and prohibiting it.[55] Further, the ICANN Board recently announced that it would delay moving forward with CCT Review recommendations 14 and 15, which recommend amendments to existing agreements to help prevent DNS abuse. The Board underlined that this delay is because "*there are still ongoing community discussions to reach a common community understanding of DNS abuse and related terms.*"[56] The SSR2 Review Team observes that the unstructured and unbounded nature of these discussions complicates finding a resolution and that ICANN org and contracted parties have an incentive to postpone resolution of this problem indefinitely. We recommend a three-pronged approach to this problem, including a temporary specification for a short-term, time-bounded CCWG for the medium-term, and a structured EPDP for the longer-term horizon.

ICANN org has had descriptions and working definitions of "DNS abuse" and related terms integrated with its activities for over a decade, including (but not limited to) ICANN org's Security, Stability, and Resiliency Frameworks from 2009 to 2017,[57] the ICANN's consensus community findings in the New gTLD Program as well as subsequent consensus on

[53] Briefing Materials: Discussion with ICANN Compliance - Completed 14 May 2019, ICANN Compliance Response to SSR2 Questions as of 26 April 2019, https://community.icann.org/display/SSR/Briefing+Materials.

[54] Letter from Jamie Hedlund, SVP, ICANN Contractual Compliance & Consumer Safeguards and Managing Director, Washington, DC Office to the Independent Compliance Working Party, "RE: Letter of 27 February 2018 from Independent Compliance Working Party," 4 April 2018, https://www.icann.org/en/system/files/correspondence/hedlund-to-vayra-04apr18-en.pdf. See also footnote 44 re: Letter of 27 February 2018 from the Independent Compliance Working Party.

[55] Briefing Materials, https://community.icann.org/display/SSR/Briefing+Materials, 4. Note: see response to question 6.

[56] ICANN Board, "Approved Resolutions | Regular Meeting of the ICANN Board," Main Agenda, Competition, Consumer Trust, Consumer Choice Review Team (CCT-RT) Pending Recommendations, 22 October 2020, https://www.icann.org/resources/board-material/resolutions-2020-10-22-en#2.a.

[57] IS-SSR Document Archive, https://www.icann.org/ssr-document-archive.

safeguards,[58] the 2013 Specification 11b contractual obligation which enumerates abusive activities,[59] and ICANN's own DNS Abuse Activity Reporting (DAAR) project.[60]

The GNSO Council also asked the Registration Abuse Policies Working Group (RAPWG) to examine issues surrounding illicit uses of domain names. The final report stated:

"*The RAPWG acknowledges that e-crime is an important issue of the ICANN community. The Internet community frequently voices concern to ICANN about malicious conduct and, in particular, the extent to which criminals take advantage of domain registration and name resolution services. Various parties—including companies, consumers, governments, and law enforcement—are asking ICANN and its contracted parties to monitor malicious conduct and, when appropriate, take reasonable steps to detect, block, and mitigate such conduct.*"[61]

The RAPWG recommended a community process, supported by ICANN resources, to create non-binding best practices to help registrars and registries address the illicit use of domain names. Ten years later, ICANN org has still not made substantive progress on these issues. [62] (See also SSR2 Recommendation 9: Monitor and Enforce Compliance.)

B. Data Access

The second major challenge involves access to data about domain names that inform security operations and research. The four types of data that have received the most attention are registration data, which facilitates tracking abusive activity to the owner and operator of the associated domain, TLD zone file data (via the Centralized Zone Data Service (CZDS)), which supports security research, reported abuse data used to inform ICANN's analysis of DNS

[58] ICANN GNSO Registration Abuse Policies Working Group, "Registration Abuse Policies Working Group Final Report," 29 May 2010. https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf, 3. Note: this report defined abuse as "*an action that: a) causes actual and substantial harm, or is a material predicate of harm, and b) Is illegal or illegitimate, or is otherwise contrary to the intention and design of a stated legitimate purpose, if such purpose is disclosed.")* See also, ICANN Operations and Policy Research, "New gTLD Program Safeguards Against DNS Abuse," July 2016, https://newgtlds.icann.org/en/reviews/dns-abuse/safeguards-against-dns-abuse-18jul16-en.pdf, 3. Note: This report also used the RAPWG distinction between *registration* and *use* abuse, noting that registration abuse is more clearly in the scope of ICANN and GNSO policy making. They identified examples of registration abuse such as: cybersquatting, front-running, gripe sites, deceptive and/or offensive domain names, fake renewal notices, name spinning, pay-per-click, traffic diversion, false affiliation, cross-TLD registration scam, domain kiting/tasting. This RAPWG also identified forms of abuse: phishing, spam, malware/botnet command-and-control, DDoS, and fast flux.

[59] ICANN, "Base Registry Agreement – Updated 31 July 2017," Specification 11 (3)(a) and Specification 11 (3) (b), https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf and ICANN, "Advisory, New gTLD Registry Agreement Specification 11 (3)(b)," 8 June 2017, https://www.icann.org/resources/pages/advisory-registry-agreement-spec-11-3b-2017-06-08-en.

[60] See question "What types of security threats does DAAR observe?" ICANN org DAAR FAQ, https://www.icann.org/octo-ssr/daar-faqs/#security-threats. Specifically: Phishing, Malware, Botnet command-and-control, and Spam.

[61] RAPWG Final Report, 6, https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf.

[62] Letter from Claudia Selli, Chair, The ICANN Business Constituency, to Maarten Botterman, Chair, Members of the Board of Directors, Internet Corporation for Assigned Names and Numbers (ICANN), 9 December 2019, 1 and 3, https://www.icann.org/en/system/files/correspondence/selli-to-botterman-09dec19-en.pdf.

abuse, and contractual compliance data to support trend analysis and evaluation of operational approaches to mitigate abuse.

i. Registration Data

Since at least 2003, ICANN org has recognized the need to balance the need for transparency and accountability of domain name registration metadata, i.e., contact information for the owners of names, and legal requirements around the world that sometimes prohibit or complicate the sharing of such information.[63] The RAPWG found that the basic accessibility of the Registration Directory Service (RDS, formally known as WHOIS) has an inherent relationship to domain registration process abuses and is a key issue related to the malicious use of domain names.[64] They also found that RDS data is not always accessible on a guaranteed or enforceable basis, is not always provided by registrars in a reliable, consistent, or predictable fashion, and that users sometimes receive different RDS results depending on where or how they perform the lookup. This drove two RAPWG recommendations:

"The GNSO should request that the ICANN Compliance Department publish more data about WHOIS accessibility, on at least an annual basis. This data should include a) the number of registrars that show a pattern of unreasonable restriction of access to their port 43 WHOIS servers, and b) the results of an annual compliance audit of compliance with all contractual WHOIS access obligations."

And

"*The GNSO should determine what additional research and processes may be needed to ensure that WHOIS data is accessible in an appropriately reliable, enforceable, and consistent fashion*."[65]

In June 2018, responding to new GDPR-related difficulties in accessing registration data, ICANN's Security and Stability Advisory Committee (SSAC) urgently advised the ICANN Board to work to amend contracts to resolve the persistent problems with data access. None of these recommendations have as yet been implemented.[66] Per ICANN org's status report to the SSR2 Review Team (on 2 July 2020), ICANN org delegated these SSAC101 recommendations to the GNSO for its Phase 2 work plan of the EPDP on access to registration data.[67] None of these recommendations were ever part of the EPDP Phase 2 work plan, the topics were not discussed in the EPDP, and the GNSO has not taken up any related work. SSAC has made

[63] ICANN, "Revised ICANN Procedure For Handling WHOIS Conflicts with Privacy Law," 18 April 2017, https://whois.icann.org/en/revised-icann-procedure-handling-whois-conflicts-privacy-law.

[64] RAPWG Final Report, 71-80, https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf.

[65] Ibid., 79-80.

[66] ICANN Security and Stability Advisory Committee, "SAC101: SSAC Advisory Regarding Access to Domain Name Registration Data," Committee advisory, 14 June 2018, https://www.icann.org/en/system/files/files/sac-101-en.pdf. Note: SSAC published a "version 2" of the document, which substantially weakened the recommendations from version 1 for the ICANN Board to work to amend contracts to resolve the persistent problems with data access. https://www.icann.org/en/system/files/files/sac-101-v2-en.pdf. See pp 4-5 for the full text of the SSAC101v2 recommendations.

[67] Jennifer Bryce to the SSR2 Review Team mailing list, 2 July 2020, Subject: SAC097 and SAC102v2 status, https://mm.icann.org/pipermail/ssr2-review/2020-July/002280.html. See page 2 of the message attachment.

other attempts also, without observable impact.[68] Some security researchers have noted that the Temporary Specification for gTLD Registration Data now allows gTLD domain registrars to redact all domain contact data from publication in RDS, even those records not covered by a privacy law such as GDPR.[69]

This latest EPDP is the most recent and most amplified version of the debate on access to registration data.[70] The minority statements consistently found that the report recommendations did not appropriately balance the rights of those providing data to registries and registrars with the public interest to prevent harms associated with malicious activities that leverage the DNS.[71] The substantial dissent from the final report implies that this process has failed to achieve community consensus on policy related to data access. Noting that the "*currently fragmented system for disclosures*" combined with a relatively uncertain legal framework is part of the problem, ICANN's CEO has recently asked the EU Commission for legal clarity on GDPR's controllership provisions.[72]

The 2013 RAA included an Across Field Validation requirement for domain registration address data.[73] Across Field Validation is a common, automated validity check (e.g., if the house number exists on the street, which exists in the city and province, and the postal code is correct). As of the date of this report, ICANN org has not enforced this validation requirement. With respect to privacy and proxy registrations, ICANN org's GNSO Council unanimously supported an accreditation policy for privacy/proxy service providers, which could include enhancing

[68] Letter from the ICANN Security and Stability Advisory Committee to Russ Weinstein, Director, Registry Services and Engagement, and Jamie Hedlund, Senior Vice President, Contractual Compliance & Consumer Safeguard, "Subject: SSAC2019-02: Registration Data Services Query Reporting," 3 May 2019, https://www.icann.org/en/system/files/files/ssac2019-02-03may19-en.pdf. Note: SSAC released SSAC 2019-2 advising that ICANN org issue guidance to all registry operators, clarifying goals, expectations, and contractual obligations for reporting port 43 queries and RDAP queries. There is no evidence this has occurred.

[69] Aaron, Greg, Lyman Chapin, David Piscitello, and Dr. Colin Strutt, "Phishing Landscape 2020: A Study of the Scope and Distribution of Phishing", Interisle Consulting Group, LLC, 13 October 2020, http://www.interisle.net/PhishingLandscape2020.pdf.

[70] ICANN Generic Names Supporting Organization, "Final Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process," 31 July 2020, https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf.

[71] Ibid., Annex F - Minority Statement, pp 151-154. Includes minority statements from: At-Large Advisory Committee (ALAC), Business Constituency (BC) / Intellectual Property Constituency (IPC), Governmental Advisory Committee (GAC), Non-Commercial Stakeholder Group (NCSG), Registrar Stakeholder Group (RrSG), Registry Stakeholder Group (RySG), Security and Stability Advisory Committee (SSAC).

[72] Letter from Göran Marby, President and Chief Executive Officer, Internet Corporation for Assigned Names and Numbers (ICANN), to Mr. Roberto Viola Director General, DG Communications Networks, Content & Technology European Commission, Ms. Monique Pariat Director General, DG Migration and Home Affairs European Commission, and Ms. Salla Saastamoinen Acting Director General, DG Justice and Consumers European Commission, 2 October 2020, https://www.icann.org/en/system/files/correspondence/marby-to-viola-et-al-02oct20-en.pdf.

[73] ICANN, "2013 Registrar Accreditation Agreement," accessed 8 December 2020, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en. Note: See Section 1(e) of the Whois Accuracy Program Specification, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#whois-accuracy.

operational practices involving responses to law enforcement and intellectual property holders.[74] The ICANN Board approved the policy in August 2016.[75] As of October 2020, ICANN has not implemented these requirements and the website dedicated to this work item has not been updated since March 2018.[76]

ii. Centralized Zone Data Service

Access to zone files has always been an important aspect of security-related operations and research. As part of the gTLD program, the community agreed for new gTLD registries to accept contractual obligations to "*provide zone data to approved requesters (e.g. law enforcement agents, IP attorneys, researchers) upon technical delegation of its gTLD.*"[77] However, usable, comprehensive access to this data has been problematic, such as when it comes to requesting and renewing access and acquiring the actual files.[78] At the moment, registries do not grant access as intended and revoke access periodically with long renewal processes.[79] These data are regularly used for studying abuse in the DNS.[80] SSAC wrote an advisory on this topic in June 2017 (SAC097), more than three years ago.[81] The ICANN Board accepted the recommendations but has still not executed them.[82] The SSR2 Review Team recognizes that certain TLDs (like brand TLDs) might require accommodations when it comes to CZDS due to brand protection or security concerns, but in general, access to critical data via the CZDS remains problematic.[83]

---

[74] ICANN, "Privacy and Proxy Services," accessed 8 December 2020, https://whois.icann.org/en/privacy-and-proxy-services. Note: see section 2, "Process of Adopting Policy Recommendations."

[75] Ibid.

[76] Registrar WHOIS Validation Working Group, "Documents," last updated 21 March 2018, https://community.icann.org/display/AFAV/Documents.

[77] ICANN, "CZDS Centralized Zone Data Service," accessed 7 December 2020, https://czds.icann.org/home.

[78] Piscitello, Dave, "Unspecific CZDS contract language makes zone data access approvals a dice roll," blog, The Security Skeptic, 13 August 2019, https://www.securityskeptic.com/2019/08/unspecific-contract-language-makes-zone-data-access-approvals-a-dice-roll.html.

[79] Piscitello, Dave, "Unspecific CZDS contract language makes zone data access approvals a dice roll," The Security Skeptic blog, 14 August 2019, https://www.securityskeptic.com/2019/08/unspecific-contract-language-makes-zone-data-access-approvals-a-dice-roll.html, and ICANN SSAC, "SAC 096: SSAC Advisory Regarding the Centralized Zone Data Service (CZDS) and Registry Operator Monthly Activity Reports," 16 June 2017, https://www.icann.org/resources/files/1207653-2017-06-16-en.

[80] Claffy, KC, and David Clark, "Workshop on Internet Economics (WIE 2019) Report," April 2020, https://ccronline.sigcomm.org/2020/ccr-april-2020/workshop-on-internet-economics-wie-2019-report%EF%BB%BF/.

[81] ICANN Security and Stability Advisory Committee, "SAC097: SSAC Advisory Regarding the Centralized Zone Data Service (CZDS) and Registry Operator Monthly Activity Reports," 12 June 2017, https://www.icann.org/en/system/files/files/sac-097-en.pdf.

[82] ICANN Security and Stability Advisory Committee, "Security and Stability Advisory Committee (SSAC) Advice Status," last updated 31 October 2020, https://features.icann.org/board-advice/ssac. See "SAC097: SSAC Advisory Regarding the Centralized Zone Data Service (CZDS) and Registry Operator Monthly Activity Reports, R-1 (12Jun2017)."

[83] Partridge, Mark VB, and Jordan A. Arnot. "Expansion of the domain name system: advantages, objections and contentions." DePaul J. Art Tech. & Intell. Prop. L 22 (2011): 317 (see page 5 of the article), and "CZDS-API-Testbed -- Mailing list for CZDS API users to sign up for and participate in API discussion topics," https://mm.icann.org/mailman/listinfo/czds-api-testbed. See complaint threads in archive (note that access is restricted to subscribers, but subscription is open.)

