Security, Stability, and Resiliency (SSR2) Review

Executive Summary

This report is an early draft of the findings and recommendations from the SSR2 Review Team. There are several items that the SSR2 RT continues to iterate on, but overall the review team believes the report is at a point where public feedback would provide useful and critical input to inform the final report.

In particular, the SSR2 RT would appreciate feedback on:

- the findings and recommendations;
- which part of ICANN (e.g., the Board, ICANN org, or the ICANN community) should address each recommendation;
- what metrics would be most appropriate to make each recommendation measurable, while avoiding over engineering the solution;
- what priority should be given to each recommendation;
- any additional reports or other material you feel the review team should consider before completing their recommendations (please see the SSR2 wiki,[1] including “background materials,” “briefing materials” and “Q&As” for material the team has reviewed).

Per the established community review process, the community also will have additional opportunities for input on the SSR2's final report.

Overview

Introduction

[To be added in the final report.]

Background

[To be added in the final report.]

Objectives

Under the ICANN org Bylaws[2] (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”).’

Specifically:

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

[1] ICANN SSR2 Review Team wiki, https://community.icann.org/display/SSR/SSR2+Review.

[2] “Bylaws for Internet Corporation for Assigned Names and Numbers,” ICANN, as amended 28 November 2019, https://www.icann.org/resources/pages/governance/bylaws-en.

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

iii. The SSR Review Team shall also assess the extent to which ICANN 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.

SSR2 Recommendations - Summary

The SSR2 Review Team has aligned all SSR2 recommendations with the 2021-2025 ICANN Strategic Plan[3] and its goals and objectives. The report specifies the relevant objectives that the individual recommendations support; the SSR2 RT 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 high priority.

#	Recommendation	Owner	Priority
1	**Complete the implementation of all relevant SSR1 recommendations**		High
2	**SSR1 Recommendation 9 - Information Security Management Systems and Security Certifications** 2.1. ICANN org should establish a road map of its industry-standard security audits and certification activities that are being undertaken, including milestone dates for obtaining each certification and noting areas of continuous improvement.		High

[3] "ICANN Strategic Plan for Fiscal Years 2021 – 2025," ICANN, last updated 29 March 2019, https://www.icann.org/public-comments/strategic-plan-2018-12-20-en.

	2.2. 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. 2.3. ICANN org should also provide reasoning for their choices, demonstrating how they fit into its security and risk management strategies 2.4. ICANN org should implement an Information Security Management System and undergo a third-party audit. 2.5. In order to reap the benefits of a certification and audit regimen, ICANN org should be audited and certified by a third party along the lines of industry security standards and should assess certification options with commonly accepted international standards (e.g., ITIL, ISO 27001, SSAE-18) for its operational responsibilities.		
3	**SSR1 Recommendations 12,15, and 16 - SSR Strategy and Framework, Metrics, and Vulnerability Disclosures** 3.1. ICANN org should address security issues clearly, publicly (with consideration for operational security, e.g., after an established moratorium and anonymization of the information, if required), and promote security best practices across all contracted parties. 3.2. ICANN org should also capture SSR-related best practices in a consensus document, establish clear, measurable, and trackable objectives, and then implement the practices in contracts, agreements, and MOUs. 3.3. ICANN org should implement coordinated vulnerability disclosure reporting. Disclosures and information regarding SSR-related issues should be communicated promptly to trusted, relevant parties (e.g., those affected or required to fix the given issue), such as in cases of breaches at any contracted party and in cases of key vulnerabilities discovered and reported to ICANN org. 3.4. ICANN org should establish a clear communication plan for reports to the community and produce regular (at least annual) and timely reports containing anonymous metrics of the vulnerability disclosure process. These communiques should contain responsible disclosure as defined by the community-agreed process and include anonymized metrics.		High
4	**SSR1 Recommendation 20 and 22 - Budget Transparency and Budgeting SSR in new gTLDs** 4.1. Where possible (contractually) and reasonable in terms of effort (i.e., over 10% of the activity described in the budget line item), ICANN should be more transparent with the budget for parts of ICANN org related to implementing the Identifier Systems Security, Stability, and Resiliency (IS-SSR) Framework and performing SSR-related functions, including those associated with the introduction of new gTLDs.		Medium
5	**SSR1 Recommendation 27 - Risk Management**		High

	5.1. ICANN's Risk Management Framework should be centralized and strategically coordinated. 5.2. ICANN org should clearly articulate their risk framework and strategically align the framework against the requirements and objectives of the organization, describing relevant measures of success and how ICANN org will assess these measures. 5.3. ICANN should make information pertaining to risk management centrally available to the community. This information should be regularly updated to reflect the current threat landscape (at least annually).		
6	**Create a Position Responsible for Both Strategic and Tactical Security and Risk Management** 6.1. ICANN org should create a position responsible for both strategic and tactical security and risk management across the internal security domain of the organization, as well as the external global identifier system. 6.2. ICANN org should hire an appropriately qualified individual for that position and allocate a specific budget sufficient to execute this role's functions. 6.3. This position should manage ICANN org's Security Function and oversee the interactions of staff in all relevant areas that impact security. 6.4. The position should also provide regular reports to ICANN's Board and community. 6.5. This position would act as a pathfinder and problem-solver who would strategize and execute multi-faceted programs to achieve substantial improvements. 6.6. Additionally, this role should take part in all security-relevant contractual negotiations (e.g., supply chains for hardware and software and associated service level agreements) undertaken by ICANN org, signing off on all security-related contractual terms.		High
7	**Further Develop a Security Risk Management Framework** 7.1. ICANN org should clearly articulate their Security Risk Management Framework and ensure that it aligns strategically against the requirements and objectives of the organization. 7.2. ICANN org should describe relevant measures of success and how these measures are to be assessed. The SSR2 RT described the foundation of this in detail in the additional feedback regarding SSR1's Recommendation 9 (see 'SSR1 Recommendation 9 - Information Security Management Systems and Security Certifications' earlier in this report). 7.3. ICANN org should: 7.3.1. Adopt and implement ISO 31000 "Risk Management" and validate and certify their implementation with appropriate		High

	independent audits.[4] Risk management efforts should feed into Business Continuity and Disaster Recovery Plans and Provisions. 7.3.2. Regularly update a register of security risks and use that register to prioritize and guide the activities of the ICANN org. ICANN org should report on updates of their methodology and updates to the register of security risks. Findings should feed into BC/DR and the Information Security Management System (ISMS). 7.3.3. Name or appoint a dedicated, responsible person in charge of security risk management that will report to the C-Suite Security role as described in the recommendation "C-Suite Security Position."		
8	**Establish a Business Continuity Plan Based on ISO 22301** 8.1. ICANN org should establish a Business Continuity Plan for all the systems owned by, or under the purview of ICANN org, based on ISO 22301 "Business Continuity Management."[5] 8.2. ICANN should identify the importance of functional, acceptable timelines for BC and DR based on the urgency of restoring full functionality. 8.3. For Public Technical Identifiers (PTI) operations (IANA functions, including all relevant systems that contribute to the Security and Stability of the DNS and also Root Zone Management), ICANN org should develop a shared approach to service continuity in close cooperation with the Root Server System Advisory Committee (RSSAC) and the root server operators. 8.4. ICANN org should publish evidence (e.g., a summary) of their Business Continuity Plans and Provisions. An external auditor should be engaged to verify compliance aspects of the implementation of the resulting business continuity plans.		High
9	**Ensure the Disaster Recovery Plan is Appropriate, Functional, and Well Documented** 9.1. ICANN org should ensure that the DR plan for PTI operations (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 *Guidelines for information and communication technology readiness for business continuity.* ICANN org should develop this plan in close cooperation with RSSAC and the root server operators. 9.2. ICANN org should also establish a DR Plan for all the systems owned by or under the purview of ICANN org, again in line with		High

[4] International Standards Organization, "ISO 31000 Risk Management," https://www.iso.org/iso-31000-risk-management.html.

[5] "ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements," https://www.iso.org/standard/75106.html.

	ISO 27031 *Guidelines for information and communication technology readiness for business continuity.* 9.3. ICANN org should have a disaster recovery plan developed within twelve months of the ICANN Board's adoption of these recommendations around establishing at least a third site for disaster recovery (in addition to Los Angeles and Culpepper), specifically outside of the United States and its territories and the North American region, including a plan for implementation. 9.4. ICANN org should publish a summary of their overall disaster recovery plans and provisions. ICANN org should engage an external auditor engaged to verify compliance aspects of the implementation of these DR plans.		
10	**Improve the Framework to Define and Measure Registrar & Registry Compliance** 10.1. Establish a performance metrics framework to guide the level of compliance by Registrars and Registries for WHOIS obligations (including inaccuracy), as well as other elements that affect abuse, security, and resilience, as outlined in the RDS/WHOIS2 Review and the CCT Review.[6,7] 10.2. Allocate a specific budget line item for a team of compliance officers tasked with actively undertaking or commissioning the work of performance management tests/assessments of agreed SLA metrics. 10.3. Amend the SLA renewal clause from 'automatically renewed' to a cyclical four-year renewal that includes a review clause included (this review period would consider the level of compliance to the performance metrics by the Registrar and Registry and recommend the inclusion of requirements to strengthen the security and resilience where non-compliance was evident). 10.4. Further, the ICANN Board should take responsibility for bringing the EPDP[8] to closure and passing and implementing a WHOIS policy in the year after this report is published.		High
11	**Lead Efforts to Evolve Definitions Around Abuse and Enable Reporting Against Those Definitions** 11.1. ICANN Board should drive efforts that minimize ambiguous language and reach a universally acceptable agreement on abuse, SSR, and security threats in its contracts with contracted parties and implementation plans.		High

[6] ICANN RDS-WHOIS 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.

[7] "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.

[8] ICANN Generic Names Supporting Organization, "GNSO Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Policy Recommendations for ICANN Board Consideration," 1 May 2019, https://www.icann.org/public-comments/epdp-recs-2019-03-04-en.

	11.2. ICANN org and Board should implement the SSR-relevant commitments (along with CCT and RDS/WHOIS2 Review recommendations) based on current, community vetted abuse definitions, without delay[9]. 11.3. ICANN Board, in parallel, should encourage community attention to evolving the DNS abuse definition (and application), and adopt the additional term and evolving external definition of "security threat"—a term used by the ICANN Domain Abuse Activity Reporting (DAAR) project, and the GAC (in its Beijing Communique[10] and for Specification 11[11]), and addressed in international conventions such as the Convention on Cybercrime and its related "Explanatory Notes" [12] —to use in conjunction with ICANN org's DNS Abuse definition.[13] 11.4. The ICANN Board should entrust SSAC and PSWG to work with e-crime and abuse experts to evolve the definition of DNS Abuse, taking into account the processes and definitions outlined in the Convention on Cybercrime.		
12	**Create Legal and Appropriate Access Mechanisms to WHOIS Data** 12.1. The ICANN Board should create a legal and appropriate access mechanisms to WHOIS data by vetted parties such as law enforcement. 12.2. The ICANN Board should take responsibility for, and ensure ICANN org comes to immediate closure on, implementation of the Temporary Specification for gTLD Registration Data.		High
13	**Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program** 13.1. The ICANN Board and ICANN org should work with the entities inside and outside the ICANN community that are mitigating abuse to improve the completeness and utility of DAAR, in order to improve both measurement and reporting of domain abuse.		High

[9] The CCT report itself defines both DNS Abuse and DNS Security Abuse, citing with approval at p 8, fn 11 definitions contained in an ICANN Staff document called "Safeguards against DNS Abuse 18 June 2016". The community Registration Abuse Policies Working Group (RAP) in 2010 'developed a consensus definition of abuse' which reads: "Abuse is 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." (This definition is cited with approval on page 88, footnote 287 of the CCT final report)

[10] ICANN Governmental Advisory Committee, "GAC Advice: ICANN46 Beijing Communique," last modified 11 April 2013, https://gac.icann.org/contentMigrated/icann46-beijing-communique.

[11] ICANN, "Registry Agreement," https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm.

[12] Council of Europe, "Convention on Cybercrime," ETS No. 185, p. 7, 23 November 2001, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[13] See note 50

	13.1.1. ICANN org should publish DAAR reports that identify registries and registrars whose domains most contribute to abuse according to the DAAR methodology. 13.1.2. ICANN org should make the source data for DAAR available through the ICANN Open Data Initiative and prioritize items *“daar”* and “*daar-summarized*” of the ODI Data Asset Inventory[14] for immediate community access. 13.1.3. ICANN org should publish reports that include machine-readable formats of the data, in addition to the graphical data in current reports. 13.1.4. ICANN org should provide assistance to the Board and all constituencies, stakeholder groups and advisory committees in DAAR Interpretation, including assistance in the identification of policy and advisory activities that would enhance domain name abuse prevention and mitigation.		
14	**Enable Rigorous Quantitative Analysis of the Relationship Between Payments for Domain Registrations and Evidence of Security Threats and Abuse** 14.1. ICANN org should collect, analyze, and publish pricing data to enable further independent studies and tracking of the relationship between pricing and abuse.		High
15	**Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse** 15.1. ICANN org should, make SSR requirements mandatory on contract or baseline agreement renewal in agreements with contracted parties, including Registry Agreements (base and individual) and the RAA, These contract requirements should include provisions that establish thresholds of abuse (e.g., 3% of all registrations) that would automatically trigger compliance inquiries, with a higher threshold (e.g., 10% of all registrations) at which ICANN org considers registrars and registries to be in default of their agreements. The CCT Review also recommended this approach.[15] 15.2. ICANN org should introduce a contract clause that would support contract termination in the case of “a pattern and practice” of abuse (as in section 5.5.2.4 “TERM, TERMINATION AND DISPUTE RESOLUTION” of the 2013 Registrar Accreditation Agreement)[16]. 15.3. In order to support the review of these contract changes, ICANN org should:		

[14] See: https://www.icann.org/en/system/files/files/odi-data-asset-inventory-spreadsheet-11jun18-en.csv as published by the Office of the CTO, available here: https://www.icann.org/public-comments/odi-datasets-metadata-2018-06-11-en.

[15] See recommendations 14, 15, and 16 in the “Competition, Consumer Trust, and Consumer Choice: Final Report,” https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf.

[16] “2013 Registrar Accreditation Agreement,” ICANN, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en.

	15.3.1. Ensure access to registration data for parties with legitimate purposes via contractual obligations and with rigorous compliance mechanisms. 15.3.2. Establish and enforce uniform Centralized Zone Data Service requirements to ensure continuous access for SSR research purposes. 15.3.3. Attract and collaborate with ccTLDs and the ccNSO to help address DNS abuse and security threats in ccTLDs. 15.3.4. The ICANN Board, community, and org should work with the ccNSO to advance data tracking and reporting, assess DNS abuse and security threats in ccTLDs, and develop a ccNSO plan to support ccTLDs in further mitigating DNS abuse and security threats. 15.3.5. Immediately instantiate a requirement for the RDAP services of contracted parties to white-list ICANN org address space and establish a process for vetting other entities that RDAP services of contracted parties will whitelist for non-rate-limited access. 15.4. In the longer term, ICANN Board should request that the GNSO initiate the process to adopt new policies and agreements with Contracted Parties that measurably improve mitigation of DNS abuse and security threats, including changes to RDAP and registrant information, incentives for contracted parties for abuse/security threat mitigation, establishment of a performance metrics framework, and institutionalize training and certifications for contracted parties and key stakeholders.		
16	**Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats** 16.1. ICANN org should incentivize the mitigation of abuse and security threats making the following changes to contracts: 16.1.1. Contracted parties with portfolios with less than a specific percentage (e.g., 1%) of abusive domain names (as identified by commercial providers or DAAR) should receive a fee reduction (e.g., a reduction from current fees, or an increase of the current per domain name transaction fee and provide a Registrar with a discount). 16.1.2. Registrars should receive a fee reduction for each domain name registered to a verified registrant up to an appropriate threshold. 16.1.3. Waive RSEP fees when the RSEP filings clearly indicate how the contracted party intends to mitigate DNS abuse, and that any Registry RSEP receives pre-approval if it permits an EPP field at the Registry level to designate those domain names as under management of a verified Registrant. 16.1.4. Refund fees collected from registrars and registries on domains that are identified as abuse and security threats and are taken down within an appropriate period after registration (e.g., 30 days after the domain is registered). 16.2. Given all parties (ICANN org, contracted parties, and other critical stakeholders such as Registries, Registrars, Privacy/Proxy Service Providers, Internet Service Providers,		High

	and the contracted parties) must understand how to accurately measure, track, detect, and identify DNS abuse, ICANN org should institutionalize training and certifications all parties in areas identified by DAAR and other sources on the common methods of abuse **[citation to be added]** and how to establish appropriate mitigation efforts. Training should include as a starting point: Automatic tracking of complaint numbers and treatment of complaints; Quarterly/Yearly public reports on complaints and actions; and analysis.		
17	**Establish a Central Abuse Report Portal** 17.1. 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 inflow, with only summary and metadata flowing upstream. Use of the system should be mandatory for all gTLDs; ccTLDs should be invited to join. Responses must be publicly searchable and included in yearly reports (in complete form, or by reference). In addition, reports should be made available (e.g., via email) to non-participating ccTLDs.		High
18	**Ensure that the ICANN Compliance Activities are Neutral and Effective** 18.1. ICANN org should have compliance activities audited externally and hold them to a high standard. 18.2. The ICANN Board should empower the Compliance Office to react to complaints and require Compliance to initiate investigations and enforce contractual obligations against those aiding and abetting systemic abuse, as defined by the SLA. This additional authority could include support for step by step actions around the escalation of enforcement measures and appropriate implementable actions that ICANN org can use in response to any failures to remedy compliance violations within specified timeframes. 18.3. The ICANN Compliance Office should, as their default, involve SLAs on enforcement and reporting, clear and efficient processes, a fully informed complainant, measurable satisfaction, and maximum public disclosure.		High
19	**Update Handling of Abusive Naming** 19.1. ICANN org should build upon the current activities to investigate typical misleading naming, in cooperation with researchers and stakeholders, wherever applicable. 19.2. When misleading naming rises to the level of abusive naming, ICANN org should include this type of abuse in their DAAR reporting and develop policies and mitigation best practices. 19.3. ICANN org should publish the number of abusive naming complaints made at the portal in a form that allows independent		High

	third parties to analyze, mitigate, and prevent harm from the use of such domain names. 19.4. ICANN org should update the current "Guidelines for the Implementation of IDNs" **[citation to be added]** to include a section on names containing trademarks, TLD-chaining, and the use of (hard-to-spot) typos. Furthermore, ICANN should contractually enforce "Guidelines for the Implementation of IDNs" for gTLDS and recommend that ccTLDs do the same.		
20	**Complete Development of a DNS Regression Testing** 20.1. ICANN org should complete the development of a suite for DNS regression testing.[17] 20.2. ICANN org should ensure that the capability to perform functional testing of different configurations and software versions is implemented and maintained.		High
21	**Implement the Recommendations from SAC063 and SAC073 and Establish Formal Procedures for Key Rollovers** 21.1. ICANN org should implement the recommendations from SAC063 and SAC073 in order to ensure the SSR of the KSK rollover process. 21.2. ICANN org should establish a formal procedure, supported by a formal process modeling tool and language[18] 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, FSM) for public comment, and community feedback should be incorporated. 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 lessons learned can be used to adjust the process. 21.3. 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.		High
22	**Establish Baseline Security Practices for Root Server Operators and Operations** 22.1. ICANN org, in close cooperation with RSSAC and other relevant stakeholders, should ensure that the RSS governance		High

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

[18] 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)

	model as proposed by RSSAC037 includes baseline security best practices for root server operators and operations in order to minimize the SSR risks associated with root server operation. These best practices should include change management, verification procedures, and sanity check procedures. 22.2. ICANN org should also develop relevant KPIs to measure the implementation of these best practices and requirements and ensure yearly public reporting on how Root Server Operators (RSOs) and other relevant parties, including ICANN org, can meet these KPIs. 22.3. ICANN org should document hardening strategies of the ICANN Managed Root Server (IMRS), commonly known as L-Root, and should encourage other RSOs to do the same. 22.4. ICANN org should ensure that the IMRS uses a vulnerability disclosure process (not necessarily public), security reports and intelligence, and communication with researchers and RSSAC advice or recommendations, where applicable.		
23	**Accelerate the Implementation of the New-Generation RZMS** 23.1. ICANN and PTI operations should accelerate the implementation of new RZMS security measures regarding the authentication and authorization of requested changes. 23.2. ICANN org should launch public comment as soon as possible on changes regarding revisions to the RZMS policies.		High
24	**Create a List of Statistics and Metrics Around the Operational Status of the Unique Identifier Systems** 24.1. ICANN org should create a list of statistics and metrics that reflect the operational status (such as availability and responsiveness) of each type of unique identifier information, such as root-zone related service, IANA registries, and any gTLD service that ICANN org has authoritative purview over. 24.2. ICANN org should publish a directory of these services, data sets, and metrics on a single page on the ICANN org web site, such as under the Open Data Platform. 24.3. ICANN should publish annual and longitudinal summaries of this data, solicit public feedback on the summaries, and incorporate the feedback to improve future reports. 24.4. For both sets of KPIs, ICANN org should produce summaries over both the previous year and longitudinally, request and publish a summary of community feedback on each report and incorporate this feedback to improve follow-on reports.		Medium
25	**Ensure the Centralized Zone File Data Access is Consistently Available** 25.1. The ICANN community and ICANN org should take steps to ensure that access to CZDS as well as other data is available,		High

	in a timely manner, and without unnecessary hurdles to requesters. 25.2. ICANN org should implement the four recommendations in SSAC 97:[19] *“Recommendation 1: The SSAC recommends that the ICANN Board suggest to ICANN Staff to consider revising the CZDS system to address the problem of subscriptions terminating automatically by default, for example by allowing subscriptions to automatically renew by default. This could include an option allowing a registry operator to depart from the default on a per-subscriber basis, thereby forcing the chosen subscriber to reapply at the end of the current term. The CZDS should continue to provide registry operators the ability to explicitly terminate a problematic subscriber’s access at any time.* *Recommendation 2: The SSAC recommends that the ICANN Board suggest to ICANN Staff to ensure that in subsequent rounds of new gTLDs, the CZDS subscription agreement conform to the changes executed as a result of implementing Recommendation 1.* *Recommendation 3: The SSAC recommends that the ICANN Board suggest to ICANN Staff to seek ways to reduce the number of zone file access complaints, and seek ways to resolve complaints in a timely fashion.* *Recommendation 4: The SSAC recommends that the ICANN Board suggest to ICANN Staff to ensure that zone file access and Web-based WHOIS query statistics are accurately and publicly reported, according to well-defined standards that can be uniformly complied with by all gTLD registry operators. The Zone File Access (ZFA) metric should be clarified as soon as practicable.*		
26	**Document, Improve, and Test the EBERO Processes** 26.1. ICANN org should publicly document the ERERO processes, including decision points, actions, and exceptions. The document should describe the dependencies for every decision, action, and exception. 26.2. Where possible, ICANN org should automate these processes and test them annually. 26.3. ICANN org should publicly conduct EBERO smoke-testing at predetermined intervals using a test plan coordinated with the		High

[19] 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.