After the Board resolution of June 2018, the number of zone file access complaints increased, and they remain higher than they were in mid-2018. They are now the largest category of complaints about registry operators.[84] ICANN Contractual Compliance sometimes has not processed ZFA complaints for months after the complaints were submitted.[85] In 2018, ICANN org requested the New gTLD Subsequent Procedures Working Group (commonly referred to as the SubPro WG) to address this problem.[86] The SubPro WG did not include any mention of it in their recent 363-page draft report.[87] There is no evidence that ICANN org, ICANN Board, or the registry community has taken sufficient action to resolve CZDS access issues. SSR2 Recommendation 11 Resolve CZDS Data Access Problems focuses on this problem.

iii. DNS Abuse Activity Reporting

The ICANN DNS Abuse Activity Reporting (DAAR) project is a "*platform for studying domain name registration and security threat (abuse) behavior across top-level domain (TLD) registries and registrars*" with an overarching purpose "*to report security threat activity to the ICANN community, which can use the data to make informed decisions.*"[88] ICANN org began its DAAR program in 2017. ICANN org claimed that DAAR was intended to provide the community with a transparent, reproducible scientific approach to reporting DNS abuse.[89] Since January 2018, ICANN OCTO has been publishing a high-level monthly report based on analysis of DAAR data, but at a granularity that does not allow conclusions about which registrars/registries are harboring significant abuse. ICANN org also does not share complete (raw) data with researchers who could help improve the methodology or confirm findings. OCTO staff told the SSR2 Review Team that these objectives (actionable data, validation) were not DAAR design goals.[90] The SSR2 Review Team finds the way that ICANN org is apparently structuring agreements with data providers to be a significant inhibitor of these goals and proposes an overhaul of its DNS Abuse Analysis program with transparency, reproducibility, and actionable data products as its primary objectives.

Identifying registries and registrars harboring disproportionate levels of abuse would facilitate informed policymaking and add a measure of transparency and accountability to the domain name registration system that does not exist today. Indeed, the review team is not sure what use ICANN's investment in this area serves if the data and analyses are neither actionable nor shared for the purpose of reproducibility and validation. The SSR2 Review Team believes that discontinuing the DAAR program would be appropriate if the community and ICANN org were unable to overhaul DAAR to achieve these objectives. SSR2 Recommendation 12: Overhaul

[84] ICANN, "Contractual Compliance Performance Measurement," accessed 7 December 2020, https://features.icann.org/compliance/dashboard/report-list. Note that Zone Access File complaints accounted for 85.5% of complaints as of March 2020, vs 31.9% in March 2018.

[85] "CZDS-API-Testbed -- Mailing list for CZDS API users to sign up for and participate in API discussion topics," https://mm.icann.org/mailman/listinfo/czds-api-testbed. See complaint threads in archive (note that access is restricted to subscribers, but subscription is open.)

[86] ICANN, "New gTLD Subsequent Procedures Working Group Charter," 21 January 2016, https://gnso.icann.org/sites/default/files/filefield_48475/subsequent-procedures-charter-21jan16-en.pdf.

[87] ICANN New gTLD Subsequent Procedures Working Group, "GNSO New gTLD Subsequent Procedures Draft Final Report," accessed 7 December 2020, https://www.icann.org/public-comments/gnso-new-gtld-subsequent-draft-final-report-2020-08-20-en.

[88] DAAR FAQ, https://www.icann.org/octo-ssr/daar-faqs/#security-threats.

[89] Piscitello, Dave, "The Domain Abuse Activity Reporting System (DAAR)," ICANN APWG EU Report, October 2017, https://www.icann.org/en/system/files/files/presentation-daar-31oct17-en.pdf.

[90] Call transcript, "SSR2 call on DAAR - 24 June 2020 @ 15:00 UTC," https://community.icann.org/x/WIJIC.

DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review focuses on this problem.

iv. Complaints

The CCT report noted the difficulty of evaluating the impact of safeguards given the lack of transparency from ICANN Contractual Compliance regarding complaints and lack of enforcement of public interest commitments in contracts.[91] The SSR2 Review Team found that a key issue for reporters of malicious domains is the complicated nature of complaint submission, differing requirements between contracted parties, and often a lack of (timely) response or action. The SSR2 Review Team believes that a centralized system to submit abuse complaints would simplify the abuse complaint process for both submitters as well as contracted parties and reduce the number of misdirected complaints.

The SSR2 Review Team believes that an overhauled DNS Abuse Analysis program would enable ICANN Contractual Compliance to establish standard expectations regarding the prevalence of abuse. Since blocklists may not be 100% accurate and can be manipulated, ICANN will have to put effort into validating analysis results, and contracted parties must have the opportunity to refute ICANN's notice.

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 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.

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.

This recommendation can be considered implemented when ICANN org publishes the web page that includes the first output of the CCWG as well as the process for keeping the web page up to date.

[91] CCT Report, 9-10, https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf.

This recommendation can be considered effective when ICANN org is able to offer increased transparency and accountability with respect to accepted and community-vetted descriptions and clarity to community discussions and interpretation of policy documents, thus enabling other stakeholders to define codes of conduct around DNS abuse.

SSR2 Recommendation 11: Resolve CZDS Data Access Problems

11.1. The ICANN community and ICANN org should take steps to ensure that access to CZDS data is available, in a timely manner and without unnecessary hurdles to requesters, e.g., lack of auto-renewal of access credentials.

This recommendation can be considered implemented when ICANN org and the community makes access to CZDS data available in a timely manner and without unnecessary hurdles to requesters.

This recommendation can be considered effective when ICANN org reports a decrease in the number of zone file access complaints and improves the ability for researchers to study the security-related operations of the DNS.

This recommendation aims to establish proper access to the security-relevant zone file data used by academics and security specialists. This recommendation requires action from the ICANN Board, ICANN org, and the GNSO.

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.

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.

12.3. ICANN org should publish reports that identify registries and registrars whose domains most contribute to 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.

This recommendation can be considered implemented when ICANN org's DNS Abuse Analysis efforts introduce metrics that produce actionable, accurate, and trustworthy data.

This recommendation can be considered effective when all of the data available to ICANN org is also available to the community and independent researchers, perhaps with a time delay, to provide validation and feedback.

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 gTLDs; the participation of each ccTLD would be voluntary. In addition, ICANN org should share abuse reports (e.g., via email) with all ccTLDs.

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.

This recommendation can be considered implemented when ICANN org simplifies the process of submitting and receiving abuse complaints and offers insight into the number of complaints and some metadata (e.g., type of abuse reported, dates, time to resolution) for researchers and community members. This recommendation can be considered complete when the portal is up and running.

This recommendation can be considered effective when contracted parties have to spend less time on misdirected complaints, and the research community as well as the broader ICANN community can see and study the associated data about those complaints.

Due to the complexity of this enterprise, this recommendation is expected to take several years (at least three) after the ICANN Board approves the implementation of this recommendation.

3. Policy Development Process (PDP) Alternatives

It is important to address claims that a consensus policy developed by a Policy Development Process (PDP) is the only path to implementing several of our recommendations. There are many ways the ICANN Board can move forward on implementing our recommendations. The Board could choose contract negotiations, issue advisories to contracted parties, or use a time-limited and expert-supported cross-community working group.[92] ICANN org could even issue a Temporary Specification based on a Board conviction that DNS abuse is an acute public safety concern that needs urgent attention. The Board's recent use of the Temporary Specification in response to the inconsistencies between the EU's GDPR and ICANN org's own Bylaws is a useful case study. The ICANN community had years to develop a registration data access

[92] Past examples for advisories to contracted parties are available on the Registrar Advisories website (https://whois.icann.org/en/registrar-advisories).

policy that would be consistent with the GDPR but effectively postponed the problem. We see a similar pattern with respect to DNS abuse and access to registration data to fight abuse.

ICANN org can and does conduct bilateral contract negotiations. Changes to ICANN org's registrar and registry contracts have occurred without a consensus policy created by a PDP. When ICANN org upgraded to the 2013 RAA and 2017 Base Registry Agreement, ICANN org and a negotiating team representing the respective industry managed the process, without any PDP. The community had an opportunity to comment on draft text, but only the negotiating team was involved in the discussions and decisions.[93] These closed-door negotiations between ICANN org and the contracted parties are a valuable vehicle for progress but are limited when it comes to DNS abuse because these negotiations exclude all other stakeholders including governments, businesses, and the public that all have an interest in reducing abusive registrations. SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review addresses this gap.

Especially in the wake of the EPDP being unable to resolve access to registration data, the tremendous conflicts of interest that weigh down the PDP process, and the slow progress in addressing DNS anti-abuse, the review team believes that an EPDP process concerned with abuse will not bring about an effective solution on its own. The EPDP on access to registration data took years to complete, and the final product garnered dissent from a majority of the ICANN community; there were substantial minority statements from the At-Large Advisory Committee (ALAC), Business Constituency and Intellectual Property Constituencies (BC/IPC), Noncommercial Stakeholder Group (NCSG), Registrars Stakeholder Group (RrSG), and Registries Stakeholder Group (RySG). The BC/IPC minority report warned: "*Regulators and legislators should note that the ICANN multi-stakeholder model has failed the needs of consumer protection, cybersecurity, and law enforcement.*"[94] SSAC's minority report also warned that ICANN's policy development process "*has not provided outcomes that are reasonably suitable for security and stability.*"[95]

In summary, mitigating, preventing, and stopping existing DNS abuse is challenged by the ambiguity of existing terminology and contractual requirements, conflicts of interest across all parties who would need to act, and varied commitments of governments around the world to also address DNS abuse via other legal processes. Some DNS abuse-related policies and contractual obligations already exist, but ICANN org and contracted parties need to more effectively implement and enforce them, and the community needs to develop additional policies, contractual obligations, and activities to keep pace with DNS abuse. The SSR2 Review Team views DNS abuse as a critical need that warrants and justifies strong ICANN leadership in this area. The GDPR Temporary Specification demonstrated that the ICANN Board maintains policymaking authority in response to various needs. Moreover, the Board has fiduciary duties to ensure ICANN org policies and derivative contracts are fit for purpose for ICANN org as a

[93] 2013 Registrar Accreditation Agreement, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en. Note: ICANN can amend contracts either through consensus policy or by negotiation between ICANN org and the other relevant parties to the contract as per the RAA, Section 1.2, Consensus Policies and Temporary Policies Specification, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#consensus-temporary.

[94] GNSO EPDP Phase 2 Report, BC/IPC Minority Statement, 114-121, https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf.

[95] Ibid., 145-162, SSAC Minority Statement.

California non-profit public benefit corporation tasked with oversight of DNS security, stability, and policymaking in the public interest. A new Temporary Specification combined with a new EPDP may be the best approach.[96]

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.

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.

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 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.

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.

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 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.[97]

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

[96] The SSR2 Review Team believes that ICANN org has compiled a sufficient body of knowledge, including the knowledge that led to the DAAR program and the DAAR reports themselves, to compile an Issues Report, thus justifying starting an EPDP rather than a PDP.

[97] ICANN, "PDP Team Charter," page last edited 23 July 2018, 12-14, https://community.icann.org/display/EOTSFGRD/EPDP+Team+Charter.

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.

SSR2 Recommendations 14 and 15 can be considered implemented when ICANN Contractual Compliance has the tools to appropriately respond to contracted parties failing to respond to DNS abuse, specifically the existence of anti-abuse related obligations in all relevant contracts and agreements.

SSR2 Recommendations 14 and 15 can be considered effective when ICANN Contractual Compliance uses those tools to deal with egregious policy violations on the part of contracted parties.

The intended outcome of SSR2 Recommendations 14 and 15 is to empower ICANN Contractual Compliance to deal with the worst offenders when it comes to DNS abuse, which the ICANN Contractual Compliance team has stated it lacks sufficient tools to do.

These recommendations require action from ICANN org and the ICANN community and are intended to guide policy creation. These recommendations are attainable, but ICANN org can only complete them over time.

4. Privacy and Data Stewardship

Privacy is a constantly evolving issue due to the ever-increasing amount of data collection and analysis by third parties (in addition to the traditional government entities) as well as the evolving privacy legislation landscape. The SSR2 Review Team concludes that ICANN org has not been as proactive as it should be given the changing landscape, as evidenced by its inconsistencies in the data available in and about the RDS.[98]

There is a proliferation of web pages with no dates associated with them throughout the ICANN website that discuss various aspects of the privacy of registration data. This lack of timestamps made it impossible for the review team to do reasonable research on ICANN org's history on this topic.[99] As of October 2020, the RDS website and related documentation are also out of date and do not include or reference relevant community documents. There are a few ICANN web pages on RDS, but these do not cross-reference. ICANN's current RDS web page was last updated in 2017, and thus does not reference the current Temporary Specification measures or EPDP status.[100] The review team considers the lack of information and consistency on the website to be reflective of ICANN org's own lack of clarity and consistency on the issues surrounding privacy.

[98] See Section E.2.b.i. Registration Data and Section E.2.b.ii. Centralized Zone Data Service in this report.

[99] Examples include: https://whois.icann.org/en/privacy-and-proxy-services, https://whois.icann.org/en/privacy, https://whois.icann.org/en/revised-icann-procedure-handling-whois-conflicts-privacy-law, and https://www.icann.org/rdap. Note: These pages all seem to be many years old, and several include a note at the bottom: "On 17 May 2018 the ICANN Board adopted a Temporary Specification for gTLD Registration Data. This page is under review and will be updated to address the Temporary Specification."

[100] ICANN, "About WHOIS," last updated July 2017, https://whois.icann.org/en/about-whois.

In Section E.2.b.i. Registration Data, the review team also pointed out the need to balance transparency and accountability of domain name registration metadata in light of various privacy regulations such as the GDPR. By ensuring consistency in its own website as well as in the consensus policies and agreements with registry operators and registrars, ICANN org will help ensure the safe management and protection of collection, retention, escrow, transfer, and display of registration data, which includes contact information of the registrant, administrative, and technical contacts as well as technical information associated with a domain name.

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 stewardship, with particular attention to the information around the 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).

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.

This recommendation can be considered implemented when ICANN org's actions regarding privacy and their management of the RDS are properly documented, and specifically assigned resources within ICANN org keep the organization in line with current best practices and legal requirements in this space.

This recommendation can be considered effective when ICANN org can demonstrate ongoing compliance with best practices and legal requirements in data handling and privacy.

F. Additional SSR-related Concerns Regarding the Global DNS

The SSR2 Review Team recognizes that ICANN org is just one of the many entities in the DNS ecosystem. That said, ICANN org is among those in a unique position to influence and guide SSR-related actions across the entire ecosystem. This section offers specific recommendations for where ICANN org can improve its policies and practices for itself and the entire global DNS. By modeling best practices in the management of the IMRS, sharing the consolidated input of researchers, offering tools for testing and analysis, and other possible actions discussed in this section, ICANN org can take steps to improve both its own SSR actions and help others understand how to improve theirs.

1. Name Collision

While ICANN org provides detailed material and training on name collision, there is no restriction of registrants utilizing a unique identifier for a private zone that collides with a public zone. The SSR2 Review Team believes that the recently concluded and published study (hereafter referred to as the 2019 NCAP study) is a step in the right direction to handle unwanted name collisions.[101] However, this study did not address the continued need for mechanisms to discover unreported name collisions, both malicious and accidental. The study also concluded that there was no recent research on name collisions (since 2017) and took the decrease in reported name collisions as an indicator that the current mechanisms are working.[102] On the other hand, peer-reviewed research in 2016 found that the last round of gTLDs measurably exacerbated the name collision problem.[103] The decrease of reported name collisions as indicated by traditional reporting mechanisms may not imply the absence of name collisions. Instead, the nature of name collisions may have changed in such a way as to evade those traditional mechanisms. There has also been a decrease in the delegation of new gTLDs in recent years, which may further impact the absolute numbers of reported name collisions.[104]

Even though a controlled interruption framework was proposed to avoid potential name collision of domain names in a 2014 ICANN-commissioned report (hereafter referred to as the Phase One Report), this controlled interruption framework has never been tested against evolving name collision attack scenarios.[105] For example, SSAC advised that "*Instead of a single controlled interruption period, ICANN should introduce rolling interruption periods, broken by periods of normal operation, to allow affected end user systems to continue to function during the 120-day test period with less risk of catastrophic business impact.*"[106] In the Phase One Report, the authors based some of their inferences on the lack of email and phone calls from second-level domain registrants, which does not adequately reflect the complexity of the problem.[107] The Phase One Report also discussed several alternate approaches to the controlled interruption framework, including the use of honeypots, DNAME, and string-to-string approaches, but these approaches were never considered for implementation.[108] The SSR2 Review Team concludes, in contrast to the Phase One Report, that name collision is still a challenge that merits further study and mitigation.