	ICANN contracted parties in advance to ensure that all exception legs are exercised and publish the results. 26.4. ICANN org should improve the process by allowing the gTLD Data Escrow Agent to send the data escrow deposit directly to the EBERO provider.		
27	**Update the DPS and Build Consensus Around future DNSKEY Algorithm Rollovers** 27.1. PTI operations should update the DPS to facilitate the transition from one digital signature algorithm to another, including an anticipated transition from the RSA digital signature algorithm to ECDSA or to future post-quantum algorithms, which will create a more resilient DNS while providing the same or greater security. 27.2. As 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.		Medium
28	**Develop a Report on the Frequency of Measuring Name Collisions and Propose a Solution** 28.1. ICANN org should produce findings that characterize the nature and frequency of name collisions and resulting concerns. The ICANN community should implement a solution before the next round of gTLDs. 28.2. ICANN org should facilitate this process by initiating an independent study of name collisions through to its eventual completion and adopt or account for the implementation or non-adoption of any resulting recommendations. By “independent,” SSR2 RT means that ICANN org should ensure that the SSAC Name Collision Analysis Project (NCAP) work party research and report evaluation team’s results need to be vetted by parties that are free of any financial interest in TLD expansion. 28.3. ICANN org should enable community reporting on instances of name collision. These reports should allow appropriate handling of sensitive data and security threats and should be rolled into community reporting metrics.		Medium
29	**Focus on Privacy and SSR Measurements and Improving Policies Based on Those Measurements** 29.1. ICANN org should monitor and regularly report on the privacy impact of technologies like DoT (DNS over TLS) and DoH (DNS over HTTPS). 29.2. ICANN org’s consensus policies and agreements with registry operators and registrars should, therefore, have clauses to reflect compliance with these while ensuring that the DNS is		High

	not fragmented because of the need to maintain/implement minimum requirements governing the 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. 29.3. ICANN org should: 29.3.1. Create specialized units within the contract compliance function that focus on 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 evolving RDAP framework. 29.3.2. Monitor relevant and evolving privacy legislation (e.g., CCPA and legislation protecting personally identifiable information (PII)) and ensure that ICANN org's policies and procedures are aligned and in compliance with privacy requirements and the protection of personally identifiable information as required by relevant legislation and regulation.[20] 29.3.3. Develop and keep up to date a policy for the protection of personally identifiable information. The policy should be communicated to all persons involved in the processing of personally identifiable information. Technical and organizational measures to appropriately protect PII should be implemented. 29.3.4. Conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they, at a minimum, have procedures in place to address privacy breaches. 29.4. ICANN org's DPO should also be responsible for external DNS PII. The DPO should provide guidance to managers and stakeholders regarding responsibilities and procedures and monitor and report on relevant technical developments.		
30	**Stay Informed on Academic Research of SSR Issues and Use That Information to Inform Policy Debates** 30.1. 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 S&P, as well as the operational security conferences APWG, M3AAWG, and FIRST, and publish a report for the ICANN community summarizing implications of publications that are relevant to ICANN org or contracted party behavior. 30.1.1. These reports should include recommendations for actions, including changes to contracts with registries and registrars, that could mitigate, prevent, or remedy SSR harms to		Medium

[20] The Review Team is aware of the ICANN org Charter outlining approach to government engagement https://www.icann.org/en/system/files/files/proposed-org-engagement-govt-standards-charter-25feb19-en.pdf and the Legislative report (the Tracker) https://www.icann.org/legislative-report-2019. However we would like a more specific focus on privacy and data protection.

	consumers and infrastructure identified in the peer-reviewed literature. 30.1.2. These reports should also include recommendations for additional study to confirm peer-reviewed findings, a description of what data would be required to execute additional recommended studies, and how ICANN can offer to help broker access to such data, e.g., CZDS.		
31	**Clarify the SSR Implications of DNS-over-HTTP** 31.1. ICANN org should commission an independent investigation(s) into the SSR-related implications of DoH deployment trends, as well as implications for the future role of IANA in the Internet ecosystem. The intended outcome is to ensure that all stakeholders have the opportunity to understand the SSR-related implications of these developments, and the range of alternatives (or lack thereof) various stakeholders have to influence the future.		High

Guidance for Future SSR Review Teams - Takeaways

In order to allow more straightforward evaluations by future SSR review teams, the SSR2 RT will strive to phrase its own recommendations according to the SMART criteria: wherever possible, recommendations will be *specific, measurable, assignable, relevant, and trackable*. The SSR2 RT believes that clearer and action-oriented recommendations will simplify implementation, tracking, and the assessment process to be undertaken by the next SSR review. The SSR2 RT has included additional information on the process and methodology used by the SSR2 RT to fulfill their mandate in 'Appendix C: Process and Methodology.'

Workstream 1: Review of SSR1 Implementation and Impact

In 2012, the ICANN Board found *"that the 28 Recommendations in the [SSR1] Final Report are feasible and implementable,"*[21] and unanimously accepted and instructed staff to implement all 28 SSR1 recommendations[22]. One of the SSR2 RT'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."*

[21] "Regular Meeting of the ICANN Board of Directors," ICANN, last updated 18 October 2012, https://www.icann.org/resources/board-material/minutes-2012-10-18-en.

[22] "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.

The SSR2 RT performed this assessment from its inception until the end of 2018 (exclusive of the period of suspension by the ICANN Board of the team's work that occurred Oct. 2017 — June 2018). This preamble contextualizes the team's process and methodology. Appendix C - Process and Methodology outlines the assessment process, the types of evidence and data used, and finally, the methodology adopted in reaching a conclusion on the level of implementation of the recommendations. Each review is a learning opportunity, and the "takeaways" section describes our lessons learned. Most importantly, having assessed the SSR1 Recommendations, the SSR2 RT notes the importance and the necessity to provide recommendations that are metric-based with measurable performance indicators. This observation is underpinned by the need to ensure effective implementation and assessment of any of ICANN's review team's recommendations.

SSR1 Recommendations Overview

The SSR2 RT reviewed all 28 SSR1 recommendations and found that out of 28 recommendations, 27 remain relevant as of the publication of this report. The team considers no recommendation to be implemented in full, for the reasons as outlined in Appendix D: Findings Related to SSR1 Recommendations. Instead, the team found partial implementations of 26 SSR1 recommendations and found 2 to not be implemented. A summary of this information in Table 1.

Table 1: 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	N	Y	Y
Implemented	P	P	P	P	P	N	P	P	N	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
Work needed	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

Key: Y = Yes N = No P = Partial - = Not Applicable

While the detailed assessment of each of the SSR1 recommendations, as found in Appendix D: Findings Related to SSR1 Recommendations, speaks to the specific implementations, their issues, and the team's ideas for further work, the team notes 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. 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 also 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.

The SSR2 RT finds that ICANN org's implementation of the SSR1 recommendations is incomplete. The team notes that the open, untrackable nature of the SSR1 recommendations contributes to partial implementations, as noted in the preamble. The SSR2 RT also finds many areas for improvement when it comes to SSR matters in general, as described in the later sections of this report.

Assessment of SSR1 Recommendations

As noted in Process and Methodology for Review of the SSR1 Recommendations, the SSR2 team reviewed each of the original SSR1 Recommendations. To summarize the results from that review:

SSR2 Recommendation 1: The SSR2 RT strongly recommends that the ICANN Board and ICANN org complete the implementation of the SSR1 Recommendations.

The results in this report offer direction where the original guidance is not sufficiently measurable and provides additional recommendations below that expand upon the original SSR1 recommendations.

SSR2 Recommendation 2: SSR1 Recommendation 9 - Information Security Management Systems and Security Certifications

At the moment, it is unclear how ICANN org is approaching security certification and audit.

2.6. ICANN org should establish a road map of its industry-standard security audits and certification, including milestone dates for obtaining each certification and noting areas of continuous improvement.

2.7. 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.

2.8. ICANN org should also provide reasoning for their choices, demonstrating how they fit into its security and risk management strategies

2.9. ICANN org should implement an Information Security Management System and undergo a third-party audit.

2.10. In order to reap the benefits of a certification and audit regimen, ICANN org should be audited and certified by a third party along the lines of industry security standards (e.g., ITIL, ISO 27001, SSAE-18) for its operational responsibilities.

See Appendix D - SSR1 Recommendation 9 for more detail on the findings and conclusions made by the SSR2 RT against this recommendation.

SSR2 Recommendation 3: SSR1 Recommendations 12,15, and 16 - SSR Strategy and Framework, Metrics, and Vulnerability Disclosures

4.2. ICANN org should address security issues clearly, publicly (with consideration for operational security, e.g., after an established moratorium and anonymization of the information, if required), and promote security best practices across all contracted parties.

4.3. ICANN org should also capture SSR-related best practices in a consensus document, establish clear, measurable, and trackable objectives, and then implement the practices in contracts, agreements, and MOUs.

4.4. ICANN org should implement coordinated vulnerability disclosure reporting. Disclosures and information regarding SSR-related issues should be communicated promptly to trusted, relevant parties (e.g., those affected or required to fix the given issue), such as in cases of breaches at any contracted party and in cases of key vulnerabilities discovered and reported to ICANN org.

4.5. ICANN org should establish a clear communication plan for reports to the community and produce regular (at least annual) and timely reports containing anonymous metrics of the vulnerability disclosure process. These communiques should contain responsible disclosure as defined by the community-agreed process and include anonymized metrics.

Oversight for the disclosure process, including determining moratorium timing and public disclosure, should fall within the mandate of the C-Suite role as described in Workstream 2 - C-Suite Security Position.

See Appendix D - SSR1 Recommendation 12, SSR1 Recommendation 15, and SSR1 Recommendation 16 for more detail on the findings and conclusions made by the SSR2 RT against these recommendations.

SSR2 Recommendation 4: SSR1 Recommendations 20 and 22 - Budget Transparency and Budgeting SSR in new gTLDs

While SSR-related activities may be covered under various items within ICANN's annual budget, it is not clear how ICANN org allocates funds to specific SSR-related functions.

4.1. Where possible (contractually) and reasonable in terms of effort (i.e., over 10% of the activity described in the budget line item), ICANN should be more transparent with the budget for parts of ICANN org related to implementing the Identifier Systems Security, Stability, and Resiliency (IS-SSR) Framework and performing SSR-related functions, including those associated with the introduction of new gTLDs.

Various ICANN org departments have insufficient resources to address SSR concerns. SSR1 Recommendation 20 intends a greater degree of granularity for examination and public comment of SSR-related budget items as well as regular review, which is currently impossible.

See Appendix D - SSR1 Recommendation 20 and SSR1 Recommendation 22 for more detail on the findings and conclusions made by the SSR2 RT against these recommendations.

SSR2 Recommendation 5: SSR1 Recommendation 27 - Risk Management

5.4. ICANN's Risk Management Framework should be centralized and strategically coordinated.

5.5. ICANN org should clearly articulate their risk framework and strategically align the framework against the requirements and objectives of the organization, describing relevant measures of success and how ICANN org will assess these measures.

5.6. ICANN should make information pertaining to risk management centrally available to the community. This information should be regularly updated to reflect the current threat landscape (at least annually).

Risk management activities, including the DNS Risk Framework Working Group's report[23] and the 2016 Identifier Systems Security, Stability and Resiliency Framework for FY15-16,[24] as assessed by the team were comprehensive and appropriate.

See Appendix D - SSR1 Recommendation 27 for more detail on the findings and conclusions made by the SSR2 RT against these recommendations.

Workstream 2: Key Stability Issues within ICANN

This workstream relates to Bylaw 4.6(c) (ii) A, 4.6(c) (ii) B as well as 4.6(c) (iii) and focused on three key areas: 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; and 3. completeness and effectiveness of ICANN's internal security processes and the effectiveness of the ICANN security framework.

C-Suite Security Position

Rationale and Findings

[23] "DNS Risk Management Framework Report," DNS Risk Management Framework Working Group, last modified 4 October 2013,

[24] "Identifier Systems Security, Stability, and Resiliency Framework – FY 15-16," https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf.

Currently, SSR concerns are split across the ICANN organization. The SSR2 RT 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*
>
> 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'*

as well as securing, monitoring and managing data-assets, such as private data from the community of contracted parties, that are entrusted to ICANN org for safe-keeping.

However, having the roles related to SSR decentralized under two separate units within ICANN org is unlikely to be effective given the need for a close correlation between an executive-suite role that sets strategic objectives, regulatory compliance, and budgeting and the responsibility of securing the organization's assets. Due to the importance of proper management of these managerial tasks, this recommendation is also informed by several other SSR2 Recommendations, in particular:

This recommendation is also informed by several other SSR2 Recommendations, in particular:

- SSR1 Recommendations 12,15, and 16 - SSR Strategy and Framework, Metrics, and Vulnerability Disclosures
- SSR2 Recommendation 7: Further Develop a Security Risk Management Framework
- SSR2 Recommendation 15: Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse

The SSR2 RT found that security risk management is an integral part of ICANN org's mission, but this area has not received the specific and intentional attention, investment, or commitment it requires to be effective. Responsibilities related to the coordination and budgeting needed to implement security-related requirements in ICANN's Bylaws and commitments in ICANN's Strategic Plan should fall under the purview of an Executive Level C-Suite to ensure that there is a strategic alignment for all related activities.

SSR2 Recommendation 6: Create a Position Responsible for Both Strategic and Tactical Security and Risk Management

The SSR2 RT considers it necessary 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.[25]

6.1. ICANN org should create a position responsible for both strategic and tactical security and risk management across the internal security domain of the organization, as well as the external global identifier system.

6.2. ICANN org should hire an appropriately qualified individual for that position and allocate a specific budget sufficient to execute this role's functions.

6.3. This position should manage ICANN org's Security Function and oversee the interactions of staff in all relevant areas that impact security.

6.4. The position should also provide regular reports to ICANN's Board and community.

6.5. This position would act as a pathfinder and problem-solver who would strategize and execute multi-faceted programs to achieve substantial improvements.

6.6. Additionally, this role should take part in all security-relevant contractual negotiations (e.g., supply chains for hardware and software and associated service level agreements) undertaken by ICANN org, signing off on all security-related contractual terms.

This position would fulfill the responsibilities at the Executive C-Suite level of a Chief Security Officer (CSO) and Chief Information Security Officer (CISO).

Security Risk Management

Rationale and Findings

Security risk management is an ongoing process to help an organization in identifying security risks and implementing strategies to mitigate the identified security risks. To better understand the approaches and frameworks that have been adopted by ICANN org to handle security risks of the unique identifier systems managed by ICANN org, the team revisited implementation documents for the SSR1 recommendations. The SSR2 RT held conference calls with ICANN org staff and units responsible with security, stability, and resiliency of the DNS and also scheduled a face to face meeting at ICANN Office, Los Angeles, CA, with several ICANN org staff subject matter experts to discuss a range of issues relating to the completeness and effectiveness of SSR processes and the effectiveness of the ICANN org security framework.[26]

SSR2 RT used its stakeholder engagement meetings, structured interview, and focus group discussion to collect feedback from ICANN stakeholders on the current approaches and

[25] 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.

[26] "ICANN SSR - Meeting #4 - 09 -10 October 2017 - (F2F in Los Angeles, CA)," last modified 13 November 2017, https://community.icann.org/pages/viewpage.action?pageId=69277737.

strategies that are currently under use by ICANN to handle risks related to the management of SSR. The SSR2 RT determined from this data that more work needs to be done by ICANN org to improve the approaches and frameworks currently in use the organization to handle the security risks to the unique identifier systems managed by ICANN org.

SSR2 Recommendation 7: Further Develop a Security Risk Management Framework

7.4. ICANN org should clearly articulate their Security Risk Management Framework and ensure that it aligns strategically against the requirements and objectives of the organization.

7.5. ICANN org should describe relevant measures of success and how these measures are to be assessed. The SSR2 RT described the foundation of this in detail in the additional feedback regarding SSR1's Recommendation 9 (see 'SSR1 Recommendation 9 - Information Security Management Systems and Security Certifications' earlier in this report).

7.6. ICANN org should:

7.6.1. Adopt and implement ISO 31000 "Risk Management" and validate and certify their implementation with appropriate independent audits.[27] Risk management efforts should feed into Business Continuity and Disaster Recovery Plans and Provisions.

7.6.2. Regularly update a register of security risks and use that register to prioritize and guide the activities of the ICANN org. ICANN org should report on updates of their methodology and updates to the register of security risks. Findings should feed into BC/DR and the Information Security Management System (ISMS).

7.6.3. Name or appoint a dedicated, responsible person in charge of security risk management that will report to the C-Suite Security role as described in the recommendation "C-Suite Security Position."

Business Continuity Management and Disaster Recovery Planning

Rationale and Findings

ICANN org has a variety of functions that are important to the health of the Domain Name System (DNS), as well as the functionality of the Internet and information technologies more generally. These urgently needed functions include the IANA registries and their administration (this includes the management and maintenance of critical registries like the root zone, IP and AS numbers, and protocol registries). Beyond managing these crucial resources, ICANN org also provides other functions, including the coordination of technical and organizational relations. Most importantly, the impact of IANA registries becoming unavailable or losing integrity would lead to negative consequences all over the world.

[27] International Standards Organization, "ISO 31000 Risk Management," https://www.iso.org/iso-31000-risk-management.html.

The SSR2 team believes that ICANN org needs to engage in well planned, executed, and documented Business Continuity Management as well as Disaster Recovery Planning. Based on a similarly rigorous and documented analysis of risks (Reference findings and recommendation), ICANN org needs to identify the services it provides, and determine how it would address Business Continuity (BC) and Disaster Recovery (DR) for the essential functions it provides. These analyses and plans would benefit from being written down and accessible so that future review teams, as well as auditors, can review them. Providing access and third-party audit reports would improve transparency and trustworthiness beyond addressing ICANN's strategic goals and objectives.

The SSR2 RT emphasizes that well-maintained standards are crucial to this process. In particular, ISO 31000 "Risk Management,"[28] the ISO/IEC 27000 family "Information Security Management Systems,"[29] and ISO 22301 "Business Continuity Management"[30] would be useful as guidance and, more importantly, serve as target standards for third-party, independent audits. While ICANN org is somewhat particular in its organizational structure and mission, ISO standards are flexible and applicable to ICANN, particularly when it comes to ICANN org and the IANA function.

The SSR2 RT's analysis and experience during the assessment of the SSR1 Recommendations underline that clear documentation and independent audits are necessary to ensure that BC and DR plans are appropriate, functional, and well documented. During the team's research, it was often impossible for team members and also staff members to find and present sufficiently detailed documentation that would allow for a proper assessment of ICANN org's provisions. Considering that ICANN has a public profile and global mission, the use of external expert auditors, as well as providing more detailed and well-maintained documentation to future reviews, would contribute to transparency and legitimacy beyond improving BC and DR provisions. Therefore, ICANN org would benefit from making public the tender for auditors as well as their (if necessary, redacted) reports.

SSR2 Recommendation 8: Establish a Business Continuity Plan Based on ISO 22301

8.5. ICANN org should establish a Business Continuity Plan for all the systems owned by, or under the purview of ICANN org, based on ISO 22301 "Business Continuity Management."[31]

8.6. ICANN should identify the importance of functional, acceptable timelines for BC and DR based on the urgency of restoring full functionality.

[28] "ISO 31000 Risk Management," https://www.iso.org/iso-31000-risk-management.html.

[29] International Standards Organization, ISO/IEC 27000 standard suite, https://www.iso.org/search.html?q=27000&hPP=10&idx=all_en&p=0&hFR%5Bcategory%5D%5B0%5D=standard.

[30] International Standards Organization, "ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements," October 2019, https://www.iso.org/standard/75106.html.

[31] "ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements," https://www.iso.org/standard/75106.html.

8.7. For Public Technical Identifiers (PTI) operations (IANA functions, including all relevant systems that contribute to the Security and Stability of the DNS and also Root Zone Management), ICANN org should develop a shared approach to service continuity in close cooperation with the Root Server System Advisory Committee (RSSAC) and the root server operators.

8.8. ICANN org should publish evidence (e.g., a summary) of their Business Continuity Plans and Provisions. An external auditor should be engaged to verify compliance aspects of the implementation of the resulting business continuity plans.

SSR2 Recommendation 9: Ensure the Disaster Recovery Plan is Appropriate, Functional, and Well Documented

9.5. ICANN org should ensure that the DR plan for PTI operations (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 *Guidelines for information and communication technology readiness for business continuity.* ICANN org should develop this plan in close cooperation with RSSAC and the root server operators.

9.6. ICANN org should also establish a DR Plan for all the systems owned by or under the purview of ICANN org, again in line with ISO 27031 *Guidelines for information and communication technology readiness for business continuity.*

9.7. ICANN org should have a disaster recovery plan developed within twelve months of the ICANN Board's adoption of these recommendations around establishing at least a third site for disaster recovery (in addition to Los Angeles and Culpepper), specifically outside of the United States and its territories and the North American region, including a plan for implementation.

9.8. ICANN org should publish a summary of their overall disaster recovery plans and provisions. ICANN org should engage an external auditor engaged to verify compliance aspects of the implementation of these DR plans.

Workstream 3: Review of Security, Stability, and Resilience of the DNS System

This workstream relates to Bylaw 4.6(c) (ii) A, 4.6(c) (ii) B, 4.6(c) (ii) C, and 4.6(c) (iii) and focused on the effectiveness of ICANN org's stewardship over the areas of the Internet's globally unique identifier systems over which ICANN org has purview. The evaluation of this effectiveness necessarily considers performance indicators, measures, and metrics that span administrative domains and operations that include (but are not limited to) ICANN org. However, the focus of this work relates only to those systems within ICANN org's remit.

Abuse and Compliance

Rationale and Findings

Since its founding, ICANN org has had a remit to help ensure the security, stability, and resiliency of the Internet's unique identifier systems. While there is a strong record of ICANN org's policies and actions supporting competition and growth in the domain space, ICANN org's record regarding their support of impactful SSR measures appears insufficient when considered against the criticality of the systems in question.

Globally, there has been an increased risk of attacks against critical infrastructures, malicious political interference, and a range of cybercrimes. Any deficiency by ICANN org in fulfilling its responsibilities relating to the security, stability, and resiliency of the DNS runs the risk of malicious actors capitalizing on this failure and disrupting the Internet as a whole. Damages associated with cybercrime globally are projected to cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. The *2019 Official Annual Cybercrime Report* notes that

> *"This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined."*[32]

The SSR2 RT identified a significant upward trend in examples of abusive behaviors that can leverage the DNS. According to the research available, cybercriminals and other threat actors capitalize on identifiable gaps in DNS security measures currently in place. These trends have been particularly noteworthy since the ICANN Board adopted SSR1 Recommendations in 2012; see Appendix F: Research Data on Reports of DNS Abuse Trends for additional supporting information.

In the review of ICANN org's activities, the SSR2 RT found that the publications, statements, and related actions by ICANN org have consistently understated or omitted the impact of systemic abuse of the DNS and its use as a platform for launching systematic attacks on individual and organizational systems worldwide. One aspect of fulfilling this obligation is to use the definitions for 'DNS Abuse' and 'DNS Security Abuse,' which ICANN org has had in place for a decade, **[citation to be added]** to take action now. The SSR2 RT noted that the question of defining DNS abuse is an ongoing, systemic challenge that impacts ICANN org's operations and interactions with Registrars.[33] Other Bylaw-mandated review teams have made similar recommendations.[34]

[32] "Cybersecurity Ventures Official Annual Cybercrime Report," Cybercrime Magazine, 7 December 2018, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

[33] ICANN Government Advisory Committee, "DNS Abuse Mitigation," Briefing during ICANN Policy Forum 65, 24-27 June 2019, https://gac.icann.org/briefing-materials/public/icann65-gac-briefing-05.1-dns-abuse-mitigation-v1-6jun19.pdf.