---

[101] Scarfone, Karen, "Managing the Risks of Top-Level Domain Name Collisions: Findings for the Name Collision Analysis Project (NCAP) Study," ICANN OCTO, 27 May 2020, https://www.icann.org/en/system/files/files/managing-risks-tld-2-name-collision-07may20-en.pdf.

[102] Ibid, 43.

[103] Chen, Qi Alfred, Eric Osterweil, Matthew Thomas, and Z. Morley Mao. "MitM Attack by Name Collision: Cause Analysis and Vulnerability Assessment in the New gTLD Era." 2016 IEEE Symposium on Security and Privacy (SP) (May 2016), 675-690. doi:10.1109/sp.2016.46.

[104] ICANN, New gTLD website, https://newgtlds.icann.org/en/program-status/statistics. Note: as of 12 December 2020, only 9 gTLDs remain in process of the original 1930 available.

[105] ICANN, "Mitigating the Risk of DNS Namespace Collisions Phase One Report," 6 July 2014, 6, https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf, and ICANN, "Name Collision Occurrence Management Framework," 30 July 2014, 2-3, https://www.icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf.

[106] ICANN SSAC, "SAC066: SSACComment Concerning JAS Phase One Report on Mitigating the Risk of DNS Namespace Collisions," 6 June 2014, 4, https://www.icann.org/en/system/files/files/sac-066-en.pdf.

[107] Mitigating the Risk of DNS Namespace Collisions Phase One Report, 22, https://www.icann.org/en/system/files/files/name-collision-mitigation-study-06jun14-en.pdf.

[108] Ibid.

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.

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.

This recommendation can be considered implemented when ICANN org produces a framework to produce findings that characterize the nature and frequency of name collisions and resulting concerns by identifying metrics and devising mechanisms to measure the extent to which the controlled interruption mechanism is successful.

The recommendation can be considered effective when ICANN org and the community are able to detect, act on, and ultimately minimize the existence of name collisions and respond to evolving name collision scenarios.

This recommendation must be completed before the next round of gTLDs.

2. Research and Briefings

An enormous amount of activity is now occurring in the academic research community related to SSR issues in the naming, routing, and addressing layers. The ICANN community has an opportunity to leverage this activity and expertise to inform policies and technology development that will measurably reduce SSR-related harms in the ecosystem. But there is no existing function to make sure ICANN org itself and the community it serves stay aware of these developments.

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 contracted party behavior.[109]

[109] Conference links: ACM CCS <https://dl.acm.org/conference/ccs>, ACM Internet Measurement Conference <https://www.sigcomm.org/events/imc-conference>, Usenix Security <https://www.usenix.org/conferences>, CCR <https://www.ccrsummit.com/>, SIGCOMM <https://www.sigcomm.org/>, IEEE Symposium on Security and Privacy <https://www.ieee-security.org/index.html>, FIRST <https://www.first.org/>. Note: The suggested implementation could be to contact the organizers (technical program committee chairs, steering group organizers, etc.) and ask for digests of the proceedings and/or invite committee members from these venues to

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.

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.

This recommendation can be considered implemented when ICANN org creates and maintains a public archive of digests or readouts from various networking and security research conferences.

This recommendation can be considered effective when the information coming from the research community on SSR-related issues is more accessible to people who are making policy decisions.

3. DNS Testbed

As the DNS ecosystem is already large and growing, maintaining and monitoring a regression test suite and testbed to analyze DNS behaviors and interactions is critical. The SSR2 Review Team has concluded that the ongoing DNS testbed activities by OCTO, once complete, sufficiently address this concern.[110] The review team further believes that support and maintenance of this testbed (as well as ingestion of its results and findings) is a requirement of ICANN org.

Timely completion and maintenance of this testbed would allow the ICANN community to test and research resolver behavior, which is crucial for ensuring the integrity and global availability of the DNS.

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.

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.

This recommendation can be considered implemented when ICANN org finishes developing a publicly accessible test suite for community testing and research into resolver behavior.

This recommendation can be considered effective when there is a test suite available with an annual update cycle that helps ensure the integrity and global availability of the DNS.

present relevant digests of their proceedings yearly, at one of the ICANN Community events. In such an implementation, ICANN org would preserve the readouts in an archived report.

[110] "Resolver Testbed," ICANN GitHub repository, https://github.com/icann/resolver-testbed.

4. Root Zone and Registry Concerns

A. Key Rollover

The DNSSEC key signing key (KSK) for the root zone rolled over on 11 October 2018 for the first time since the establishment of the Deliberately Unvalidatable Root Zone (DURZ) key.[111] During the rollover process, there was much debate and many calls for analyses of the details of the roll.[112] One result of the SSR2 Review Team's analysis was the understanding that properly functioning exception legs in the procedure are necessary for a secure and successful key rollover.[113] ICANN org delayed the rollover for a year while the organization took measurements to allay concerns. Discussions within the ICANN community have already begun about the timing and procedure for future rollovers, including the consideration of potential new complexities, e.g., algorithm rollovers.[114] ICANN org subsequently held an open call for comments on the process for the next scheduled KSK rollover process.[115]

Due to the criticality of security protections that are (and will be) derived from the DNSSEC-signed root zone, formally verifiable process analyses are critical to ensuring the security, stability, and resilience of the process by which DNSSEC protections are maintained during root zone KSK key rollovers.[116] Formal process modeling employs a methodology and/or programming environment to specify each task in a process, evaluate its execution (success, fail, other, etc.), and specify the follow-on actions under different results. Process-specifications like this have shown utility in complex inter-human processes that include election security, medical process safety, and more.[117] In these cases, people's tasks (in human-space) are complex and modeled in formal process-specification languages, and critical (and critical-to-life) choices and consequences are symbolically modeled and formally tracked. This modeling allows for quantitative prescriptions and predictions of what should be done and what can be

[111] ICANN, "First Root KSK Rollover Successfully Completed," 15 October 2018, https://www.icann.org/news/announcement-2018-10-15-en.

[112] ICANN, "The Recent KSK Rollover: Summary and Next Steps," ICANN blog, 30 January 2018, https://www.icann.org/news/blog/the-recent-ksk-rollover-summary-and-next-steps, and Moritz Müller, Matthew Thomas, Duane Wessels, Wes Hardaker, Taejoong Chung, Willem Toorop, and Roland van Rijswijk-Deij, "Roll, Roll, Roll your Root: A Comprehensive Analysis of the FirstEver DNSSEC Root KSK Rollover" October 2019, https://dl.acm.org/doi/10.1145/3355369.3355570.

[113] SSR2 Plenary #97 Transcript - AM Session, 17 January 2020, 35, https://community.icann.org/x/HJkzBw.

[114] Staff Report of Public Comment Proceeding: Proposal for Future Root Zone KSK Rollovers, 7 August 2020, https://www.icann.org/en/system/files/files/report-comments-proposal-future-rz-ksk-rollovers-07aug20-en.pdf. Note: comments were submitted by the Japan Registry Services, ICANN Business Constituency, ICANN Non-Commercial Stakeholder Group, ICANN Root Server System Advisory Committee, ICANN Security and Stability Advisory Committee, and several individuals.

[115] "Proposal for Future Root Zone KSK Rollovers," 1 November 2019, https://www.icann.org/public-comments/proposal-future-rz-ksk-rollovers-2019-11-01-en.

[116] Osterweil, Eric. "A Cybersecurity Terminarch: Use It Before We Lose It." *IEEE Security & Privacy* 18, no. 4 (2020): 67-70.

[117] Osterweil, Leon J., Matt Bishop, Heather Conboy, Huong Phan, Borislava I. Simidchieva, George Avrunin, Lori A. Clarke, and Sean Peisert, "Iterative Analysis to Improve Key Properties of Critical Human-Intensive Processes: An Election Security Example," ACM Transactions on Privacy and Security (TOPS), Vol. 20, No. 2, May 2017, pp. 5:1-31. (UM-CS-2016-012), and Clarke, Lori A., Yao Chen, George S. Avrunin, Bin Chen, Rachel Cobleigh, Kim Frederick, Elizabeth A. Henneman, and Leon J. Osterweil. "Process programming to support medical safety: A case study on blood transfusion." Software Process Workshop, pp. 347-359. Springer, Berlin, Heidelberg, 2005.

expected to result from choices, exceptions, and successful executions.[118] Compared to elections and medical processes, the DNS root zone KSK rollover presents itself as a tractable venue whose security and correctness are globally critical.

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.
>
> 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.

This recommendation can be considered implemented when ICANN org develops formal process and verification that offers verification of the key rollover process after each key rollover, and when ICANN org begins to run regular tabletop exercises to test and familiarize participants with the key rollover process.

This recommendation can be considered effective when the SSR of the process by which DNSSEC protections are maintained during root zone KSK key rollovers are formally verifiable.

This recommendation must be completed in conjunction with each key rollover.

B. Root Zone Change Management

The SSR2 Review Team observed that PTI has done well in implementing mechanisms that reduce the possibility of manipulating the TLD data and the root zone.[119] The root zone management follows a workflow system for managing TLD labels in the root zone called the Root Zone Management System (RZMS). This workflow follows a conservative approach to change management, as each change requires a review by multiple parties.[120]

Even though there are no known security and stability issues that involve the misuse of the RZMS, the potential exists for trivial cyberattacks during the authentication process for all parties involved in the RZMS workflow. Communication with TLD operators is now done by sending clear text emails and access to the system using a simple user/password combination.

---

[118] Iterative Analysis to Improve Key Properties of Critical Human-Intensive Processes: An Election Security Example, Leon J. Osterweil, Matt Bishop, Heather Conboy, Huong Phan, Borislava I. Simidchieva, George Avrunin, Lori A. Clarke, Sean Peisert, ACM Transactions on Privacy and Security (TOPS), Vol. 20, No. 2, May 2017, pp. 5:1-31. (UM-CS-2016-012).

[119] Jennifer Bryce to the SSR2 Review Team mailing list, 27 March 2019, Subject: DNS SSR answers, https://mm.icann.org/pipermail/ssr2-review/2019-March/001569.html.

[120] Internet Names and Numbers (IANA), "Root Zone Change Request Process," accessed 8 December 2020, https://www.iana.org/help/root-zone-process.

Authentication of change requests should be more stringent and involve multi-factor authentication (MFA) and secure communication (e.g., encryption) when using email.

The IANA functions team is currently building its next-generation RZMS, which involves a substantial rewrite of the authorization model.[121] The next generation RZMS should involve a robust and secure authentication and authorization model for submission and approval of the requests as well as additional functionality that would enhance the security and stability of the global DNS system, including:

- Ensuring the integrity and authenticity of change requests for the TLD data.
- Imposing secure communications on all levels that involve request management.
- Being resilient to possible deceiving activities that involve authoritative DNS servers for root and TLD zones.
- Being quick to respond to deletion requests (removal of NS or DS records).
- Consideration of (involving SSAC and RSSAC assessment and public approval process) additional automated technical checks and procedures for the quick remediation of the issues that may affect seamless TLD DNS operations.
- Consideration by SSAC and RSSAC of the implementation of RFC 8078 and related updates for automated DNSSEC Delegation Trust Maintenance (CDS/CDNSKEY).122

Although ICANN org has previously announced the development and implementation of the new RZMS system with more stringent security requirements around communication, the SSR2 Review Team did not find any indication as to when ICANN org plans to put the new system into service.

SSR2 Recommendation 21: Improve the Security of Communications with TLD Operators

> 21.1. ICANN org and PTI operations should accelerate the implementation of new 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.

This recommendation can be considered implemented when ICANN org and PTI have a next-generation RZMS that involves a robust and secure authentication and authorization model for submission and approval of the requests as well as additional functionality that would enhance the security and stability of the global DNS system.

This recommendation can be considered effective when ICANN org mitigates the potential for security and stability issues that involve the misuse of the RZMS through improved identity management procedures.

C. Root Zone Data and IANA Registries

The IANA registries include critical parameters that are specified by RFCs in the Internet Engineering Task Force (IETF), the Internet Research Task Force (IRTF), and the Independent

[121] PTI, "ccNSO Members Meeting - IANA Names Function Update," ICANN 60, 31 October 2017 slides 11-14, https://ccnso.icann.org/sites/default/files/field-attached/presentation-pti-members-31oct17-en.pdf.
[122] Gudmundsson, O. and P. Wouters, "Managing DS Records from the Parent via CDS/CDNSKEY", RFC 8078, DOI 10.17487/RFC8078, March 2017, <https://www.rfc-editor.org/info/rfc8078>.

Submission Stream.[123] The availability and integrity of these parameter registries are paramount and need to be clearly illustrated to the community through formal key performance indicators (KPI). Currently, metrics on the availability of services provided by ICANN org are not available to the community. Stakeholders need that information to assess the SSR aspects of these services over time.

ICANN org may also find the creation of KPIs for the DNS root zone (including DNSSEC, availability, integrity, abuse, etc.) to be the most efficient way to measure, track, and communicate to the community the data trends involving the root zone.

Useful KPIs may include, but are not limited to:

- The propagation delay of root zone changes to instances.
- DNS root zone (including DNSSEC, availability, integrity, etc.), so that third-parties can track SSR aspects.
- Measures that demonstrate the size, growth, and composition of the IANA registries and the global network availability of these registries.

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).

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.

This recommendation can be considered implemented when ICANN org makes the operational status metrics on the services ICANN org supports available to the community.

This recommendation can be considered effective when the community sees an increase in the transparency of ICANN org SSR-related operations.

D. DNS Cryptography

The SSR2 Review Team investigated two topics in the area of DNS cryptography. First, the team investigated the transition from the RSA algorithm to an elliptic curve algorithm for DNSSEC signatures. Second, the team investigated the need to transition to a post-quantum digital signature algorithm.[124] To keep current with advances in traditional computing technology, the size of RSA keys needs to increase over time. Alternatively, DNSSEC could shift from RSA to Elliptic Curve Cryptography (ECC), which offers the same security with

[123] IANA, "Protocol Registration Procedures," 3 January 2020, https://www.iana.org/help/protocol-registration.

[124] See "Appendix G: Cryptography" for details of the team's research.

smaller public keys and smaller signatures. In addition, there is a concern that the invention of a large-scale quantum computer could break both RSA and ECC. Before a large-scale quantum computer comes to pass, DNSSEC needs to shift to a quantum-safe algorithm. ICANN org and PTI have no provisions in the DPS to allow for such a shift.

ICANN org is not the only organization that needs to consider the expected advances in cryptography. Industry standards groups are also preparing for a post-quantum future. The most well-known activity is the NIST post-quantum cryptography project, which works with researchers around the world to develop new cryptographic primitives that are not susceptible to attack by quantum computers.[125] One can expect that project to take several more years before the resulting algorithms are ready for standardization, but it is certainly well underway.

In the meantime, researchers agree that hash-based signatures are post-quantum safe. The Internet Research Task Force (IRTF) has specified these signature algorithms in their Crypto Forum Research Group (CFRG), using small private and public keys with a low computational cost.[126] However, the signatures are quite large, and a private key can only produce a finite number of signatures. These two properties make hash-based signatures undesirable in the DNSSEC environment.

ICANN org's documentation does not take into account the need to transition from the current algorithm to another. This leaves ICANN org unprepared for the expected advances in cryptographic key signing algorithms.

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.

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 lessons learned from the first root KSK rollover in 2018.

This recommendation can be considered implemented when PTI updates the DPS to allow the transition from one digital signature algorithm to another and develops a consensus plan for future root DNSKEY algorithm rollovers.

This recommendation can be considered effective when ICANN org is prepared for more advanced algorithms to be used for key signing, including any increases of key length and timing for key rollover.

[125] National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Resource, Center, "Post-Quantum Cryptography," Created January 03, 2017, Updated November 23, 2020, https://csrc.nist.gov/projects/post-quantum-cryptography.
[126] IRTF, Crypto Forum Research Group, https://irtf.org/cfrg.

5. Emergency Back-end Registry Operator (EBERO)

An EBERO provider serves as a specific DR infrastructure component and represents an important role in offering necessary systems and operational capacity to take over all critical functions of a failing gTLD registry.

An EBERO provider is temporarily activated if a gTLD operator is at risk of failing to sustain critical registry functions.[127] This process ensures the availability of the gTLD operator's functions, protects registrants, and provides an additional layer of protection to the DNS. As indicated by various well-known standards such as ISO 22301, best practice guidance requires that DR processes be tested regularly (see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures).