[34] See CCT Review (https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf) recommendations 6, 19, 20, 25, 2-8, 14, 15, 16, 18, 20, and RDS (WHOIS) Review (https://www.icann.org/zh/system/files/files/rds-whois2-review-03sep19-en.pdf) recommendations R4.1, R4.2, R5.1, R15.1, LE 1, SG1.

New gTLDs and the Limitations of Registrar and Registry Agreements

In anticipation of the expansion of the gTLD program in 2010, the ICANN community prepared a memorandum[35] describing measures to mitigate malicious conduct in the new TLD program. The published version of the memorandum included recommendations for vetting registry operators, but the implementation of background checks for criminal or malicious activity was limited. This memorandum also recommended that registries name and define registry-level abuse contacts and procedures, but to date, no uniform or formal procedures are available or enforced, which adversely impacts registry-level security threat mitigation. The memorandum further recommended the centralization of access to zone files, but ongoing problems accessing zone file data via ICANN's Centralized Zone Data Service (CZDS) continue to hamper security mitigations, investigations, and research.[36,37,38,39] Problems with CZDS access include: registries failing to approve and provide access to zone data for legitimate users, registries failing to renew access to zone data for legitimate users, and registries failing to provide daily zone file data.[40]

Law enforcement, governments, security communities, and commercial and user interest groups all argued for contractual obligations to mitigate abuse during the deliberations of the 2013 RAA.[41,42] The few measures that survived the closed negotiations between ICANN org staff and registrars were significantly weakened. The SSR2 RT found no evidence that ICANN Compliance has addressed the ongoing, systemic abuse in the new gTLD environment.[43,44,45,46]

[35] 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

[36] ICANN, “CZDS Centralized Zone Data Service,” accessed 20 January 2020, https://czds.icann.org/home.

[37] “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.

[38] ICANN Security and Stability Advisory Committee, "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.

[39] 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.

[40] See notes 21 through 24

[41] “2013 Registrar Accreditation Agreement,” ICANN, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en.

[42] Ah Kang, Jeong, Seong Hoon, Steven Ko, Kaili Ren, Aziz Mohaisen, “Transparency in the New gTLD Era: Evaluating the DNS Centralized Zone Data Service,” 2016, pp 54-59. https://doi.org/10.1109/HotWeb.2016.18.

[43] ICANN, "Statistical Analysis of DNS Abuse in gTLDs (SADAG) Report,” 13 October 2017, https://www.icann.org/public-comments/sadag-final-2017-08-09-en.

[44] “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.

[45] Independent Compliance Working Party letter to Mr. Hedlund at ICANN, 27 February 2018, https://www.icann.org/en/system/files/correspondence/vayra-to-hedlund-27feb18-en.pdf.

[46] Dave Piscatello and Dr. Colin Strutt, "Criminal Abuse of Domain Names: Bulk Registration and Contact Information Access,” Interisle Consulting Group, 17 October 2019, http://interisle.net/criminaldomainabuse.html.

Specific areas of the 2013 RAA that have not been implemented nor sufficiently specified as of the date of this report include:

- Contracts do not include any language or terms specifically addressing systemic abuse and obligations of registrars in this regard.
- ICANN org has not required the implementation of a cross-field validation requirement for a domain registration address data check, which has the potential to reduce fraudulent domain name registrations significantly. This cross-field validation requirement was to become effective six months after ICANN and a working group of registrar volunteers "*agreed that cross-field validation is technically and commercially feasible.*"[47]
- ICANN org has not implemented the requirements noted in the "Specification on Privacy and Proxy Registrations."[48] Among other elements, the accreditation program requirements are to include detailed frameworks for provider responses to requests from law enforcement authorities and intellectual property holders.

ICANN org has asserted that it lacks both enforcement mechanisms to contend with systemic abuse. As stated by the head of ICANN Compliance, Jamie Hedlund, in an April 2018 correspondence to the SSR2 RT:

> "*There are potential limitations on the actions that ICANN org can take in addressing DNS infrastructure abuse. Neither the Registry Agreement (RA) nor the 2013 Registrar Accreditation Agreement (RAA) has enforceable provisions prohibiting or authorizing sanctions against systemic DNS infrastructure abuse. In addition, the RA and ICANN policies as currently defined do not authorize ICANN org to require registries to suspend or delete potentially abusive domain names. Similarly, the RAA does not authorize ICANN org to require registrars to suspend or delete potentially abusive domain names.*"

However, ICANN Compliance has not publicly requested specific changes to the RAA or RA, nor has it incorporated functionality to monitor service levels, penalties, or circumstances that warrant suspension of a registrar's or registry's privilege to process new registrations. Further, ICANN Compliance also has failed to leverage the work of reputable security experts in the community and implement measures to address abuse flagged by them.

The European Commission adopted the General Data Protection Regulation (GDPR) on 14 April 2016; it became enforceable beginning 25 May 2018, allowing over two years for organizations such as ICANN org to modify their practices to support a greater granularity of control over access to personal data. Unfortunately, ICANN org did not clarify the application of GDPR to the Internet's unique identifier system while the law was being developed and failed to

[47] ICANN, "2013 RAA Whois Accuracy Program Specification Review," 17 July 2015, https://www.icann.org/public-comments/2013-whois-accuracy-spec-review-2015-05-14-en.

[48] ICANN, "2013 Registrar Accreditation Agreement", Specification on Privacy and Proxy Registrations, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#privacy-proxy.

act in a timely manner to implement GDPR in a way that balances privacy with the security, stability, and resiliency of the internet.

The “Temporary Specification for gTLD Registration Data,”[49] which was adopted by the ICANN Board on 17 May 2018, denies global access to WHOIS for GDPR-allowed uses such as cybersecurity, e-crime, and consumer protection. Industry surveys, research data analyses, and input from numerous stakeholders have indicated that changes to WHOIS policy unnecessarily have created serious SSR impediments and threaten DNS security, stability, and resiliency. For example, a uniform method of access to non-public WHOIS data is not defined, even for law enforcement.

RDS Data, DNS Abuse, and Compliance

The Security Stability and Advisory Committee (SSAC) has published several reports documenting issues with the domain name registration process.[50] Those reports urged both ICANN org and registrars to improve WHOIS data validation, eliminate excessive WHOIS rate-limiting, reconsider wholesale redaction of WHOIS point of contact data, and to act when notified of domain abuse. The SSR2 RT was unable to find any data that ICANN org has implemented those recommendations. In 2012, for example, SSAC recommended that registrars adopt multi-factor authentication, but ICANN did not make it a contractual obligation. In 2019, hijackings of government and private domain accounts in 2019 could have been mitigated if registrars had made multi-factor authentication a contractual obligation, as suggested by SSAC.

The Government Advisory Committee (GAC) has also called for WHOIS validation, security checks, security threat reporting, and complaint handling,[51] as did several ICANN constituencies.[52],[53],[54]

While ICANN org has invested substantial resources in the Domain Abuse Activity Report (DAAR) Program, the SSR2 RT was unable to find any information through the DAAR Program that offered data on the association of security threats to registrars and registries. The SSRT RT found that neither the DAAR project nor the Specification 11 3b implementation provides sufficient information to satisfy the stated objectives of these activities. No registrar reporting is

[49] ICANN, “Temporary Specification for gTLD Registration Data,” accessed 20 January 2020, https://www.icann.org/resources/pages/gtld-registration-data-specs-en/#temp-spec.

[50] ICANN Security and Stability Advisory Committee, SSAC Documents: Reports by Number, https://www.icann.org/groups/ssac/documents.

[51] ICANN Government Advisory Committee, “GAC Statement on DNS Abuse,” 18 September 2019, https://gac.icann.org/contentMigrated/gac-statement-on-dns-abuse.

[52] ICANN Business Continuity, Positions & Statements, https://www.bizconst.org/positions-statements.

[53] ICANN Intellectual Property Constituency, “IPC Public Comments,” https://www.ipconstituency.org/public-comments.

[54] ICANN, "Executive Summaries: ALAC Policy Comments & Advice” last modified 10 January 2020, https://community.icann.org/pages/viewpage.action?pageId=102142603.

provided, in part, because rate limiting impedes the DAAR project's data collection project's data collection.

Currently, DAAR lacks critical indicators and data. A stated purpose of DAAR is to "*provide the ICANN community with a reliable, persistent, and reproducible set of data from which security threat (abuse) analyses could be performed.*"[55] Since January 2018, ICANN OCTO has been publishing a high-level monthly report based on analysis of DAAR data, but the current reports make it nearly impossible to draw conclusions about which registrars/registries are harboring significant abuse.

Identifying registries and registrars in the published DAAR reports would give the ICANN community visibility into which registrars harbor the majority of suspicious domains, data that could facilitate informed policymaking and add a measure of transparency and accountability to the domain name registration system that does not appear to exist today.

The recent report, "Criminal Abuse of Domain Names",[56] noted several registrars that have high concentrations of malicious domains and offer bulk registration services and very low registration pricing that attracts criminals or attackers. These findings also corroborate findings from ICANN org's "Statistical Analysis of DNS Abuse in gTLDs" (SADAG), commissioned and published by ICANN org in 2017.[57]

ICANN Compliance

ICANN org historically has stated in compliance and SSR2-related matters that it does not have the contractual tools necessary to enforce against registries and registrars. However, ICANN org has never stated what tools it needs or how its current, narrow interpretation of the RAA and RAs hamper its work.[58],[59] While this has been a subject of community concern for over a decade, particularly during the negotiations over the 2013 RAA[60],[61] , the closed-door

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

[56] Dave Piscitello and Dr. Colin Strutt, "Criminal Abuse of Domain Names: Bulk Registration and Contact Information Access," Interisle Consulting Group, 17 October 2019, http://interisle.net/criminaldomainabuse.html.

[57] ICANN, "Statistical Analysis of DNS Abuse in gTLDs (SADAG) Report," 13 October 2017, https://www.icann.org/public-comments/sadag-final-2017-08-09-en.

[58] ICANN SSR2 RT, "Briefing Materials," last modified 31 May 2019, https://community.icann.org/display/SSR/Briefing+Materials.

[59] Independent Compliance Working Party letter to Mr. Hedlund at ICANN, 27 February 2018, https://www.icann.org/en/system/files/correspondence/vayra-to-hedlund-27feb18-en.pdf.

[60] ICANN, "Negotiations Between ICANN and Registrars to Amend the Registrar Accreditation Agreement Concluded," last modified 1 October 2013, https://community.icann.org/display/RAA/Negotiations+Between+ICANN+and+Registrars+to+Amend+the+Registrar+Accreditation+Agreement+Concluded.

[61] ICANN, "Proposed Final 2013 RAA," 3 June 2013, https://www.icann.org/public-comments/proposed-raa-2013-04-22-en.

negotiations between ICANN org and contracted parties have not brought about the stronger contractual language necessary to aid enforcement.

ICANN org has been unable to address abuse mitigation effectively under the existing Compliance regime, notwithstanding the abuse detection and mitigation obligations that ICANN's contracts with registries and registrars place on them. Contracted parties have been unable to find a consensus process to adopt or implement AGB obligations or recommendations from the GAC or the SSAC (e.g., SAC 101). The GAC advice concerning Specification 11 of the 2013 Registry Agreement, for example, emphasized three key provisions[62]:

1. Registry-Registrar provisions to prohibit domains being misused for criminal activity and suspend as appropriate given applicable laws;
2. Registry operators to perform technical analysis of their gTLD space to protect domains from pharming, phishing, malware, and botnets; and
3. Registries to maintain records of analysis, actions taken from them and also provide them to ICANN upon request.

Accredited parties do not consistently implement consensus policies and resulting contracts regarding abuse. Compliance has few options to enforce the agreements and has not exercised those enforcement clauses that do exist, taking into account the community's interpretation of the contract clauses on available avenues for enforcement. Leveraging contracts between ICANN org and registrars and registries is important, in that it demonstrates a public commitment to desired outcomes and allows ICANN Compliance to enforce provisions on behalf of the community's interests. ICANN org historically has had a relatively "hands-off" approach to these contracts, as demonstrated by the unchanging nature of the 2013 RAA.

Historically, ICANN org has rewarded contracted parties with fee reductions to incentivize certain business practices (e.g., domain tasting[63]). The existing contract framework enables ICANN to impose such changes. Registry Operators who submit an RSEP that is deemed by ICANN org to raise potential security and stability concerns are subjected to an RSTEP panel and associated fees up to $100,000—effectively a tax on innovation. Waiving such fees could promote, instead of impede, innovation focused on minimizing DNS abuse.

Known problems with bad actors "hiding out" in certain TLDs continue to frustrate efforts to eliminate security threats from the DNS. ICANN org does not have a history of action or transparency in addressing this in specific TLDs. Transparent reporting of this behavior would help focus ICANN org's and the community's effort toward eradicating DNS security problems and help re-establish trust for that portion of the namespace.

[62] ICANN Government Advisory Committee, Annex 1 of "GAC Communiqué –Beijing, People's Republic of China," 11 April 2013, https://www.icann.org/en/system/files/correspondence/gac-to-board-18apr13-en.pdf.
[63] ICANN, "The End of Domain Tasting | Status Report on AGP Measures," 12 August 2009, https://www.icann.org/resources/pages/agp-status-report-2009-08-12-en.

Further, ICANN’s complaints process is confusing and lacks insightful or impactful data about abuse handling. The SSR2 Review agrees with the CCT Review findings and recommendations, including: 1) that “current data available from ICANN Compliance are insufficient to measure the enforcement of various contract provisions and the success of safeguards in mitigating downstream consequences to DNS expansion. Part of the problem is transparency, in part due to the lack of granularity of the data that are being collected,” and recommends several reforms of ICANN Compliance; and 2) there are several TLDs with a disproportionate level of DNS security abuse and enhancements to various enforcement mechanisms are needed, as well as more and better data on both competition and pricing, and on the impact of safeguards on consumer protection.

The SSR2 Review agrees with the RDS/WHOIS2 Review findings and recommendations, including: 1) the need for ICANN Compliance to proactively monitor and enforce registrar obligations with regard to RDS (WHOIS) data accuracy, understand inaccuracy issues, and mitigate them; 2) the need for ICANN Compliance to factor in studies such as the ARS to detect patterns of failure to validate and verify WHOIS data as required by the RAA, and take action on patterns that are detected; 3) the continuing need for the Accuracy Reporting System; 4) and the need for implementation of the PPSAI to ensures that the underlying registration data of domain name registrations using Privacy/Proxy providers affiliated with registrars shall be verified and validated,.

Since ICANN org derives most of its funding from registrars and registries, the SSR2 RT noted that there was a possibility of conflict of interest at an organizational level between ensuring compliance (and so negatively impacting sources of income) and improving the overall SSR of the DNS.

SSR2 Recommendation 10: Improve the Framework to Define and Measure Registrar & Registry Compliance

The SSR2 RT recommends that ICANN org update core policies, contracts, and practices that impact security threat mitigation and consumer using a data-driven approach.

Specifically, ICANN org should:

10.5. Establish a performance metrics framework to guide the level of compliance by Registrars and Registries for WHOIS obligations (including inaccuracy), as well as other elements that affect abuse, security, and resilience, as outlined in the RDS/WHOIS2 Review and the CCT Review.[64,65]

10.6. Allocate a specific budget line item for a team of compliance officers tasked with actively undertaking or commissioning the work of performance management tests/assessments of agreed SLA metrics.

[64] ICANN RDS-WHOIS 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.

[65] “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.

10.7. Amend the SLA renewal clause from 'automatically renewed' to a cyclical four-year renewal that includes a review clause included (this review period would consider the level of compliance to the performance metrics by the Registrar and Registry and recommend the inclusion of requirements to strengthen the security and resilience where non-compliance was evident).

10.8. Further, the ICANN Board should take responsibility for bringing the EPDP[66] to closure and passing and implementing a WHOIS policy in the year after this report is published.

SSR2 Recommendation 11: Lead Efforts to Evolve Definitions Around Abuse and Enable Reporting Against Those Definitions

11.5. ICANN Board should drive efforts that minimize ambiguous language and reach a universally acceptable agreement on abuse, SSR, and security threats in its contracts with contracted parties and implementation plans.

11.6. ICANN org and Board should implement the SSR-relevant commitments (along with CCT and RDS/WHOIS2 Review recommendations) based on current, community vetted abuse definitions, without delay[67].

11.7. ICANN Board, in parallel, should encourage community attention to evolving the DNS abuse definition (and application), and adopt the additional term and evolving external definition of "security threat"—a term used by the ICANN Domain Abuse Activity Reporting (DAAR) project, and the GAC (in its Beijing Communique[68] and for Specification 11[69]), and addressed in international conventions such as the Convention on Cybercrime and its related "Explanatory Notes" [70] —to use in conjunction with ICANN org's DNS Abuse definition.[71]

11.8. The ICANN Board should entrust SSAC and PSWG to work with e-crime and abuse experts to evolve the definition of DNS Abuse, taking into account the processes and definitions outlined in the Convention on Cybercrime.

[66] ICANN Generic Names Supporting Organization, "GNSO Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Policy Recommendations for ICANN Board Consideration," 1 May 2019, https://www.icann.org/public-comments/epdp-recs-2019-03-04-en.

[67] The CCT report itself defines both DNS Abuse and DNS Security Abuse, citing with approval at p 8, fn 11 definitions contained in an ICANN Staff document called "Safeguards against DNS Abuse 18 June 2016". The community Registration Abuse Policies Working Group (RAP) in 2010 'developed a consensus definition of abuse' which reads: "Abuse is 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." (This definition is cited with approval on page 88, footnote 287 of the CCT final report)

[68] ICANN Governmental Advisory Committee, "GAC Advice: ICANN46 Beijing Communique," last modified 11 April 2013, https://gac.icann.org/contentMigrated/icann46-beijing-communique.

[69] ICANN, "Registry Agreement," https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm.

[70] Council of Europe, "Convention on Cybercrime," ETS No. 185, p. 7, 23 November 2001, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[71] See note 50

SSR2 Recommendation 12: Create Legal and Appropriate Access Mechanisms to WHOIS Data

12.3. The ICANN Board should create a legal and appropriate access mechanisms to WHOIS data by vetted parties such as law enforcement.

12.4. The ICANN Board should take responsibility for, and ensure ICANN org comes to immediate closure on, implementation of the Temporary Specification for gTLD Registration Data.

SSR2 Recommendation 13: Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program

13.2. The ICANN Board and ICANN org should work with the entities inside and outside the ICANN community that are mitigating abuse to improve the completeness and utility of DAAR, in order to improve both measurement and reporting of domain abuse.

13.2.1. ICANN org should publish DAAR reports that identify registries and registrars whose domains most contribute to abuse according to the DAAR methodology.

13.2.2. ICANN org should make the source data for DAAR available through the ICANN Open Data Initiative and prioritize items *“daar”* and “*daar-summarized*” of the ODI Data Asset Inventory[72] for immediate community access.

13.2.3. ICANN org should publish reports that include machine-readable formats of the data, in addition to the graphical data in current reports.

13.2.4. ICANN org should provide assistance to the Board and all constituencies, stakeholder groups and advisory committees in DAAR Interpretation, including assistance in the identification of policy and advisory activities that would enhance domain name abuse prevention and mitigation.

13.3. ICANN Board should annually solicit and publish feedback from entities inside and outside the ICANN community that are mitigating abuse in order to help enhance ICANN org’s data on domain abuse activity.

SSR2 Recommendation 14: Enable Rigorous Quantitative Analysis of the Relationship Between Payments for Domain Registrations and Evidence of Security Threats and Abuse

14.2. ICANN org should collect, analyze, and publish pricing data to enable further independent studies and tracking of the relationship between pricing and abuse.

[72] See: https://www.icann.org/en/system/files/files/odi-data-asset-inventory-spreadsheet-11jun18-en.csv as published by the Office of the CTO, available here: https://www.icann.org/public-comments/odi-datasets-metadata-2018-06-11-en.

SSR2 Recommendation 15: Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse

15.5. ICANN org should, make SSR requirements mandatory on contract or baseline agreement renewal in agreements with contracted parties, including Registry Agreements (base and individual) and the RAA, These contract requirements should include provisions that establish thresholds of abuse (e.g., 3% of all registrations) that would automatically trigger compliance inquiries, with a higher threshold (e.g., 10% of all registrations) at which ICANN org considers registrars and registries to be in default of their agreements. The CCT Review also recommended this approach.[73]

15.6. ICANN org should introduce a contract clause that would support contract termination in the case of "a pattern and practice" of abuse (as in section 5.5.2.4 "TERM, TERMINATION AND DISPUTE RESOLUTION" of the 2013 Registrar Accreditation Agreement)[74].

15.7. In order to support the review of these contract changes, ICANN org should:

15.7.1. Ensure access to registration data for parties with legitimate purposes via contractual obligations and with rigorous compliance mechanisms.

15.7.2. Establish and enforce uniform Centralized Zone Data Service requirements to ensure continuous access for SSR research purposes.

15.7.3. Attract and collaborate with ccTLDs and the ccNSO to help address DNS abuse and security threats in ccTLDs.

15.7.4. The ICANN Board, community, and org should work with the ccNSO to advance data tracking and reporting, assess DNS abuse and security threats in ccTLDs, and develop a ccNSO plan to support ccTLDs in further mitigating DNS abuse and security threats.

15.7.5. Immediately instantiate a requirement for the RDAP services of contracted parties to white-list ICANN org address space and establish a process for vetting other entities that RDAP services of contracted parties will whitelist for non-rate-limited access.

15.8. In the longer term, ICANN Board should request that the GNSO initiate the process to adopt new policies and agreements with Contracted Parties that measurably improve mitigation of DNS abuse and security threats, including changes to RDAP and registrant information, incentives for contracted parties for abuse/security threat mitigation, establishment of a performance metrics framework, and institutionalize training and certifications for contracted parties and key stakeholders.

SSR2 Recommendation 16: Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats.

16.3. ICANN org should incentivize the mitigation of abuse and security threats making the following changes to contracts:

16.3.1. Contracted parties with portfolios with less than a specific percentage (e.g., 1%) of abusive domain names (as identified by commercial providers or DAAR) should receive a fee reduction (e.g., a reduction from current fees, or an increase of the current per domain name transaction fee and provide a Registrar with a discount).

16.3.2. Registrars should receive a fee reduction for each domain name registered to a verified registrant up to an appropriate threshold.

[73] See recommendations 14, 15, and 16 in the "Competition, Consumer Trust, and Consumer Choice: Final Report," https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf.

[74] "2013 Registrar Accreditation Agreement," ICANN, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en.

16.3.3. Waive RSEP fees when the RSEP filings clearly indicate how the contracted party intends to mitigate DNS abuse, and that any Registry RSEP receives pre-approval if it permits an EPP field at the Registry level to designate those domain names as under management of a verified Registrant.