The SSR2 Review Team was unable to verify that ICANN org coordinated the necessary end-to-end testing of the entire EBERO process described in the "Common Transition Process Manual - Version 3".[128] ICANN org and the EBERO providers tested the parts of the process (a test was conducted with .doosan, and another test was conducted with .mtpc), with the most recent test conducted in 2017.[129] The SSR2 Review Team found the results of those tests in meeting proceedings rather than on any dedicated ICANN web page.[130] The review team recognizes that the details of how an end-to-end EBERO process is tested are out of scope for an SSR review; however, being able to verify that the tests occurred and review the results of those tests is critical for community transparency.

It is also worth noting that while the EBERO processes are documented in the Common Transition Process Manual, that document was extremely difficult to find as it is embedded in the EBERO Agreement.

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.

[127] ICANN, "Emergency Back-end Registry Operator," n.d., https://www.icann.org/resources/pages/ebero-2013-04-02-en.

[128] ICANN, "Emergency Back-End Registry Operator Agreement," August 2019, https://www.icann.org/en/system/files/files/cira-ebero-15aug19-en.pdf. Note: see Exhibit B - Common Transition Processes.

[129] ICANN, EBERO Exercise report, presentation at Tech Day ICANN 55, 7 March 2016, https://meetings.icann.org/en/marrakech55/schedule/mon-tech/presentation-ebero-07mar16-en.pdf, and Murphy, Kevin, "Second emergency registry tested with dead dot-brand," Domain Incite, 27 April 2017, http://domainincite.com/21724-second-emergency-registry-tested-with-dead-dot-brand.

[130] Arias, Francisco, "EBERO Exercises," presentation at Tech Day ICANN60, 30 October 2017, https://ccnso.icann.org/sites/default/files/field-attached/presentation-ebero-exercises-30oct17-en.pdf.

24.2. ICANN org should make the Common Transition Process Manual easier to find by providing links on the EBERO website.

This recommendation can be considered implemented when ICANN org coordinates annual end-to-end testing of the full EBERO process with public documentation for the outcome.

This recommendation can be considered effective when ICANN org is able to validate that the EBERO process functions as intended, protecting registrants and providing an additional layer of protection to the DNS.

Appendix A: Further Suggestions

Throughout the review process, the SSR2 Review Team noted several areas where changes would improve the efficiency and capabilities of future review teams. While these items are outside the mandate of the review team, we hope ICANN org considers the following suggestions as input into future review efforts. They are listed in priority order.

Suggestion 1

ICANN org should implement an online progress tracking function for each recommendation from each review team. By providing online visibility into progress throughout the implementation, the whole community can observe implementation details and provide feedback on any shortcomings. To accomplish the desired transparency and visibility, greater granularity regarding the implementation plans and progress are needed than can be seen on the CCT implementation web pages today.[131] The SSR2 Review Team believes that Recommendation 1 would have been unnecessary if such a function had been in place for the implementation of the recommendations from the SSR1 Review Team. In addition, building on the concept of a CCT implementation shepherd, ICANN org should provide quarterly reports to the members of the review team that produced the recommendations, allowing the review team members themselves to provide regular feedback on whether the implementation is producing the intended effect, and avoiding questions from the next generation of the review team when they assess the implementation. The SSR2 Review Team believes that the assessment of the SSR1 Review Team recommendations would have been straightforward had such a function been in place before the SSR2 Review Team was seated.

Suggestion 2

To avoid misunderstanding and broken expectations, ICANN org should develop a clear written process for obtaining contracted resources for review teams, including milestones and points for review team approval. Every review team will need a technical writer, so ICANN org should supply the review team with a technical writer starting at the review team's very first meeting.

Suggestion 3

To facilitate the investigation, shortly after the Public Comment period ends, and to "*address the increasing needs of inclusivity, accountability, and transparency,*" as stated by strategic goal 2.1, the SSR2 Review Team suggests that ICANN org should create an email mailing list for announcements about Public Comment periods. At the moment, finding information about Public Comment can be quite challenging. Implementing this suggestion will serve to increase awareness among mailing list subscribers of Public Comment periods, without a requirement for additional effort. The existence of these messages will allow members of future review teams and other relevant parties to find information through readily available mail archive search tools easily.

The SSR2 Review Team suggests that ICANN org should send at least three messages per Public Comment period to this email mailing list. The first message should be sent at the opening of the Public Comment period, and it should include a stable URL to the relevant draft

[131] ICANN, "Competition, Consumer Trust, and Consumer Choice Review Team (CCT-RT) Accepted Recommendations – Plan for Implementation and Next Steps," accessed 19 December 2020, https://www.icann.org/public-comments/cct-rt-implementation-plan-2019-09-11-en.

document. The second message should be sent at the close of the Public Comment period, and it should include a stable URL to the collection of submitted comments. The third message should indicate whether consensus was reached, and if so, it should include a stable URL to the final document. Other messages might also be useful, such as an extension to the Public Comment period. In addition, the SSR2 Review Team suggests that ICANN org create a web page dedicated to listing all public calls for comments, which would then be linked to the page of the relevant documents.

Suggestion 4

To enable transparent discussions about security, ICANN org should consider establishing an open information assurance platform to share security and abuse information to make the information more fluid and quicker to disclose.

Appendix B: Definitions and Acronyms

Definitions

An assessment of this type requires a common understanding of the key terms associated with the review. Initially, the SSR2 Review Team (SSR2 Review Team) operated under the following definitions:[132]

- Abuse: See "DNS abuse" below
- Business Email Compromise (BEC): A type of scam targeting companies where electronic mail accounts of employees are either spoofed or compromised to do fraudulent wire transfers.
- Botnet: A network of computers infected with malware and controlled as a group without the knowledge of the owners of the computers.
- Digital Certificate Fraud: An attacker breaches a Certification Authority (CA) to generate and obtain fraudulent certificates to launch further attacks; an attacker can also use fraudulent certificates to authenticate as another individual or system, or to forge digital signatures.
- Distributed Denial-of-Service (DDoS) Attack: A malicious attempt to disrupt a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic from multiple (Distributed) sources.
- DNS abuse: Intentional misuse of the universal identifiers provided by the DNS for cybercrime infrastructure and directed users to websites that enable other forms of crime, such as child exploitation, intellectual property infringement, and fraud.
- Domain Name System (DNS): The DNS is a distributed online database service that translates easy-to-remember domain names to numerical Internet Protocol (IP) addresses; for example, the DNS will translate www.icann.org to 192.0.34.65 (specified in RFCs 1034 and 1035).
- Identifier Systems Security, Stability, and Resiliency (IS-SSR) Framework: A document, updated periodically, that "describes ICANN's role and boundaries in supporting a single, global interoperable Internet and the challenges for the Internet's unique Identifier Systems."
- Malware: Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.
- Phishing: The fraudulent attempt to obtain sensitive information by disguising oneself as a trustworthy entity in an electronic communication.
- Ransomware: Malware that is designed to block access to a computer system until a sum of money is paid.
- Resiliency: The capacity of the Identifier System to effectively withstand, tolerate, and survive malicious attacks and other disruptive events without disruption or cessation of service.
- Scamming: A fraudulent hoax made to look like a real business activity or investment opportunity designed to make money.
- Security: The capacity to protect and prevent misuse of Internet unique identifiers.
- Security threat: Phishing, scamming, malware, ransomware, spam, DDoS attacks, digital certificate fraud, and botnets are among the most critical security threats.
- Spam: Unsolicited bulk electronic mail.
- Stability: The capacity to ensure that the Identifier System operates as expected and that users of unique identifiers have confidence that the system operates as expected.

[132] ICANN, "SSR Role & Remit," accessed on 27 December 2019, https://www.icann.org/resources/pages/ssr-role-remit-2015-01-19-en.

- Unique Identifiers: ICANN's technical mission includes helping to coordinate, at the overall level, the allocation of the Internet's system of unique identifiers: specifically, top-level domain names, blocks of Internet Protocol (IP) addresses and autonomous system (AS) numbers allocated to the Regional Internet Registries, and protocol parameters as directed by the IETF.

Acronyms

- AS: Autonomous System
- BC: Business Continuity
- CISO: Chief Information Security Officer
- CSO: Chief Security Officer
- CZDS: Centralized Zone Data Service
- DAAR: Domain Abuse Activity Reporting
- DNS: Domain Name System
- DNSSEC: the DNS Security Extensions (as specified in RFCs 4033, 4034, and RFC 4035)
- DoH: DNS over HTTPS
- DoT: DNS over TLS
- DPS: DNSSEC Practice Statement
- DR: Disaster Recovery
- DURZ: Deliberately Unvalidatable Root Zone
- EBERO: Emergency Back-end Registry Operator
- EPDP: Expedited Policy Development Process
- FSM: Finite-State Machine
- gTLD: generic top-level domain
- GNSO: Generic Names Supporting Organization
- HTTP: HyperText Transfer Protocol
- HTTPS: HyperText Transfer Protocol Secure
- IANA: Internet Assigned Numbers Authority
- IETF: Internet Engineering Task Force
- IMRS: ICANN Managed Root Server
- IP: Internet Protocol
- IRTF: Internet Research Task Force
- IS-SSR Framework: Internet Identifier Systems Security, Stability, and Resiliency Framework
- ISMS: Information Security Management System
- ISO: International Organization for Standardization
- ITIL: IT Infrastructure Library
- KSK: key signing key
- NCAP: Name Collision Analysis Project
- NIST: National Institute of Standards and Technology
- OCTO: Office of the Chief Technology Officer
- PII: Personally Identifiable Information
- PTI: Public Technical Identifiers
- RDS: Registration Directory Service
- RAA: Registrar Accreditation Agreement
- RAPWG: Registration Abuse Policies Working Group
- RDAP: Registration Data Access Protocol
- RSSAC: Root Server System Advisory Committee
- SADAG: Statistical Analysis of DNS Abuse in gTLDs
- SMART: specific, measurable, assignable, relevant, and trackable

- SOP: Strategic and Operating Plans
- SSAC: Security and Stability Advisory Committee
- SSAE: Statement on Standards for Attestation Engagements
- SSR: Security, Stability, and Resiliency
- SSR1: first SSR review process
- SSR2: second SSR review process
- TLS: Transport Layer Security

Appendix C: Process and Methodology

Process and Methodology for the Review of SSR1 Recommendations

The assessment process of the SSR2 Review Team outlined below is based on briefings from, and discussions with, ICANN org staff responsible for implementation; the systematic review of a substantial amount of relevant ICANN documents and implementation reports created by ICANN org; and additional research and interviews.[133] The team also used outreach sessions at ICANN Public Meetings in Barcelona and Kobe to liaise with relevant community stakeholders. The assessment was both quantitative and qualitative, wherever possible, depending on the specific recommendation.

Many SSR1 recommendations were high level and lacked specificity. The SSR2 Review Team had no authority to access and analyze the internal workings of ICANN and thus asked ICANN org to provide their implementation plans and evidence of successful implementation to the SSR2 Review Team members. The recommendations themselves, and the documentation provided by ICANN org lacked defined KPIs and targets, measurable objectives, and implementation plans. This made the measurement or tracking of the implementations challenging. Furthermore, the wording of some of the recommendations left room for interpretation. This occasionally led to a different understanding of the recommendation by the SSR2 team from the one used by ICANN org staff.

For each recommendation, ICANN org staff provided initial answers on implementation to the team in 2017, reporting on how they implemented the SSR1 recommendations. ICANN staff cited web pages or documents, arranged presentations from various departments within ICANN org, and also provided the team with briefings on the recommendations over nine months. The team also reviewed a substantial number of background documents relevant to this review. The team conducted interviews with ICANN org staff, requested additional information, and used the input of relevant stakeholders and its own research to conduct further analysis where appropriate.

After receiving replies from ICANN org to the questions submitted and completing its research and due diligence to the best of its ability, the team drafted strawman assessments for each recommendation in mid to late 2018, which were discussed online, on the team's weekly calls, and in face-to-face meetings. The team edited text as needed and approved the conclusions and findings for each SSR1 recommendation with the intention for its inclusion in the draft SSR2 team report, with the team's approved consensus protocols, and noting minority objections where applicable.

After discussing online and on calls, and going through multiple iterations, the team decided to structure their assessment draft according to the following methodology, which focused on task completion, relevance, and further work required:

1. What was done to implement the recommendation?
2. Was the recommendation fully implemented?

[133] ICANN SSR2 Review Team wiki, https://community.icann.org/display/SSR/SSR2+Review. See in particular Background Materials and Briefing Materials.

3. Did the implementation have the intended effect?
4. How was the assessment conducted?
5. Is the recommendation still relevant today?
6. If so, what further work is needed? If not, why not?

The first question speaks to what ICANN org did to implement the recommendation. Question two gives the team's assessment of the level of implementation as of the "fully implemented date" provided by staff. The team encountered many recommendations that seem to have been only partially implemented or where implementation plans were missing. In these cases, the team identified specific areas for improvement. In some cases, it was difficult to establish clear preconditions and targets necessary for successful implementation due to missing implementation plans, documentation, and missing performance indicators. The third question addresses if and to what extent the implementation had the intended effect. The fourth question speaks to how the SSR2 team conducted the assessment. Readers can trace documents and other evidence used by the team on a per-recommendation basis. Based on question five, the team also evaluated whether each recommendation was still relevant in 2018. Finally, the team then decided whether current circumstances warrant additional work to implement a form of this recommendation, which would then inform the SSR2 team's own set of recommendations.

Process and Methodology for ICANN SSR, DNS SSR, and Future Challenges

The SSR2 Review Team conducted a series of interviews with ICANN org staff.[134] Questions focused on the completeness and effectiveness of ICANN org's security processes and the effectiveness of the ICANN org security framework.

The SSR2 Review Team organized around a specific process to affirm the findings and develop recommendations for consideration of ICANN, including:

- Reviewing, analyzing, and summarizing relevant documentation.
- Conducting investigations within the identified areas of concern.
- Conducting relevant interviews as appropriate.
- Drafting summary of the rationales, findings, and recommendations.

Workstream 2 focused on SSR concerns within ICANN org itself, whereas Workstream 3 focused on the SSR of the global identifier systems: the global DNS, the IANA numbers databases (IP allocations and ASNs), and the IANA protocol registries. The review team specifically considered reports and other input on the risks, threats, and abuse of the DNS, and then mapped the resulting data to the relevant ICANN component(s), procedures, and policies. Within Workstream 4 regarding future challenges for SSR, the SSR2 Review Team considered current research on DNS abuse, the impact of the continued evolution of the types and volume of devices in the DNS, emerging technology, areas of concern identified in other workstreams that may have future implications, and ICANN institutionalized methodologies for threat analysis and mitigation.
The SSR2 Review Team recognized that this workstream was dependent on the emerging themes from the other dependent areas. More specifically, in addition to commonly identified

[134] ICANN SSR2 Review Team wiki, https://community.icann.org/display/SSR/SSR2+Review. See in particular Briefing Materials.

challenges, the stability and resilience of the DNS may face other specific challenges under the workstream as related to ICANN SSR and DNS SSR.

Appendix D: Findings Related to SSR1 Recommendations

This section includes a detailed assessment of each of the SSR1 recommendations. The findings here discuss the specific implementations, their issues, and the team's ideas for further work. The SSR2 Review Team noted the following reappearing issues:

1. There is a lack of indicators, measurement, and goalposts that would allow the community and ICANN org to track and understand the security space and their own activities.

2. There is a lack of publicly available evidence, definitions, and procedures, inhibiting observation of SSR activities, which leads to a lack of clarity regarding what is being done, when it is done, by whom, and how.

3. There is a lack of community review and accountability, denying the ICANN community opportunities to provide input on SSR matters.

4. ICANN org does not currently have an overarching strategy, identifiable goals, or a clear and comprehensive SSR policy. Without a functional SSR strategy and integrated security and risk management (e.g., policy, procedures, standards, baselines, guidelines), SSR-related responsibilities are not assigned, measured, and tracked, leading to a lack of transparency and accountability.

SSR1 Recommendation 1

"ICANN should publish a single, clear and consistent statement of its SSR remit and limited technical mission. ICANN should elicit and gain public feedback in order to reach a consensus-based statement."