16.3.4. Refund fees collected from registrars and registries on domains that are identified as abuse and security threats and are taken down within an appropriate period after registration (e.g., 30 days after the domain is registered).

16.4. Given all parties (ICANN org, contracted parties, and other critical stakeholders such as Registries, Registrars, Privacy/Proxy Service Providers, Internet Service Providers, and the contracted parties) must understand how to accurately measure, track, detect, and identify DNS abuse, ICANN org should institutionalize training and certifications all parties in areas identified by DAAR and other sources on the common methods of abuse **[citation to be added]** and how to establish appropriate mitigation efforts. Training should include as a starting point: Automatic tracking of complaint numbers and treatment of complaints; Quarterly/Yearly public reports on complaints and actions; and analysis.

SSR2 Recommendation 17: Establish a Central Abuse Report Portal

17.2. 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 inflow, with only summary and metadata flowing upstream. Use of the system should be mandatory for all gTLDs; ccTLDs should be invited to join. Responses must be publicly searchable and included in yearly reports (in complete form, or by reference). In addition, reports should be made available (e.g., via email) to non-participating ccTLDs.

SSR2 Recommendation 18: Ensure that the ICANN Compliance Activities are Neutral and Effective

18.4. ICANN org should have compliance activities audited externally and hold them to a high standard.

18.5. The ICANN Board should empower the Compliance Office to react to complaints and require Compliance to initiate investigations and enforce contractual obligations against those aiding and abetting systemic abuse, as defined by the SLA. This additional authority could include support for step by step actions around the escalation of enforcement measures and appropriate implementable actions that ICANN org can use in response to any failures to remedy compliance violations within specified timeframes.

18.6. The ICANN Compliance Office should, as their default, involve SLAs on enforcement and reporting, clear and efficient processes, a fully informed complainant, measurable satisfaction, and maximum public disclosure.

Abusive Naming

The SSR2 RT distinguishes between misleading and abusive naming. Misleading Naming would direct a reasonable user to resources they would not expect based on the name; for example, a name reasonably associable with entity A leads to a resource provided by entity B. Misleading names can be accidental or purposefully misleading. Misleading naming includes, but is not limited to, "visually indistinguishable" names (comprising all character sets supported by the DNS and IDN, Unicode & ASCII), TLD-chaining (e.g., google.com.to), names containing trademarks, and the use of (hard to spot) typos. Abusive naming involves the use of purposefully misleading names to direct users to websites that enable crime, such as phishing, malware distribution, child exploitation, intellectual property infringement, and fraud.

Rationale and Findings

This abuse of the DNS impacts on security across the board, as criminals prey on consumers but also large corporations. With cybercrime increasing in terms of instances as well as in terms of damage, abusive naming might also impact ICANN org's perceived legitimacy. The SSR2 RT notes that some forms of misleading naming, such as “visually indistinguishable” names[75], are hard to spot and that ICANN policy and actions need to be balanced and fair. For example, ‘gøgler’ is an official word in Danish, albeit its similarities to google (better example needed). At the same time, many abusive names can be spotted rather easily by registrars if they choose to use a combination of automated and manual review. The SSR2 RT believes that making the use of misleading naming harder contributes to improved security of the DNS, increased legitimacy for ICANN, and counteracts cybercrime.

The process might work as follows**:**

- The key parties to implement would be registrars, as they “see” name registrations first and process requests. ICANN should, however, support this implementation by giving guidelines and providing resources (e.g., code, APIs) to contracted parties.
- If a requested name is recognized as suspicious (e.g., similar or visually indistinguishable from a registered trademark or well-known brand, a well-known name with a typo, chaining of TLDs, etc.), registration should be denied, tracked after registration, or otherwise addressed.
- This appeals process should be automated in order to scale, but there should be some aspect of human oversight.

It is impossible to determine how misleading naming will evolve. Therefore, the targets for removal and countermeasures have to depend on measurement at the time. For example, DAAR could be used to report the effectiveness of current measures. If the methods used to curtail abusive naming fall below a certain threshold, updates should be required.

SSR2 Recommendation 19: Update Handling of Abusive Naming

19.5. ICANN org should build upon the current activities to investigate typical misleading naming, in cooperation with researchers and stakeholders, wherever applicable.

19.6. When misleading naming rises to the level of abusive naming, ICANN org should include this type of abuse in their DAAR reporting and develop policies and mitigation best practices.

19.7. ICANN org should publish the number of abusive naming complaints made at the portal in a form that allows independent third parties to analyze, mitigate, and prevent harm from the use of such domain names.

19.8. ICANN org should update the current "Guidelines for the Implementation of IDNs" **[citation to be added]** to include a section on names containing trademarks, TLD-

[75] ICANN SSAC, “IDN Homographs,” ICANN 63, October 2018, https://ccnso.icann.org/sites/default/files/field-attached/presentation-ssac-idn-homograph-22oct18-en.pdf.

chaining, and the use of (hard-to-spot) typos. Furthermore, ICANN should contractually enforce "Guidelines for the Implementation of IDNs" for gTLDS and recommend that ccTLDs do the same.

DNS Testbed

Rationale and Findings

As the DNS ecosystem is already large and is growing, maintaining and monitoring a regression test suite and testbed to analyze DNS behaviors and interactions is critical. The SSR2 RT has concluded that the ongoing DNS testbed activities by OCTO sufficiently address this concern, and the SSR2 RT 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 testing and research into resolver behavior, a crucial aspect for ensuring the integrity and availability of the DNS globally.

SSR2 Recommendation 20: Complete Development of a DNS Regression Testing

20.3. ICANN org should complete the development of a suite for DNS regression testing.[76]

20.4. ICANN org should ensure that the capability to perform functional testing of different configurations and software versions is implemented and maintained.

Key Rollover

Rationale and Findings

The DNSSEC Root rolled over its Key Signing Key (KSK) on 11 October 2018 for the first time since the Deliberately Unvalidatable Root Zone (DURZ) key. During this process, there was much debate and many calls for analyses of the details of the roll.[77],[78] One aspect of this rollover illustrated is the necessity for properly functioning exception-legs in the procedure. Specifically, the rollover was delayed for a year while measurements were taken to allay concerns. Discussions have already begun about the timing and procedure for future rollovers, including additional complexities, e.g., algorithm rollovers. At the time of this writing, ICANN is

[76] “Resolver Testbed,” ICANN GitHub repository, https://github.com/icann/resolver-testbed.

[77] 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&sa=D&ust=1579205545765000&usg=AFQjCNGr2uuSZFUK1SBrQJfEtoqn63wDWw

[78] 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.

holding an open call for comments on the process for the next scheduled KSK rollover process.[79]

The SSR2 RT found that other groups within the ICANN community have evaluated the actions around the KSK rollover and have made several recommendations that do not appear to have been implemented by ICANN org (see SAC063[80] and SAC073[81]).

For example, the global DNS Root is served by 13 instances of name server letters ('a' through 'm'), most of which consist of multiple anycast instances around the world.he Root Zone Maintainer (RZM) makes changes and propagates them to, all of the instances. In 2014 RSSAC published RSSAC002, an advisory on the measurement of the root server system, but it is not clear if or how much of this advisory ICANN org has implemented. The review team found no evidence that the propagation delay between publication to each of the letters, and then to each of a letter's instances, is well understood. Propagation delay is (for example) a relevant aspect of ensuring that validating resolvers are able to retrieve the sane DNSKEY RRset, and rollover timing can be predictable.

Software and systems process analysis is a research branch of computer science's software engineering.[82] Goals and benefits of work done in this discipline include understanding the nature, the errors, the guarantees, and other important facets of inherently complex processes. Among the reasons to formally model processes are to prove if the execution of a process is safe, if it can be defined to be error-free, to enforce forethought about how to handle errors and exceptions (instead of reaching an error state at runtime without having thought of how to handle it), and more. Modern research exists into applying software process analyses to prove election safety (i.e., to prove election outcomes have not been interfered with), medical process safety (i.e. to ensure that the process doctors follow for procedures are error-free and that exception legs are foreseen and thought through to protect patients, etc.). Additionally, tools exist to provide provable assurances of qualities such as safety and correctness of the execution of processes. The DNS' Root KSK rollover procedure could benefit from the assurances and guidance of these techniques. A large body of work and tool suites (including visualization) exist that help with the creation of processes. Following a formal process modeling analysis would allow, for example, stakeholders to follow a structured procedure to foresee complex situations before they arise, to create remediations for problems before they happen, and to have clarity on what must happen under exigent circumstances (with 'formally provable' assurances of safety).

[79] "Proposal for Future Root Zone KSK Rollovers," 1 November 2019, https://www.icann.org/en/system/files/files/proposal-future-rz-ksk-rollovers-01nov19-

[80] ICANN SSAC, "SSAC Advisory on DNSSEC Key Rollover in the Root Zone," SAC063, 7 November 2013, https://www.icann.org/en/system/files/files/sac-063-en.pdf.

[81] ICANN SSAC, "SAC073: SSAC Comments on Root Zone Key Signing Key Rollover Plan – Design Teams Draft Report," 5 October 2015, https://www.icann.org/en/system/files/files/sac-073-en.pdf.

[82] International Conference on Software and System Processes, http://icssp-conferences.org/.

SSR2 Recommendation 21: Implement the Recommendations from SAC063 and SAC073 and Establish Formal Procedures for Key Rollovers

21.4. ICANN org should implement the recommendations from SAC063 and SAC073 in order to ensure the SSR of the KSK rollover process.

21.5. ICANN org should establish a formal procedure, supported by a formal process modeling tool and language[83] 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, FSM) for public comment, and community feedback should be incorporated. 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 lessons learned can be used to adjust the process.

21.6. 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.

Root Server Operations

Rationale and Findings

As a Root Server Operator, ICANN org's role in operating a critical part of the global DNS resolution infrastructure is hugely important. Threats to the DNS have been documented[84] and shared by ICANN org with the community.

In June 2018, RSSAC released RSSAC037, "A Proposed Governance Model for the DNS Root Server System," which recommends a "Strategy, Architecture, and Policy Function" offering guidance on matters concerning the RSS "performance monitoring and measurement function" as part of the new governance model.[85] A companion document—RSSAC 0038 [86]—asks ICANN to drive progress on implementation of RSSAC 0037, per the RSSAC Advice status from the ICANN Board.[87] The SSR2 RT notices that a governance model for RSS could be a good starting point in better coordination of the operations of RSOs. Although RSSAC037 proposes to have the development of best practices for RS operations covering availability, performance,

[83] 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)

[84] "Independent Review of the ICANN Root Server System Advisory Committee (RSSAC) Final Report," prepared Lyman Chapin, Jim Reid, and Colin Strutt of the Interisle Consulting Group, LLC, 2 July 2018, https://www.icann.org/en/system/files/files/rssac-review-final-02jul18-en.pdf.

[85] "RSSAC037A: Proposed Governance Model for the DNS Root Server System", ICANN Root Server System Advisory Committee, 12 June 2018, https://www.icann.org/en/system/files/files/rssac-037-15jun18-en.pdf.

[86] "RSSAC Advisory on a Proposed Governance Model for the DNS Root Server System," ICANN Root Server System Advisory Committee, 12 June 2018, https://www.icann.org/en/system/files/files/rssac-038-15jun18-en.pdf

[87] "Root Server System Advisory Committee (RSSAC) Advice Status," ICANN Board, last updated 30 November 2019, https://features.icann.org/board-advice/rssac.

scalability, and security, the document does not explicitly target the security measures necessary for the smooth and secure implementation of the governance model. The implementation status of the RSSAC037 governance model is also not known, although there has been a recent call for nominations to serve on the RSS Governance Working Group (GWG).[88]

The SSR2 RT also notices that ICANN org does not have a published (living) document that describes the common best practices for DNS resolution to minimize SSR risks. This document could be maintained by ICANN OCTO to promote best practices by applying hardening strategies on IMRS and encouraging other RSOs to do the same.