SSR2 Conclusion: This recommendation remains relevant as it was partially implemented but did not fully achieve the intended effect of having a consensus-based, clear, and consistent statement describing ICANN org's SSR remit and technical mission.

Rationale:

- The team observed that a statement exists, and that ICANN org updated (but no longer maintains) that statement as a result of a review by the community.[135] Despite the existence of this statement and its clear definitions of "Security, Stability, and Resiliency" the use of these definitions remains inconsistent. Side conversations with team members who have access to the text of ICANN org's contracts with various contracted parties have indicated that the definitions of "security" and "stability" used within ICANN org's agreements with contracted parties are different.[136]

[135] SSR Role & Remit, https://www.icann.org/resources/pages/ssr-role-remit-2015-01-19-en, and "Security, Stability & Resiliency of the DNS Review Team – Draft Report: Report of Public Comments," last modified 18 May 2012, http://www.icann.org/en/system/files/files/report-comments-ssr-rt-draft-report-18may12-en.pdf.

[136] See also the Base New gTLD section 7.3 https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html vs. ICANN org's definitions of S&S https://www.icann.org/groups/ssac

- No metrics were provided to evaluate whether the implementation had the intended effect of providing clear and consistent information on its SSR remit and the limits of its technical mission. Given the different ways that the term "SSR" is used throughout ICANN, it did not lead to the common definition that was expected by the SSR1 Review Team.

SSR1 Recommendation 2

"ICANN's definition and implementation of its SSR remit and limited technical mission should be reviewed in order to maintain consensus and elicit feedback from the Community. The process should be repeated on a regular basis, perhaps in conjunction with the cycle of future SSR reviews."

SSR2 Conclusion: This recommendation remains relevant and was not fully implemented. The intended effect of having a regular public review process for ICANN org's SSR remit and associated technical mission was not achieved.

Rationale:

- The SSR2 Review Team did not find evidence that regular reviews of the SSR remit have happened. There have been no opportunities to comment specifically on the remit and mission statement since 2013.

SSR1 Recommendation 3

"Once ICANN issues a consensus-based statement of its SSR remit and limited technical mission, ICANN should utilize consistent terminology and descriptions of this statement in all materials."

SSR2 Conclusion: This recommendation is still relevant but was not fully implemented. The intended effect of working from a consistent terminology and set of descriptions for SSR-related materials was not achieved.

Please see SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting for the SSR2 recommendation that expands upon the original SSR1 recommendation.

Rationale:

- A blog post from July 2013 lists ICANN org's security terminology available to the whole community; however, these definitions do not appear to be consistently integrated into other SSR-related documents.[137]
- ICANN org's staff report on this recommendation indicates that staff would add key terms to ICANN org's public glossary on an ongoing basis as part of the Strategic and Operating Plan (SOP); as SSR activities evolve, terminology and descriptions will be updated as part of SOP. However, the glossary (found in the blog post noted above) has not been updated since February of 2014.

[137] ICANN, "ICANN's Security Terminology," blog, last modified 8 July 2013, https://www.icann.org/news/blog/icann-s-security-terminology.

SSR1 Recommendation 4

"ICANN should document and clearly define the nature of the SSR relationships it has within the ICANN Community in order to provide a single focal point for understanding the interdependencies between organizations."

SSR2 Conclusion: This recommendation remains relevant but was not fully implemented. The intended effect of providing an open and transparent resource that describes ICANN org's SSR relationships was not achieved.

Please see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management for the SSR2 recommendation that expands upon the original SSR1 recommendation.

Rationale:

- ICANN org staff created a document for the SSR2 Review Team that tracks ICANN SSR-related roles and responsibilities, and lists every organization with which ICANN org has ever had a formal relationship.138 The document includes specific references to documents that underpin each of those relationships, and a description of the SSR components of that relationship. Many of the references listed in that document, however, cannot be located online. The document often shows the SSR components of the relationships as "unknown."

SSR1 Recommendation 5

"ICANN should use the definition of its SSR relationships to maintain effective working arrangements and to demonstrate how these relationships are utilized to achieve each SSR goal."

SSR2 Conclusion: This recommendation is still relevant but was not fully implemented. The review team was unable to determine if ICANN org achieved the intended effect of effective working arrangements in support of each SSR goal.

Please see SSR2 Recommendation 3: Improve SSR-Related Budget Transparency for the SSR2 recommendation that expands upon the original SSR1 recommendation.

Rationale:

- The team expected the IS-SSR Framework to include information on how the key relationships called for in SSR1 Recommendation 4 are used to achieve SSR goals; however, this information is not readily available.[139]
- The SSR2 team lacked sufficient information to assess if working relationships are functional.

SSR1 Recommendation 6

"ICANN should publish a document clearly outlining the roles and responsibilities for both the SSAC and RSSAC in order to clearly delineate the activities of the two groups. ICANN should seek consensus for this across both groups, recognizing the history and circumstances of the

[138] "SSR Relationships," ICANN, 23 January 2017, https://www.icann.org/en/system/files/files/ssr-relationships-fy17-23jan17-en.pdf.

[139] Ibid.

formation of each. ICANN should consider appropriate resourcing for both groups, consistent with the demands placed upon them."

SSR2 Conclusion: This recommendation is still relevant but was not implemented. ICANN org did not achieve the intended effect of making the roles of SSAC and RSSAC clear to all interested parties.

Rationale:

- The roles and responsibilities for SSAC and RSSAC are captured in a document.[140] However, this public document is still marked as "DRAFT UNDER REVIEW." It appears that work was started on this recommendation, however, it concluded without addressing organizational reviews of SSAC and RSSAC. If consensus was achieved, the SSR2 Review Team could not locate the final document.
- The document is based on the ICANN Bylaws from before the IANA transition. The parts of the Bylaws that describe SSAC and RSSAC are largely the same, but RSSAC is now explicitly charged with responding "to requests for information or opinions from the Board." The update did not resolve the potential for overlap of roles and responsibilities between the SSAC and RSSAC in the ICANN Bylaws:

  > *"SSAC is to advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems;*
  >
  > *RSSAC is to advise the ICANN community and Board on matters relating to the operation, administration, security, and integrity of the Internet's Root Server System."*

SSR1 Recommendation 7

"ICANN should build on its current SSR Framework by establishing a clear set of objectives and prioritizing its initiatives and activities in accordance with these objectives."

SSR2 Conclusion: The recommendation remains relevant and was partially implemented. The intended effect of having clear, publicly reviewed SSR objectives and associated prioritization effort, was not achieved.

Please see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management, and SSR2 Recommendation 3: Improve SSR-Related Budget Transparency for the SSR2 recommendations that expands upon the original SSR1 recommendation.

Rationale:

- SSR-related activities are reported on regularly as part of Strategic and Operating Plans (SOP), including in ICANN's regular portfolio management reporting and SSR quarterly reports.[141] The SOP were informed by the IS-SSR Framework, which included SSR

[140] ICANN, "DRAFT UNDER REVIEW: The Roles and Responsibilities of ICANN's Security and Stability Advisory Committee and Root Server System Advisory Committee," 5 March 2015, https://www.icann.org/en/system/files/files/draft-rssac-ssac-roles-responsibilities-05mar15-en.pdf.

[141] ICANN, "ICANN Strategic Plan for Fiscal Years 2021 – 2025," n.d., https://www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf , and Dave Piscitello, "Identifier Systems SSR Activities Reporting," ICANN Blog, last modified 21 January 2015, https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-en.

priorities, objectives, and activities. That framework, however, is no longer produced, leaving a gap around how the SOP takes into account SSR-related actions. The process for updating SSR-related documents is not clear since the last publication of the IS-SSR Framework was published in 2016.[142]
- The IS-SSR Framework offered an opportunity for the community to inform SSR strategy. ICANN org no longer produces that framework, resulting in insufficient opportunities to collect community input from the full range of ICANN stakeholder groups on how ICANN org approaches SSR activities.
- Strategic planning for security, stability, and resiliency issues appear to be centered on the Office of the CTO (OCTO), and given the existence of the SOP, the RT recognized that a level of planning around SSR activities exists within OCTO. The level of detail and planning envisioned in the recommendation, however, does not include public discussions equally across all ICANN org stakeholders.

SSR1 Recommendation 8

"ICANN should continue to refine its Strategic Plan objectives, particularly the goal of maintaining and driving DNS availability. Clear alignment of Framework & Strategic Plan."

SSR2 Conclusion: While this recommendation remains relevant today and was partially implemented, the implementation of this recommendation did not achieve the intended effect of providing a clearer link between SSR-related strategy and operational work.

Please see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management, and SSR2 Recommendation 3: Improve SSR-related Budget Transparency for the SSR2 recommendations that expands upon the original SSR1 recommendation.

Rationale:
- Available documents on the SSR1 Review Implementation homepage indicate that SSR guidance is included and addressed in relevant reports, strategies, and procedures.[143] However, the available reports do not provide sufficient insight into SSR activities and lack detail regarding the implementation and the execution of SSR activities.
- The SOP does not indicate which activities, priorities, and expenditures in the SOP are SSR-related. Crucially, the mechanisms envisioned by SSR1 have been replaced by other organizational and process tools, complicating both assessment and implementation.

SSR1 Recommendation 9

"ICANN should assess certification options with commonly accepted international standards (e.g., ITIL, ISO and SAS-70) for its operational responsibilities. ICANN should publish a clear roadmap towards certification."

SSR2 Conclusion: This recommendation remains relevant. The SSR2 Review Team was unable to determine if this recommendation was fully implemented and achieved the intended

[142] ICANN, IS-SSR Framework – FY15-16, https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf.
[143] SSR1 Review Implementation Home, wiki, last updated 22 August 2017, https://community.icann.org/display/SSR/SSR1+Review+Implementation+Home.

effect, as the original recommendation lacked the necessary specificity regarding which certification or certifications ICANN org should target or what ends were being pursued.

Please see SSR2 Recommendation 4: Improve Risk Management Processes and Procedures, and SSR2 Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications for the SSR2 recommendations that expand upon the original SSR1 recommendation.

Rationale:

- According to interviews with ICANN org staff, ICANN org has pursued some certifications focused on IANA, e.g., SOC2/3 Certification of Root Zone KSK System, SOC2 Certification for the Registry Assignment and Maintenance Systems, and SysTrust for the implementation of DNSSEC at the root level.144 Outside of the IANA functions, ICANN org generates reports using continuous improvement frameworks in IT and cybersecurity, has an annual financial audit, performs an annual EFQM self-assessment and documentation review, and obtains professional advice to help measure performance and drive improvement.145
- ICANN org also reports that all information security staff are trained using SANS offerings.146
- ICANN org reports that the outcomes of internal audits are reported to the ICANN Board only.147
- The SSR2 Review Team was unable to find any document that could be used as a roadmap for SSR process certification, making community review impossible.

SSR1 Recommendation 10

"ICANN should continue its efforts to step up contract compliance enforcement and provide adequate resources for this function. ICANN also should develop and implement a more structured process for monitoring compliance issues and investigations."

SSR2 Conclusion: This recommendation remains relevant and was not fully implemented. The intended effect of having adequate resources applied to contract compliance enforcement and developing an ongoing structured process for monitoring compliance was not achieved.

Please see SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties, and SSR2 Recommendation 9: Monitor and Enforce Compliance for the SSR2 recommendations that expand upon the original SSR1 recommendation.

Rationale:

- The assessment is based on publicly available information (e.g., the Contractual Compliance Reporting page) as well as an ICANN staff report that provided evidence of implementation of the recommendation.[148] Regular public reporting of compliance activities

[144] See Working Document, "SSR2 questions and answers," n.d., 6, https://community.icann.org/pages/viewpage.action?pageId=64076120.
[145] Ibid., 24.
[146] Ibid., 11.
[147] Ibid., 6.
[148] The SSR1 implementation report is available at https://community.icann.org/download/attachments/54691765/SSR%20Recs%201-28.pdf?api=v2 (slides 28-30)

is part of ICANN org's Strategic and Operating Plan (SOP). ICANN org has a dedicated public page for Contractual Compliance reporting, including data on monthly, quarterly, and annual data; ten different reports queryable over a rolling 13-month period; and metrics and data as explicitly requested by different working groups. Some Contractual Compliance auditing and outreach programs are now in place. ICANN org created new positions after the SSR1 Review to ensure the fulfillment of goals and objectives in this area.

- Complaint mechanisms were updated by migrating to the ICANN org website, automating, and launching a bulk complaint tool. Additionally, ICANN staff indicated that a Pulse Survey was conducted.[149] ICANN org launched a quality check for inaccuracies within the RDS data. RDS accuracy reporting has been underway since the 2012 WHOIS Review Team recommended the action.
- Compliance enforcement reports for 2017 and 2016 contain little evidence of SSR enforcement actions, despite the new gTLD base registry agreement (July 2017) that contains specific obligations on contracted parties relating to security and stability, and may assist further implementation.150 It is unclear to the SSR2 Review Team how ICANN org's goal to reduce the incidence and impact of registration abuse and malicious conduct carries through compliance actions or other initiatives. The majority of the issues in the staff SSR1 implementation report highlight matters relating to WHOIS. Additionally, the registrar agreement (RAA 2013) contains vague enforcement rights for ICANN org in relation to registrars whose operation endangers registrar and registry services, the DNS, or the Internet.
- ICANN org produces monthly reports about its compliance enforcement work, but it is not clear the extent to which SSR issues are handled within the compliance process.151

SSR1 Recommendation 11

"ICANN should finalize and implement measures of success for new gTLDs and IDN fast track that expressly relate to its SSR-related program objectives, including measurements for the effectiveness of mechanisms to mitigate domain name abuse."

SSR2 Conclusion: This recommendation remains relevant but is not measurable. While actions have been taken to mitigate domain name abuse, it was not possible to determine if or how much this impacted the mitigation of domain abuse.

The DNS landscape has changed since the first SSR Review Team made its recommendations as a result of the new gTLD expansion, in particular. However, the recommendation to embed SSR considerations as a key measure of success in the management of the DNS space remains just as relevant, if not more so, today as it was in 2011.

Please see SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties, SSR2 Recommendation 12: Overhaul DNS

---

and the SSR2- RT briefing on this recommendation is available at https://community.icann.org/download/attachments/66085372/SSR1%20Compliance%20Briefing%20June%202017%20v3.pdf?version=2&modificationDate=1499814488000&api=v2.

[149] See "SSR Recommendation 10 Implementation" in the consolidated SSR1 Implementation Report, https://community.icann.org/download/attachments/54691765/SSR%20Recs%201-28.pdf?api=v2.

[150] ICANN, 31 July 2017, https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf.

[151] See ICANN's "Contractual Compliance Performance Measurement" reports, https://features.icann.org/compliance/dashboard/report-list.

Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review, and SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting, for the SSR2 recommendations that expand upon the original SSR1 recommendation.

Rationale:

- The SSR2 Review Team was unable to find any document describing the measures for success, including measurements for the effectiveness of mechanisms to mitigate domain name abuse, that has community consensus. This lack of measurable criteria has also been noted in the recent CCT's report and recommendations.[152]
- Specification 11 of the new Registry Agreement contains substantial SSR obligations on registries, including obligations to periodically conduct technical analysis and maintain statistical reports to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. These exact obligations have been part of the standard new gTLD registry agreement since applications opened in 2012. ICANN org has a compliance graph, but it measures the number of complaints and categories.[153] This remains difficult to track given its reporting is spread across several pages.

SSR1 Recommendation 12

"ICANN should work with the Community to identify SSR-related best practices and support the implementation of such practices through contracts, agreements and MOUs and other mechanisms."

SSR2 Conclusion: SSR1 Recommendation 12 was not fully implemented and remains particularly relevant today. The effect of having defined and implemented SSR-related best practices was not achieved.

Please see SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties, and SSR2 Recommendation 9: Monitor and Enforce Compliance, for the SSR2 recommendations that expand upon the original SSR1 recommendation.

Rationale:

- Specification 11 of the new Registry Agreement (RA) contains substantial SSR obligations on registries. The obligations in this RA have been part of the standard new gTLD registry agreement since applications opened in 2012. However, ICANN org has apparently not used these provisions as a baseline for assessing how effective they are in meeting the goals of SSR1 Recommendation 12.
- The report entitled "Identifier System Attack Mitigation Methodology" is dated February 2017. The paper sets out suggestions said to have been generated "*within ICANN and by Identifier System security experts throughout the Community.*"[154] However, it is not clear

[152] CCT Report, 9, https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf.

[153] See ICANN Contractual Compliance Performance Reports, https://features.icann.org/compliance and "Contractual Compliance Performance Measurement" reports, https://features.icann.org/compliance/dashboard/report-list.

[154] Phifer, Lisa, and David Piscitello, "Identifier System Attack Mitigation Methodology," ICANN white paper, 13 February 2017, https://www.icann.org/en/system/files/files/identifier-system-attack-mitigation-methodology-13feb17-en.pdf.

what process was followed in arriving at the best practices set out in the document. There is no evidence in the linked-to paper of any integration of those best practices into agreements into which ICANN org enters. There is no evidence of work prior to 2017 contained in the report.
- The Identifier System Attack Mitigation Methodology report outlined a non-exhaustive list of attacks against the Identifier System. Although there have been some agreements, renewals, specifications, and MOUs since February 2017, nothing specifically from that paper has ever been included in the contracts with contracted parties.
- The ICANN Security Awareness Resource Locator page has not been updated since 2014.[155]
- The SSR2 review found no evidence of staff periodically informing SO/ACs of best practices or inviting them to identify additional best practices.
- The staff report on this SSR1 recommendation indicates that work with the Anti-Phishing Working Group (APWG) Internet Policy Committee on publishing recommendations for web application protection and development of resources for security awareness is complete. There was an advisory from APWG on "What to Do if Your Website Has Been Hacked by Phishers," but it was produced prior to SSR1. While there is a report from the 4th Global DNS Stability, Security and Resiliency Symposium held in Puerto Rico in 2012, the ICANN website does not appear to have a set of recommendations for web application protection and development of resources for security awareness.[156]

SSR1 Recommendation 13

"ICANN should encourage all Supporting Organizations to develop and publish SSR-related best practices for their members."

SSR2 Conclusion: This recommendation remains relevant but was not implemented. The intended effect of having a regular process for Supporting Organizations (SOs) to publish SSR-related best practices for their members was not achieved.

Please see SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties, and SSR2 Recommendation 9: Monitor and Enforce Compliance, for the SSR2 recommendations that expand upon the original SSR1 recommendation.

Rationale:
- ICANN org considers work on this recommendation ongoing and reports that as part of SOP, ICANN staff contacts all SOs and ACs to encourage identification and publication of a best practices repository page. ICANN org reports further that their staff engages in a variety of ongoing activities to encourage global use of SSR best practices, as part of SOP. The SSR2 Review Team was unable to find evidence that ICANN org conducted this outreach, nor evidence that SOs published SSR-related best practice guidance for their members.
- ICANN org staff reported that they were not aware of any recent steps that have been taken to encourage SOs and ACs to produce and publish best practice repositories for SSR-related information, stating that "*it is likely that the 2012 information on the ccTLD website may be the most recent example of SSR-related information published by a Supporting*

[155] ICANN Security Awareness Resource Locator, last updated 8 August 2014, https://www.icann.org/resources/pages/security-awareness-resource-2014-12-04-en.
[156] "DNS Stability, Security and Resilience," Meeting Report of the 4th Global Symposium, ICANN and APWG, 25 October 2012, https://www.icann.org/en/system/files/files/dns-symposium-25oct12-en.pdf.

Organization."[157] Moreover, staff reported that only ccNSO currently publishes the SSR-related best practices for their members.

SSR1 Recommendation 14

"ICANN should ensure that its SSR-related outreach activities continuously evolve to remain relevant, timely and appropriate."

SSR2 Conclusion: This recommendation remains relevant but has not been implemented, and therefore did not achieve its intended effect of improving the timeliness, relevancy, and appropriateness of ICANN's SSR-related outreach activities.

Please see SSR2 Recommendation 18: Informing Policy Debates for the SSR2 recommendation that expands upon the original SSR1 recommendation.

Rationale:

- The Engagement Interface did not directly address how the outreach activities "evolve" to remain relevant.[158] The implementation focused, instead, on reporting what is being done at any given time. As the focus on evolving activities is not being addressed, the recommendation has not been implemented.

SSR1 Recommendation 15

"ICANN should act as a facilitator in the responsible disclosure and dissemination of DNS security threats and mitigation techniques."

SSR2 Conclusion: This recommendation remains relevant and was not fully implemented. While a process exists "on paper," it is not possible to assess if that process is functional and effective.

Please see SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties, SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review, and SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting, for the SSR2 recommendations that expand upon the original SSR1 recommendation.

Rationale:

- While ICANN org has implemented a vulnerability disclosure process, there are no public statistics or other information on how often such a process has been invoked.
- ICANN org has implemented a Vulnerability Disclosure Program for ICANN's public-facing assets.159 When vulnerabilities against DNS infrastructure are reported to ICANN org, ICANN org (when feasible) disseminates to responsible external third parties. However, it is the responsibility of the third-party to remediate any vulnerability within their platform(s).

[157] SSR2 wiki, Review Team Review Team Documents & Drafts, "SSR1 Recommendations table" n.d., 26, https://community.icann.org/pages/viewpage.action?pageId=64076120.
[158] ICANN, Engagement Interface, accessed 13 December 2020, https://features.icann.org/events-near-you.
[159] ICANN, "Process for Reporting Vulnerabilities Within ICANN Organization Online Services," accessed 13 December 2020, https://www.icann.org/vulnerabilities.

- Since 2013, none of the IS-SSR reports contain any statistics or metrics related to disclosure reporting. It is impossible to tell from published materials if the vulnerability disclosure reporting methodology has ever been invoked, or if it is functional. No data, even in anonymized form, is available about ICANN org as a vulnerability coordinator, nor its work in emergency coordination and SSR-related crisis management.

SSR1 Recommendation 16

"ICANN should continue its outreach efforts to expand Community participation and input into the SSR Framework development process. ICANN also should establish a process for obtaining more systematic input from other ecosystem participants."

SSR2 Conclusion: This recommendation remains relevant and was only partially implemented. Given the lack of evidence that current outreach activities have resulted in expanded community participation, this recommendation cannot be considered to have achieved its intended effect.

Please see SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties, SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review, SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting, and SSR2 Recommendation 18: Informing Policy Debates, for the SSR2 recommendations that expand upon the original SSR1 recommendation.

Rationale:

- Ongoing involvement in related communities has accomplished the "participation" objective but was unable to determine how information is "systematic[ally]" incorporated. This recommendation envisions greater public engagement with SSR initiatives, including frameworks and annual reports. This recommendation resulted in no obvious changes to the way the IS-SSR Framework and Annual Reports are created.
- There is ongoing outreach to related communities with existing relationships to ICANN org, which accomplishes the "participation" objective. However, the recommendation requests outreach to additional SSR communities.
- There is no evidence that current outreach activities have resulted in expanded community participation.
- The recommendation specifically asks for a more systematic process for getting input from other ecosystem participants. This makes the final deliverable of the SSR1 Implementation Status Report seem out of place.160
- The Implementation Report says that staff would "support a variety of capability building initiatives by the Security Team."161 The SSR2 Review Team was unable to determine if and how these capability-building initiatives would affect greater engagement in the development of the IS-SSR Frameworks because ICANN org no longer updates the IS-SSR Frameworks.
- The SSR2 Review Team was unable to find evidence from the public record what the capability-building initiatives were or when they were conducted.

[160] ICANN, SSR Review Implementation Report, June 2015, https://www.icann.org/en/system/files/files/ssr-review-implementation-30jun15-en.pdf.
[161] Ibid., 7.

SSR1 Recommendation 17

"ICANN should establish a more structured internal process for showing how activities and initiatives relate to specific strategic goals, objectives and priorities in the SSR Framework."

SSR2 Conclusion: This recommendation remains relevant. Due to a lack of trackable indicators, the status of implementation is impossible to ascertain from publicly available materials. The recommendation did not achieve its intended effect as ICANN org no longer maintains the SSR Framework.

Please see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management for the SSR2 recommendation that expands upon the original SSR1 recommendation.

Rationale:

- The implementation report refers to the deliverables in SSR1 Recommendation 2 as a guide to how SSR1 Recommendation 17 was implemented. However, SSR1 Recommendations 2 and 17 have different goals. SSR1 Recommendation 2 asks that the SSR-related activities and remit go through regular public consultation, whereas SSR1 Recommendation 17 suggests that SSR-related initiatives relate to specific strategic goals, objectives, and priorities. The deliverables for SSR1 Recommendation 2 do not meet the requirements of SSR1 Recommendation 17.
- The most recent Annual Report reviewed by SSR2 (FY18) lists eighteen separate initiatives for the fiscal year and then describes how those initiatives connect to the overall mission of the Office of the CTO and ICANN's overall strategic plan. The Annual Plan then links to activity reports that describe the work completed in a reporting period (six months).
- The connection between the SSR Annual Report and ICANN's Strategic Plan is not clear. Furthermore, the Strategic Plan does not mention the SSR Annual Reports and barely mentions SSR-related activities. If a more structured internal process for showing how activities and initiatives relate to specific strategic goals, objectives, and priorities in the IS-SSR Framework is present, it is not available publicly or to the SSR2 Review Team. However, the section of the most recent annual report that identifies annual initiatives does attempt to relate them to ICANN's Strategic Plan.
- Other SSR1 recommendations attempt to align and integrate ICANN's SSR activities with the overall Strategic Plan. The implementation of SSR1 Recommendation 17 falls well short of providing a structured and easily reviewed internal process.

SSR1 Recommendation 18

"ICANN should conduct an annual operational review of its progress in implementing the SSR Framework and include this assessment as a component of the following year's SSR Framework."

SSR2 Conclusion: This recommendation remains relevant. The SSR2 Review Team was unable to find any evidence of either an internal review process or a public review process that would have resulted in regular updates to the IS-SSR Framework, and so cannot determine whether this recommendation achieved its intended results.

Please see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management for the SSR2 recommendation that expands upon the original SSR1 recommendation.

Rationale:

- SSR1 Recommendation 18 suggests a recursive approach where the review of a previous year's activity will influence the decisions about the initiatives in the future. The SSR2 Review Team did not find evidence of an informal or undocumented internal process, nor did it find a public, annual, operational review of the implementation of the IS-SSR Framework.

SSR1 Recommendation 19

"ICANN should establish a process that allows the Community to track the implementation of the SSR Framework. Information should be provided with enough clarity that the Community can track ICANN's execution of its SSR responsibilities."

SSR2 Conclusion: This recommendation remains relevant. Due to a lack of specificity of "enough clarity," this recommendation is not measurable in its entirety. This recommendation has not achieved its intended effect as the community remains unable to track SSR-related activities in a reasonable time frame and in an open and transparent manner.

Please see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management for the SSR2 recommendation that expands upon the original SSR1 recommendation.

Rationale:

- ICANN org reports that the publication of the annual IS-SSR Framework162 tracks progress against the activities committed to in the previous year's framework. Additionally, regular project management reporting, operating plans, and budgets are considered tools that provide details on SSR activities. However, publishing an annual IS-SSR Framework on the website does not seem to serve the purpose of informing the community and allowing them to track the implementation of the framework. Documentation of the implementation lags very much behind the implementation, so it does not offer the community a way to track the SSR-related activities.
- Moreover, it appears that the SSR1 RT provided an example to have a public dashboard for tracking the SSR-related activities, as was done to implement one of the recommendations of ATRT. However, there is no evidence that such a dashboard is available to the community or public for SSR-related activities.

SSR1 Recommendation 20

"ICANN should increase the transparency of information about organization and budget related to implementing the SSR Framework and performing SSR-related functions."

SSR2 Conclusion: This recommendation remains relevant and was partially implemented. The intended effect of improved transparency around SSR-related details as they relate to the organization and the budget was not achieved.

Please see SSR2 Recommendation 3: Improve SSR-related Budget Transparency for the SSR2 recommendation that expands upon the original SSR1 recommendation.

[162] IS-SSR Document Archive, https://www.icann.org/ssr-document-archive.

Rationale:

- ICANN's Planning Process cycle has a threefold approach encompassing a Strategic Plan, a Five-Year Operating Plan, and an Annual Operating Plan & Budget.[163] The cycle culminates with Achievement & Progress Reporting. Phase I, as described in the Implementation Reports on the SSR1 Implementation Wiki, is now in place to provide public information about SSR-related plans, budgets, and activities (as outlined in SSR1 Recommendation 2); this is integrated with ICANN's IS-SSR Framework and reports on SSR activities and expenditures.[164] Periodic SSR activity reporting augments this public information.[165] Phase II is underway to identify mechanisms that provide more detailed public information on SSR-related budgets and expenditures across multiple ICANN departments. Currently, public information on this topic for FY18 can be found on the Rec #20 wiki page.[166]
- Staff also developed an after-event-report that includes budget and resource impacts related to managing an event.[167] No after-event reports have been published as of March 2020. A template for a public version of these reports can be found on the Rec #20 wiki page.
- Annual reporting on SSR-related activities does take place in the framework documents and annual reports. Budget documents have very high-level line items to activities related to SSR. Those same activities do not appear to be reported on in ICANN's regular project management reporting. The Implementation Report says that ICANN will "*Integrate SSR Framework and reports on SSR activities and expenditures into the planning framework and process to provide public information about SSR-related plans, budgets and activities*."[168] However, as noted for SSR1 Recommendation 19, the ICANN Portfolio Management System and the KPI Project Dashboard have very limited amounts of information that the community can use to track SSR-related efforts.
- The FY2018 approved budget has three portfolio areas related to SSR: Identifier Evolution; Security, Stability, and Resiliency of Internet Identifiers; and Technical Reputation. Only the first two (Identifier Evolution and SSR of Internet Identifiers) have dedicated budgets at the portfolio level; no detail of these budgets is provided. The staff implementation report also says that ICANN will *"Identify mechanisms that provide more detailed public information on SSR-related budgets and expenditures across multiple ICANN departments,"* suggesting further work is expected on this aspect of implementation.

SSR1 Recommendation 21

"ICANN should establish a more structured internal process for showing how organization and budget decisions relate to the SSR Framework, including the underlying cost-benefit analysis."

[163] "ICANN Planning Process," https://www.icann.org/resources/pages/governance/planning-en.

[164] SSR1 Review Implementation Home, https://community.icann.org/display/SSR/SSR1+Review+Implementation+Home.

[165] Identifier Systems SSR Activities Reporting, https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-en.

[166] SSR1 Review Implementation, Rec #20, last updated 18 September 2018, https://community.icann.org/display/SSR/Rec+%2320.

[167] Identifier Systems SSR Activities Reporting, https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-en.

[168] See SSR1 Implementation Report updates for Recommendation 20, https://community.icann.org/download/attachments/54691765/SSR%20Recs%201-28.pdf?api=v2.

SSR2 Conclusion: This recommendation remains relevant and was partially implemented. It did not achieve the intended effect of an open and transparent process regarding SSR-related budget decisions.

Please see SSR2 Recommendation 3: Improve SSR-Related Budget Transparency for the SSR2 recommendation that expands upon the original SSR1 recommendation.

Rationale:

- In the staff implementation report, there are three deliverables mentioned:
  - Integration of the IS-SSR Framework and reports into the planning framework and process to provide public information about SSR-related plans, budgets, and activities.
  - Identification of mechanisms that provide more detailed public information on SSR-related budgets and expenditures across multiple ICANN departments.
  - Exploration after-event reports that include budget and resource impact related to managing the event.
- The staff report specifically mentions a report template for publishing information related to budgets and resources impacted by security events.[169] The staff report suggests that this will be published annually every fiscal year, starting in FY18. An examination of SSR-related pages on the ICANN website indicates that no report has been published. Annual reporting on SSR-related activities does take place in the framework documents and annual reports. The budget document has some very high-level line items for activities related to SSR. However, those same activities do not appear to be reported on in ICANN's regular project management reporting. This observation is the same as in SSR1's findings for SSR1 Recommendation 20. In addition, the reporting on budget and resource impacts of SSR events appears to have never been done, and the template for supporting that reporting does not appear to be available for public review or comment.
- ICANN's planning process ensures that activities planned and budgeted for, including those related to SSR, are identified by specific objectives. There has been no plan for requesting public comments on the template being used for publishing more detailed public information on SSR-related budgets and expenditures. The template now appears to have been replaced by the annual report for the fiscal year.

SSR1 Recommendation 22

"ICANN should publish, monitor and update documentation on the organization and budget resources needed to manage SSR issues in conjunction with introduction of new gTLDs."

SSR2 Conclusion: This recommendation remains relevant and was partially implemented. The implementation did not achieve the full, intended effect.

Please see SSR2 Recommendation 3: Improve SSR-related Budget Transparency for the SSR2 recommendation that expands upon the original SSR1 recommendation.

Rationale:

- Public information on SSR-related budget and expenditures across multiple ICANN departments was posted for FY18 and can be found here: https://community.icann.org/x/DqNYAw. This report is updated annually and covers direct costs resulting from the activities required to perform the SSR functions, direct costs of shared resources, and the costs of support functions allocated to SSR. This report does not

[169] SSR1 Review Implementation, Rec #20, https://community.icann.org/display/SSR/Rec+%2320.

provide a breakdown of funding, resources, or other activities related to the New gTLD Program.

- ICANN org has also explored mechanisms that provide more public information on SSR-related budgets and expenditures across multiple ICANN departments. However, a template for that public information does not break out SSR activities or budgets related to the New gTLD Program.
- It is clear that the organization and budget for SSR issues related to the new gTLD team were provided via the security team, but also reflected in the budget and organization for the New gTLD Program (e.g., DNS Stability Panel, EBERO, other process steps, etc.). It appears that the desired outcome of the implementation of this recommendation was to improve the amount and clarity of information on the organization and budget for implementing the IS-SSR Framework and performing SSR-related functions related to the New gTLD Program.
- In the ICANN IS-SSR Document Archive, there is no document that is specific to the New gTLD Program. In the 30 September 2016 Framework, gTLDs are mentioned twice, once in Module A as a trend in the Internet ecosystem, and second in Module B as part of the overall ICANN Strategic Plan. In the FY14 SSR Framework, published in March 2013, the New gTLD Program is again mentioned as a "trend," and as a policy driver for the GNSO. The only remaining mentions of the New gTLD Program are in the section reporting on the implementation of the SSR1 recommendations.

SSR1 Recommendation 23

"ICANN must provide appropriate resources for SSR-related Working Groups and Advisory Committees, consistent with the demands placed upon them. ICANN also must ensure decisions reached by Working Groups and Advisory Committees are reached in an objective manner that is free from external or internal pressure."

SSR2 Conclusion: This recommendation remains relevant and was partially implemented. The intended effect was to allow the working groups and Advisory Committees to fulfill their mandates in an objective manner that is free from external or internal pressures and is not measurable.

Please see SSR2 Recommendation 3: Improve SSR-related Budget Transparency for the SSR2 recommendation that expands upon the original SSR1 recommendation.

Rationale:

- ICANN org does provide ICANN technical support staff to the SSAC and RSSAC to assist with writing documents. ICANN org's budget includes some funding to support SSAC and RSSAC to conduct meetings (specifically travel expenses, hotel, food); ICANN org pointed the SSR2 Review Team to the 2015 budget as an example.[170] The support funding has never been linked to, or conditioned by, any formal performance, output, or content evaluation. ICANN believes this enables adequate independence. In practice, it is not clear how RSSAC's or SSAC's work priorities are determined or evaluated by ICANN or the community, which creates an accountability gap, in addition to making it impossible to evaluate whether they have resources "consistent with the demands placed upon them." The original SSR1 report included the following text associated with this recommendation:

[170] ICANN, "FY15 Adopted Operating Plan and Budget," 1 December 2014, 77-78, https://www.icann.org/en/system/files/files/adopted-opplan-budget-fy15-01dec14-en.pdf.

"In discussions with the SSAC, it became apparent that at times they felt pressure to deliver an answer to specific problem within a very limited timeframe. This led to a shorter time period to evaluate the issue and more targeted recommendations as a result. Clearly, there will be times, when looking at immediate risks, that a timeframe is enforced upon research work. This is unavoidable. It would be prudent, however, to ensure that with proper planning, the SSAC and RSSAC are given as much time as possible to provide high-quality research work and findings."

This observation echoes circumstances and concerns over the last couple of years, especially in the context of the KSK rollover in October 2018, when SSAC struggled to respond to requests for advice on short time frames with inadequate data/research available to inform the debate.[171] The fraction of ICANN's budget directed to SSAC is likely inadequate, given the many prevailing and emerging SSR issues, and the expectations that SSAC deliver advice that requires research or synthesis of previous research. The current structure of SSAC is also not compatible with "high-quality research work," since it is composed of a set of "volunteers" mostly from industry and being subsidized by their employer for their time to participate, and thus not "free from external pressure."

- The lack of metrics and monitoring of success or failure of the New gTLD Program indicates this multistakeholder approach is not "free of external pressures." It is impossible to conclude, using metrics from the CCT RT's report on DNS abuse in new gTLDs, that the New gTLD Program has been successful from a CCT perspective. Such research falls well within the roles and responsibilities of ICANN's Security Team (See SSR1 Recommendation 24). ICANN did not undertake or fund this sort of exercise itself, likely because external pressures against this sort of SSR research activity prevailed.
- There is nothing in the SSAC operational procedures document about managing external and internal pressures, except Section 2.1.2 Withdrawals and Dissents, which means each member, and the committee itself, self-manages conflicts of interest, and all deliberations are confidential for security reasons.[172] The same appears true for RSSAC and RZERC, but in these two cases, the committees are architected such that each person represents a stakeholder.
- Important stakeholders are consistently missing from some of these SSR-related advisory committees (e.g., victims of identifier abuse, academic researchers, law enforcement, policymakers).

SSR1 Recommendation 24

"ICANN must clearly define the charter, roles and responsibilities of the Chief Security Office Team."

SSR2 Conclusion: The recommendation remains relevant and was partially implemented. It did not achieve the intended effect of having a clear charter, defined roles, and defined responsibilities for the Chief Security Office Team.

Please see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management for the SSR2 recommendation that expands upon the original SSR1 recommendation.

[171] ICANN, "First Root KSK Rollover Successfully Completed," ICANN Announcements, 15 October 2018, https://www.icann.org/news/announcement-2018-10-15-en.

[172] ICANN Security and Stability Advisory Committee, "SSAC Operational Procedures Version 5.1," 27 February 2019, 10, https://www.icann.org/en/system/files/files/operational-procedures-27feb18-en.pdf.

Rationale:

- As of 2018, there is no Chief Security Office. However, the OCTO (Office of the Chief Technical Officer) SSR team works on externally focused ICANN-related SSR issues, the CIO and team work on internally focused security issues, and the OCTO research team looks towards future SSR risks and opportunities within ICANN's limited scope and remit.173 The web page for this team describes the mission of this team in high-level terms, and links to a page of SSR "activities."174 There is no language referring to "charter," "roles," or "responsibilities" of this team. The SSR2 team assumes that the activities listed on this page are what ICANN intends as the SSR-related roles and responsibilities of OCTO:
  - Engage actively with security, operations, and public safety communities to gather and process intelligence data that indicate (imminent) threats to DNS or domain registration service operations (the "DNS ecosystem").
  - Facilitate or participate with these same communities in threat preparedness activities to protect against or mitigate threats to the DNS ecosystem.
  - Perform studies or analyze data to better understand the health and well-being of the DNS ecosystem.
  - Coordinate DNS vulnerability disclosure reporting (https://www.icann.org/vulnerability-disclosure.pdf).
  - Lend subject matter expertise to build capability among ccTLD and public safety communities in subjects relevant to the DNS ecosystem, including DNSSEC, abuse, or misuse of DNS infrastructures or operations.
  - Assist in DNS ecosystem risk management activities.
  - With ICANN's Global Stakeholder Engagements team, participate in a global, multistakeholder effort to improve cybersecurity and mitigate cybercrime.
- OCTO does not seem to have produced much in terms of SSR analysis that is available to the public. The Open Data Initiative, the DAAR reporting, and the Internet metrics project all seem to be projects with associated data that is internal to ICANN org. It is not clear how useful any of this work has been thus far to the larger community that ICANN org is intended to serve.

SSR1 Recommendation 25

"ICANN should put into place mechanisms for identifying both near and longer-term risks and strategic factors in its Risk Management Framework."

SSR2 Conclusion: This recommendation remains relevant and was partially implemented. The implementation did not have the full, intended effect.

Please see SSR2 Recommendation 4: Improve Risk Management Processes and Procedures for the SSR2 recommendation that expands upon the original SSR1 recommendation.

Rationale:

- A Risk Management Framework was accepted by the ICANN Board in 2013, having received community input during ICANN50 and ICANN51. ICANN org maintains an Enterprise Risk Management (ERM) Dashboard that lists risks to be monitored and

[173] ICANN OCTO, "Office of the Chief Technology Officer (OCTO)," accessed 27 December 2019, https://www.icann.org/octo..

[174] ICANN OCTO, "Internet Identifier System Security, Stability, and Resiliency," accessed 27 December 2019, https://www.icann.org/octo-ssr.

addressed and follows an enterprise risk management framework. However, while a mechanism has been put in place, there is a lack of clarity in terms of how risk identification feeds into relevant SSR processes and policies.

SSR1 Recommendation 26

"ICANN should prioritize the timely completion of a Risk Management Framework."

SSR2 Conclusion: This recommendation remains relevant and was partially implemented. Given that the term "timely" does not offer any specificity in what was intended or acceptable, it cannot be assessed if the intended effect was achieved.

Please see SSR2 Recommendation 4: Improve Risk Management Processes and Procedures for the SSR2 recommendation that expands upon the original SSR1 recommendation.

Rationale:

- A Risk Management Framework was accepted by the ICANN Board in 2013,175 having received community input during ICANN50 and ICANN51. A more detailed response for this recommendation is addressed under the assessment for Recommendation 27.

SSR1 Recommendation 27

"ICANN's Risk Management Framework should be comprehensive within the scope of its SSR remit and limited missions."

SSR2 Conclusion: This recommendation remains relevant. Given the absence of a definition of "comprehensive" by SSR1 or metrics for evaluation, the SSR2 Review Team was unable to assess whether this recommendation was fully implemented. ICANN org did not achieve the intended effect of providing comprehensive, easy-to-find, information on the risk management framework used by ICANN.

Please see SSR2 Recommendation 4: Improve Risk Management Processes and Procedures for the SSR2 recommendation that expands upon the original SSR1 recommendation.

Rationale:

- The SSR2 Review Team discussed whether SSR1 Recommendation 27 was implemented based on the references made by staff during various question and answer exchanges related to SSR1 Recommendation 25. The SSR2 Review Team concluded, however, that this recommendation, while it correlates to SSR1 Recommendations 25 and 26, is distinct because it asks that the framework be "comprehensive." The SSR2 Review Team was of the opinion that if SSR1 Recommendation 27 was implemented in line with what the SSR1 Review Team intended, it would have addressed the same concerns that SSR1 Recommendation 25 and 26 were probably seeking to address.
- SSR1 gave no definition as to what elements of the framework would constitute "comprehensive" or how this should be evaluated. During the review, it was noted that this recommendation would have been implemented by ICANN staff that are no longer with ICANN org. In this regard, institutional memory and a complete historical record of how they assessed the "comprehensiveness" of the Risk Management Framework was not available.

[175] ICANN, "DNS Risk Management Framework Report," last modified 4 October 2013, https://www.icann.org/public-comments/dns-rmf-final-2013-08-23-en.

- Publicly available information as to how risk management is addressed was found in piecemeal locations. As an example, staff indicated that the Board Risk Management Committee was made up of the ICANN org executive team, which provides oversight. Further, that there are function-related risk liaisons who are staff members representing each function for implementing the risk framework, and all organization personnel who own the risks inherent in their activities, focuses on risk management issues; this demonstrates that the risk function for ICANN org has not been centralized and coordinated strategically.

SSR1 Recommendation 28

"ICANN should continue to actively engage in threat detection and mitigation, and participate in efforts to distribute threat and incident information."

SSR2 Conclusion: This recommendation remains relevant and was not fully implemented. While ICANN org has engaged with a variety of groups to help detect, mitigate, and share information about threats and incidents, the intended effect of having this information made available outside those named groups was not achieved.

Please see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management, SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties, SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review, and SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting, for the SSR2 recommendations that expand upon the original SSR1 recommendation.

Rationale:

- The SSR2 Review Team did not find any publicly available data shows that ICANN org engages in threat detection and mitigation. ICANN org, when feasible, disseminates to responsible external third-parties vulnerabilities reported. However, it is the responsibility of the third-party to act on the threat and incident information disseminated.
- There is no public evidence that the ICANN organization conducts ongoing threat detection nor that anyone is tasked with this function. The ICANN community, however, has a number of groups (both open and closed) that actively conduct threat detection, including SSAC, RSSAC, TLDOPS, ccNSO incident response WG, and PSWG. The OCTO SSR team coordinates with these groups.

Appendix E: Research Data on Reports of DNS Abuse Trends

Examples connected to the DNS to varying degrees include:

- Malware: From 2016 to 2018, the number of unique URLs recognized as malicious by antivirus software more than doubled to 554,159,6213[176], and mobile malware attacks nearly doubled from 2017 to 2018 to over 116 million[177].
- Digital Certificate Fraud: APWG reports that phishers are increasingly using digital certificates to make attacks look legitimate and to defeat browser fraud detection warnings.[178] Due to ICANN's removal of access to WHOIS, SSL certificate administration no longer has access to domain name registration data and cannot use the domain name ownership records that ICANN org is charged with coordinating to validate domain name ownership. PhishLabs determined that half of all phishing sites use SSL encryption, which can fool users into thinking that a site is safe to use, for example, by virtue of the green lock symbol that appears in the browser address bar when SSL encryption is enabled. Some of the increase comes from phishers adding HTTP encryption to their phishing sites – a technique that turns a security feature against the victims.[179]
- Phishing: APWG reported that phishers are registering domain names directly to perpetrate fraud and that the methods of phishing attacks have become more effective and harder to detect.

  > "*Phishers are increasingly using web page redirects as a way of hiding their phishing sites from detection. When victims click on the links in phishing emails, redirects take the user on an unwitting journey through other sites before arriving at the phishing site itself. And then once the victim submits his or her credentials, still more redirects may take the victim to yet another domain."*[180]

- Business Email Compromise: The U.S. FBI Internet Crime Center reported a 136% increase in identified global exposed losses from 2016 to 2018 resulting from Business Email Compromise, affecting all 50 U.S. states and 150 countries worldwide. From October 2013 to May 2018, the FBI documented a multi-billion-dollar growth in BEC, which often involves fraudulent registration of domain names that are deceptively similar to one of the targeted parties.[181]
- Scams: The Australian Competition and Consumer Commission (ACCC) ScamWatch reported a near doubling in losses from scams in roughly the last three years, rising to AUD

[176] AMR, "Kaspersky Security Bulletin 2018: Statistics," 4 December 2018, https://securelist.com/kaspersky-security-bulletin-2018-statistics/89145/.
[177] Victor Chebyshev, "Mobile Malware Evolution 2018," 5 March 2019, https://securelist.com/mobile-malware-evolution-2018/89689/.
[178] APWG, "APWG Phishing Activity Trends Report 3rd Quarter 2018," 11 December 2018, https://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf.
[179] Elliot Volkman, "49 Percent of Phishing Sites Now Use HTTPS," PhishLabs blog, 6 December 2018, https://info.phishlabs.com/blog/49-percent-of-phishing-sites-now-use-https.
[180] APWG Phishing Activity Trends Report, https://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf.
[181] "Business E-Mail Compromise The 12 Billion Dollar Scam," Federal Bureau of Investigations Public Service Announcement, 12 July 2018, https://www.ic3.gov/media/2018/180712.aspx.

11.8 million in losses in 2019.[182] Domain names used to perpetrate online scams very typically infringe on brand or business names. Scammers register these names with little or no control over the volumes of similar names the scammer can register and limited access to information that investigators can use to identify the criminal actors.

- Botnets: In 2017, Spamhaus DBL listed 50,000 botnet controller domain names registered and set up by cybercriminals for the sole purpose of hosting a botnet controller. More than 25% of these registered botnet domain names have been registered through a single registrar, Namecheap.[183] In 2018, Spamhaus listed 103,503 botnet controller domain names, a 106% increase. Namecheap remained the most abused registrar, with a 220% increase in registered botnet controller domain names.[184]
- Spam: Spam is the preferred delivery infrastructure for phishing, malware, and other DNS-related threats. The average daily spam volume was 416.04 billion as of August 2019.[185]

> *"No matter how much the threat landscape changes, malicious email and spam remain vital tools for adversaries to distribute malware because they take threats straight to the endpoint. By applying the right mix of social engineering techniques, such as phishing and malicious links and attachments, adversaries need only to sit back and wait for unsuspecting users to activate their exploits."*[186]

- DDoS Attacks: Distributed denial of service (DDoS) attacks increased by 40% from mid-2017 to mid-2018.[187] DDoS maximum attack size increased globally by 174% in the first half of 2018 over the same period in 2017, and the largest attack ever recorded (1.7 Tbps) struck a major North American service provider in February 2018.[188] Because everything – from businesses to government agencies to physical public works infrastructure – is dependent on uninterrupted DNS-related services, unmitigated DDoS attacks are increasingly harmful. DDoS attacks also have become more complex, and multi-vector attacks are now the most commonly employed. Verisign reported that 52% of their attacks recorded in the second quarter of 2018 were multi-vector attacks.[189] Additionally, the Internet of Things (IoT) is a growing concern for DDoS attacks because these connected

[182] ScamWatch, Australian Competition and Consumer Commission, https://www.scamwatch.gov.au/about-scamwatch/scam-statistics.
[183] "Spamhaus Botnet Threat Report 2017," Spamhaus Malware Labs, last modified 8 January 2018, https://www.spamhaus.org/news/article/772/spamhaus-botnet-threat-report-2017.
[184] "Spamhaus Botnet Threat Report 2019," Spamhaus Malware Labs, n.d., https://www.spamhaustech.com/botnet-threat-report-2019/
[185] "Email and Spam Data," Cisco Talos Intelligence Group, https://www.talosintelligence.com/reputation_center/email_rep.
[186] "Cisco 2018 Annual Cybersecurity Report," Cisco Systems, February 2018, https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf.
[187] "H1 2018 DDOS Trends Report," Corero Network Security, n.d., https://info.corero.com/report-2018-half-year-ddos-trends-report-download.html.
[188] Kevin Whalen, "Entering the Terabit Era: Get Ready For Bigger DDoS Attacks," 5 September 2018, https://www.netscout.com/blog/entering-terabit-era-get-ready-bigger-ddos-attacks.
[189] "Q2 2018 DDOS Trends Report: 52 Percent of Attacks Employed Multiple Attack Types," Verisign blog, last modified 27 September 2018, https://blog.verisign.com/security/ddos-protection/q2-2018-ddos-trends-report-52-percent-of-attacks-employed-multiple-attack-types/.

devices are easy targets, and they continue to proliferate. The number of connected devices was 27 billion in 2017 and is predicted to reach 125 billion by 2020.[190]

[190] John English, "Getting the Network Ready to Meet IoT Expectations," NETSCOUT blog, last modified 28 February 2018, https://www.netscout.com/blog/getting-network-ready-meet-iot-expectations.

Appendix F: Research Data on Cryptography

Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) offers an alternative to the RSA public-key cryptography currently used for DNSSEC. The technique is based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys.[191]

The root KSK DPS provides guidance on key length and key rollover. The DPS says nothing, however, about the procedures for changes to the digital signature algorithm. Recent guidance from the U.S. National Security Agency recommends using 3072 bits for RSA. The Edwards-Curve Digital Security Algorithm (EdDSA) seems to offer a better alternative than very large RSA keys.[192]

Post Quantum Cryptography

Most people had not heard of quantum computing a decade ago, but it has captured the public's imagination in recent years. Part of this interest comes from the unique computational power of a quantum computer. The U.S. National Academy of Sciences recently issued a report on "Quantum Computing: Progress and Prospects," with the high-level conclusion that now is the time to start preparing for a quantum-safe future.[193]

DigiCert has estimated that it takes several quadrillion years to factor a 2048-bit RSA key using classical computing technology.[194] In the future, if a large-scale quantum computer is invented, it can break the same key much faster, perhaps in only a few months. There are still many technical challenges that must be overcome before it is possible to build a quantum computer that threatens RSA and ECC, the two main asymmetric cryptographic algorithms used to secure the Internet.

Progress towards a large-scale quantum computer must track the scaling rate of the number of physical quantum bits or "qubits" computers have and error rates. Error rates are important because they significantly impact the number of physical qubits required to make a logical qubit. Physical qubits are the individual quantum systems representing either a zero or a one; however, physical qubits are prone to errors through unavoidable interactions with their environment even at temperatures approaching absolute zero. Many physical qubits can be

---

[191] See the following RFCs for more information on potential new algorithms for DNSSEC signatures: Hoffman, P. and W. Wijngaards, "Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC", RFC 6605, DOI 10.17487/RFC6605, April 2012, <https://www.rfc-editor.org/info/rfc6605>, Sury, O. and R. Edmonds, "Edwards-Curve Digital Security Algorithm (EdDSA) for DNSSEC", RFC 8080, DOI 10.17487/RFC8080, February 2017, <https://www.rfc-editor.org/info/rfc8080>, and Wouters, P. and O. Sury, "Algorithm Implementation Requirements and Usage Guidance for DNSSEC", RFC 8624, DOI 10.17487/RFC8624, June 2019, <https://www.rfc-editor.org/info/rfc8624>.

[192] Wouters and Sury, RFC 8624, https://www.rfc-editor.org/info/rfc8624.

[193] National Academies of Sciences, Engineering, and Medicine. 2019. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press. https://doi.org/10.17226/25196.

[194] Hollebeek, Timothy, "DigiCert on Quantum: National Academy of Sciences Report," DigiCert blog, 9 January 2019, https://www.digicert.com/blog/digicert-on-quantum-national-academy-of-sciences-report/.

combined into a single logical qubit, and the additional qubits are used to detect and correct these errors. Researchers have yet to produce even a single logical qubit, though progress is rapidly being made towards that goal. Once logical qubits are available, tracking the number of logical qubits will be the metric to track.

Industry standards groups are also preparing for a post-quantum future. The most well-known activity is the NIST post-quantum cryptography project, which works with researchers around the world to develop new cryptographic primitives that are not susceptible to attack by quantum computers.[195] One can expect that project to take several more years before the resulting algorithms are ready for standardization.

In the meantime, researchers agree that hash-based signatures are post-quantum safe. The Internet Research Task Force (IRTF) has specified these signature algorithms in their Crypto Forum Research Group (CFRG), using small private and public keys with a low computational cost.[196] However, the signatures are quite large, and a private key can only produce a finite number of signatures. While these algorithms are available today, these last two properties make hash-based signatures undesirable in the DNSSEC environment.

[195] National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Resource, Center, "Post-Quantum Cryptography," Created January 03, 2017, Updated November 23, 2020, https://csrc.nist.gov/projects/post-quantum-cryptography.
[196] IRTF, Crypto Forum Research Group, https://irtf.org/cfrg.

Appendix G: Mapping of SSR2 Recommendations to the ICANN 2021-2025 Strategic Plan and the ICANN Bylaws

Relevant ICANN Bylaws

Bylaws Section 1.2.(a)(i) and 1.2 (a) (ii) and Section 27.1(c)(i)(B) regarding preserving and enhancing "the administration of the DNS and the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet,"

Bylaws Section 3.6(a) – Assisting the Board in considering and reporting on the "possible material effects, if any, of its decision on the global public interest, including a discussion of the material impacts to the security, stability and resiliency of the DNS."

Bylaws Section 12.2(b) and 12.2(c) – Working closely with the Security and Stability Advisory Committee and the Root Server System Advisory Committee in particular, and ensuring the ICANN Board and ICANN org are executing fully on their accepted advice.

Bylaws Annex G-1 The topics, issues, policies, procedures and principles referenced in Section 1.1(a)(i) with respect to gTLD registrars and gTLD registries are: "issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, security and/or stability of the Internet, registrar services, registry services, or the DNS" and "security and stability of the registry database for a TLD."

Relevant Strategic Plan Goals and Objectives

From the ICANN Strategic Plan for Fiscal Years 2021–2025.[197]

1. Strengthen the security of the Domain Name System and the DNS Root Server System.

1.1 Improve the shared responsibility for upholding the security and stability of the DNS by strengthening DNS coordination in partnership with relevant stakeholders.
1.2 Strengthen DNS root server operations governance in coordination with the DNS root server operators.
1.3 Identify and mitigate security threats to the DNS through greater engagement with relevant hardware, software, and service vendors.
1.4 Increase the robustness of the DNS root zone key signing and distribution services and processes.

2. Strategic Objective: Improve the effectiveness of ICANN's multistakeholder model of governance.

2.1. Strengthen ICANN's bottom-up multistakeholder decision-making process and ensure that work gets done and policies are developed in an effective and timely manner.
2.2 Support and grow active, informed, and effective stakeholder participation.

[197] ICANN Strategic Plan for Fiscal Years 2021–2025, https://www.icann.org/en/system/files/files/strategic-plan-2021-2025-24jun19-en.pdf.

2.3 Sustain and improve openness, inclusivity, accountability, and transparency.

3. Strategic Objective: Evolve the unique identifier systems in coordination and collaboration with relevant parties to continue to serve the needs of the global Internet user base.

3.1 Foster competition, consumer choice, and innovation in the Internet space by increasing awareness of, and encouraging readiness for Universal Acceptance, IDN implementation, and IPv6.
3.2 Improve assessment of, and responsiveness to, new technologies which impact the security, stability, and resiliency of the Internet's unique identifier systems by greater engagement with relevant parties.
3.3 Continue to deliver and enhance the IANA functions with operational excellence.
3.4 Support the continued evolution of the Internet's unique identifier systems with a new round of gTLDs that is responsibly funded, managed, risk-evaluated, and consistent with ICANN processes.

4. Strategic Objective: Address geopolitical issues impacting ICANN's mission to ensure a single, globally interoperable Internet.

4.1 Identify and address global challenges and opportunities within its remit by further developing early warning systems, such as ICANN org's Legislative and Regulatory Development Reports.
4.2 Continue to build alliances in the Internet ecosystem and beyond to raise awareness of and engage with global stakeholders about ICANN's mission and policymaking.

5. Strategic Objective: Ensure ICANN's long-term financial sustainability.

5.1 Implement a five-year Financial Plan that supports the five-year Operating Plan.
5.2 Develop reliable and predictable funding projections.
5.3 Manage operations and their costs to optimize the effectiveness and efficiency of ICANN's activities.
5.4 Ensure that the level of ICANN reserves is continuously set, reached, and maintained consistent with the complexity and risks of the ICANN environment.

#	Recommendation	Strategic Objective and Goal
1	Complete the implementation of all relevant SSR1 recommendations.	Strategic Objectives 1, 2, and 3
2	SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management	Strategic Objectives 1, 3, and 4
3	SSR2 Recommendation 3: Improve SSR-related Budget Transparency	Strategic Objectives 1, 2, 3, and 5; and Strategic Goals 2.1 and 3.4
4	SSR2 Recommendation 4: Improve Risk Management Processes and Procedures	Strategic Objectives 1, 2, 3, 4, and 5

5	SSR2 Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications	Strategic Objective 1
6	SSR2 Recommendation 6: SSR Vulnerability Disclosure and Transparency	Strategic Objectives 1, 2, 3, and 4; and Strategic Goals 1.1, 1.2, 1.3, and 4.1
7	SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures	Strategic Objectives 1, 3, and 4; and also Strategic Goals 1.1, 1.4, and 3.3
8	SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties	Strategic Objectives 1 and 3; and Strategic Goals 1.1, 1.2, 1.3, and 1.4
9	SSR2 Recommendation 9: Monitor and Enforce Compliance	Strategic Objectives 1, 2, and 3; and Strategic Goal 2.1
10	SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms	Strategic Objective 1
11	SSR2 Recommendation 11: Resolve CZDS Data Access Problems	Strategic Objective 3; and Strategic Goal 3.2
12	SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review	Strategic Objectives 1, 2, 3, 4, and 5
13	SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting	Strategic Objectives 1 and 3; and Strategic Goal 2.1
14	SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements	Strategic Objective 1; and Strategic Goal 1.1
15	SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements	Strategic Objective 1; and Strategic Goal 1.1
16	SSR2 Recommendation 16: Privacy Requirements and RDS	Strategic Objectives 1, 3, and 5
17	SSR2 Recommendation 17: Measuring Name Collisions	Strategic Objectives 1, 3, and 4; and Strategic Goal 3.4
18	SSR2 Recommendation 18: Informing Policy Debates	Strategic Objectives 1, 3, and 4; and Strategic Goal 3.2
19	SSR2 Recommendation 19: Complete Development of the DNS Regression Test Suite	Strategic Objective 1; and Strategic Goals 1.1, 1.2, 1.3, and 1.4
20	SSR2 Recommendation 20: Formal Procedures for Key Rollovers	Strategic Objectives 1, 2, and 4; and Strategic Goal 1.4

21	SSR2 Recommendation 21: Improve the Security of Communications with TLD Operators	Strategic Objective 1, and Strategic Goal 3.3
22	SSR2 Recommendation 22: Service Measurements	Strategic Objectives 1, 2, 3, 4, and 5; and Strategic Goals 1.1, 1.2, 2.1, 3.2, 3.4, and 4.1
23	SSR2 Recommendation 23: Algorithm Rollover	Strategic Objectives 1 and 3
24	SSR2 Recommendation 24: Improve Transparency and End-to-end Testing for the EBERO Process	Strategic Objective 1; and Strategic Goal 1.2

Appendix H: Public Comment Analysis

The SSR2 Review Team created a spreadsheet to record its response to public comments and changes resulting from public comments. The file is available on the Review Team Documents and Drafts page of the SSR2 wiki or can be downloaded directly using the links below.

Excel:
https://community.icann.org/pages/viewpage.action?pageId=64076120&preview=/64076120/155191048/Public%20Comment%20Feedback%20-%20March%202020.xlsx

PDF:
https://community.icann.org/pages/viewpage.action?pageId=64076120&preview=/64076120/155191042/Public%20Comment%20Feedback%20-%20March%202020.pdf

Appendix I: Fact Sheets

The ICANN organization publishes fact and expense sheets on a quarterly basis, as well as participation and milestones updates on a monthly basis. These documents bring transparency and accountability to the community on how review team resources and time are being used.

The Fact Sheet captures attendance of review team members, costs associated with professional services and travel to attend face-to-face meetings, milestones, and participation.

Definitions are as follows:

Professional Services: Approved budget for the review team to use for services of independent experts, as noted in Bylaws Section 4.6(a)(iv). Review teams may also solicit and select independent experts to render advice as requested by the review team. ICANN shall pay the reasonable fees and expenses of such experts for each review contemplated by this Section 4.6 to the extent such fees and costs are consistent with the budget assigned for such review. Guidelines on how review teams are to work with and consider independent expert advice are specified in the Operating Standards.

Travel: Amount approved for review team travel for face-to-face meetings. Examples of travel expenditures include, but are not limited to, charges for airfare, hotel, per diem reimbursement, venue meeting costs, audio-visual/tech support, and catering. These expenses include Review Team and the ICANN organization support travel.

ICANN Organization Support: Amount approved in the budget for the ICANN organization to contract outside services to support the work of the review team.

Spent to Date: Amounts include quarterly financials since inception of the work by the review team through the most recent quarter end.

Committed Services:
1. Travel: Estimated expenses for approved face-to-face meetings.
2. Professional Services: Included services from signed contracts to be provided or invoiced.

These are typically for non-employee related support services provided by contractors. Total

Spent and Committed to Date: This is the sum of the “Spent to Date” and “Committed Services” amounts through the most recent quarter end. The Committed Services amount does not include the Spent to Date amounts. Remaining Budget: This is the difference between the “Approved Budget” and the “Total Spent and Committed to Date” amounts. Fact sheet archives may be viewed at: https://community.icann.org/x/S7zRAw.