SSR2 Recommendation 22: Establish Baseline Security Practices for Root Server Operators and Operations

22.5. ICANN org, in close cooperation with RSSAC and other relevant stakeholders, should ensure that the RSS governance model as proposed by RSSAC037 includes baseline security best practices for root server operators and operations in order to minimize the SSR risks associated with root server operation. These best practices should include change management, verification procedures, and sanity check procedures.

22.6. ICANN org should also develop relevant KPIs to measure the implementation of these best practices and requirements and ensure yearly public reporting on how Root Server Operators (RSOs) and other relevant parties, including ICANN org, can meet these KPIs.

22.7. ICANN org should document hardening strategies of the ICANN Managed Root Server (IMRS), commonly known as L-Root, and should encourage other RSOs to do the same.

22.8. ICANN org should ensure that the IMRS uses a vulnerability disclosure process (not necessarily public), security reports and intelligence, and communication with researchers and RSSAC advice or recommendations, where applicable.

Root Zone Change Management

Rationale and Findings

The root zone management follows a workflow system for managing TLD labels in the root zone called the Root Zone Management System (RZMS).

In recognition of its critical role in the DNS ecosystem, ICANN org practices a conservative approach to managing the root zone, which supports the objectives for security, stability, and resiliency. In terms of the general operational workflow, processing follows a well-understood process that involves the significant review of each requested change by multiple parties. All changes are reviewed automatically and manually throughout the process, and staff is empowered to engage with the customer to ask questions and request additional steps whenever a request raises a concern before the implementation.

[88] Call for Nominations, ICANN RSS Governance WG. https://www.iab.org/2019/11/18/call-for-nominations-icann-root-server-system-governance-working-group-gwg/

Even though there were no known security and stability issues that involve the misuse of the RZMS, authentication of change requests should be more stringent and involve advanced technologies such a multi-factor authentication and secure communication when using email.

The IANA team is currently building its next-generation RZMS, which involves a substantial rewrite of the authorization model. The next generation RZMS should involve 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 implementation of RFC 8078 and related updates for automated DNSSEC Delegation Trust Maintenance (CDS/CDNSKEY).

Although the development and implementation of the new RZMS system has been announced for several years, the SSR2 RT did not find any indication as to when ICANN org plans to put the new system into service.

SSR2 Recommendation 23: Accelerate the Implementation of the New-Generation RZMS

ICANN org has committed to increasing the level of security and responsiveness of the Root Zone Management System.

23.3. ICANN and PTI operations should accelerate the implementation of new RZMS security measures regarding the authentication and authorization of requested changes.

23.4. ICANN org should launch public comment as soon as possible on changes regarding revisions to the RZMS policies.

Root Zone Data and IANA Registries

Rationale and Findings

Measures of the Root Zone Measures (Key Performance Indicators, KPIs): The SSR2 RT believes that various stakeholders need to be able to assess key SSR indicators (e.g., DNSSEC, availability, performance, integrity, abuse) of the root zone over time. Additionally, the IANA registries include many needed parameters that are specified by RFCs in the IETF, but IANA does not make available KPIs related to the availability and integrity of these registries.

Ideally KPI/services would 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 also the global network availability of these registries;
- metrics that reflect the responsiveness of the CZDS service to the community's needs and intended use of this service.

Access to critical data via the "Centralized Zone Data Service" (CZDS)[89] remain problematic.[90] At the moment, registries do not grant access as intended and revoke access periodically with long renewal processes.[91],[92] These data are regularly used for studying abuse in the DNS. **[citation to be added]**

SSR2 Recommendation 24: Create a List of Statistics and Metrics Around the Operational Status of the Unique Identifier Systems

24.5. ICANN org should create a list of statistics and metrics that reflect the operational status (such as availability and responsiveness) of each type of unique identifier information, such as root-zone related service, IANA registries, and any gTLD service that ICANN org has authoritative purview over.

24.6. ICANN org should publish a directory of these services, data sets, and metrics on a single page on the ICANN org web site, such as under the Open Data Platform.

24.7. ICANN should publish annual and longitudinal summaries of this data, solicit public feedback on the summaries, and incorporate the feedback to improve future reports.

24.8. For both sets of KPIs, ICANN org should produce summaries over both the previous year and longitudinally, request and publish a summary of community feedback on each report and incorporate this feedback to improve follow-on reports.

SSR2 Recommendation 25: Ensure the Centralized Zone File Data Access is Consistently Available

25.3. The ICANN community and ICANN org should take steps to ensure that access to CZDS as well as other data is available, in a timely manner, and without unnecessary hurdles to requesters.

[89] ICANN, "CZDS Centralized Zone Data Service," accessed 20 January 2020, https://czds.icann.org/home.

[90] "CZDS-API-Testbed," mailing list, https://mm.icann.org/mailman/listinfo/czds-api-testbed.

[91] "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.

[92] 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.

25.4. ICANN org should implement the four recommendations in SSAC 97:[93]

"Recommendation 1: The SSAC recommends that the ICANN Board suggest to ICANN Staff to consider revising the CZDS system to address the problem of subscriptions terminating automatically by default, for example by allowing subscriptions to automatically renew by default. This could include an option allowing a registry operator to depart from the default on a per-subscriber basis, thereby forcing the chosen subscriber to reapply at the end of the current term. The CZDS should continue to provide registry operators the ability to explicitly terminate a problematic subscriber's access at any time.

Recommendation 2: The SSAC recommends that the ICANN Board suggest to ICANN Staff to ensure that in subsequent rounds of new gTLDs, the CZDS subscription agreement conform to the changes executed as a result of implementing Recommendation 1.

Recommendation 3: The SSAC recommends that the ICANN Board suggest to ICANN Staff to seek ways to reduce the number of zone file access complaints, and seek ways to resolve complaints in a timely fashion.

Recommendation 4: The SSAC recommends that the ICANN Board suggest to ICANN Staff to ensure that zone file access and Web-based WHOIS query statistics are accurately and publicly reported, according to well-defined standards that can be uniformly complied with by all gTLD registry operators. The Zone File Access (ZFA) metric should be clarified as soon as practicable.

Emergency Back-End Registry Operator (EBERO)

Rationale and Findings

An EBERO[94] provider is temporarily activated if a generic Top-Level Domain (gTLD) operator is at risk of failing to sustain critical registry functions, which ensures the availability of these functions protects registrants and provides an additional layer of protection to the DNS. Only minimal testing of EBERO has been conducted. One test was conducted with .doosan,[95] and another test was conducted with .mtpc.[96] The most recent test was conducted in 2017. However, the EBERO processes do not appear to be fully documented.

[93] 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.

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

[95] ICANN, EBERO Exercise report, Tech Day ICANN 55, 7 March 2016, https://meetings.icann.org/en/marrakech55/schedule/mon-tech/presentation-ebero-07mar16-en.pdf.

[96] Kevin Murphy, "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.

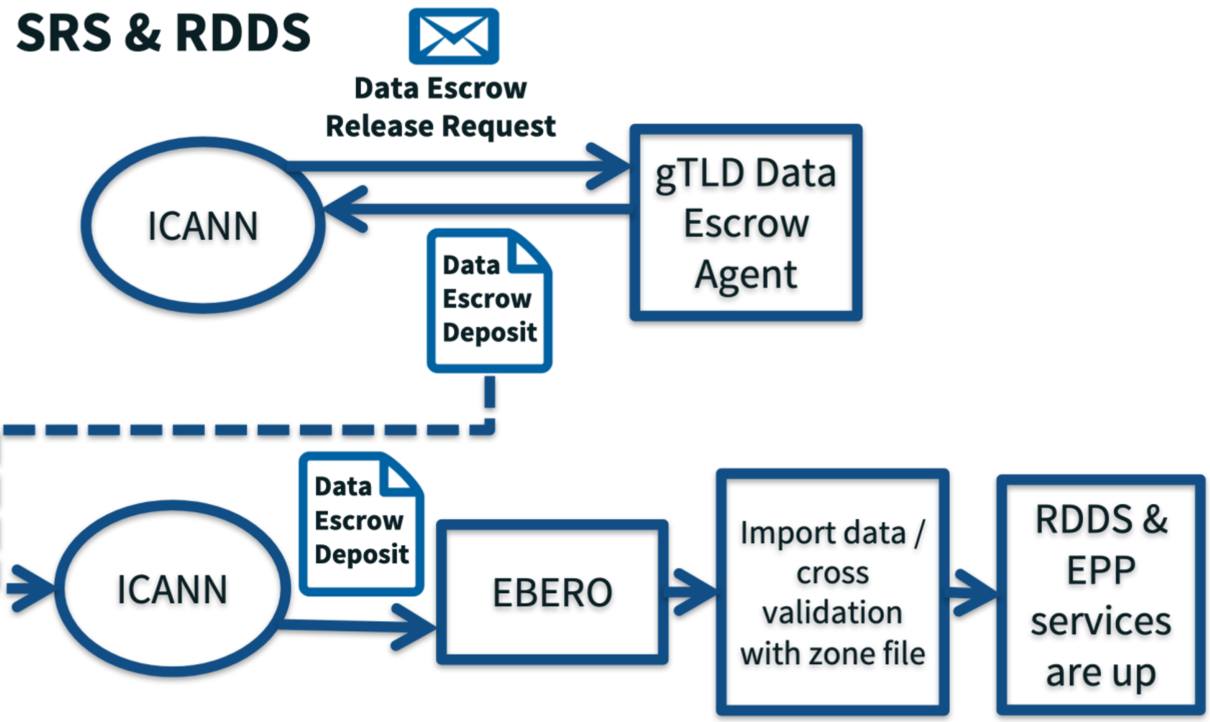
SRS & RDDS
Data Escrow Release Request
ICANN
gTLD Data Escrow Agent
Data Escrow Deposit
ICANN
Data Escrow Deposit
EBERO
Import data / cross validation with zone file
RDDS & EPP services are up

Figure 1. Diagram of Current EBERO Processes

SSR2 Recommendation 26: Document, Improve, and Test the EBERO Processes

26.5. ICANN org should publicly document the ERERO processes, including decision points, actions, and exceptions. The document should describe the dependencies for every decision, action, and exception.
26.6. Where possible, ICANN org should automate these processes and test them annually.
26.7. ICANN org should publicly conduct EBERO smoke-testing at predetermined intervals using a test plan coordinated with the ICANN contracted parties in advance to ensure that all exception legs are exercised and publish the results.
26.8. ICANN org should improve the process by allowing the gTLD Data Escrow Agent to send the data escrow deposit directly to the EBERO provider.

Workstream 4: Future Challenges

This workstream relates to Bylaw 4.6(c) (iii) and focused on two key areas: 1. Potential threats to the secure and resilient operations of the unique identifiers systems ICANN coordinates; and 2. Long term strategy of ICANN to anticipate and mitigate these threats.

Cryptography

Rationale and Findings

DNS Cryptography

The SSR2 RT investigated two topics in the area of DNS Cryptograph. 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.

Elliptic Curve Cryptography

Elliptical curve cryptography (ECC) offers an alternative to the RSA public-key cryptography that is 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. The Elliptic Curve Digital Signature Algorithm (ECDSA) is widely accepted as secure.**(cite to be added)**

"Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC" (RFC 6605)[97] has been published by the IETF to specify the use of ECDSA with curve P-256 and SHA-256 in DNSSEC. Current estimates are that ECDSA with curve P-256 has roughly the same strength to RSA with 3072-bit keys; however, the keys are smaller, and the signature processing consumes less computing power. The smaller size provides a considerable advantage for the DNS protocol, especially when DNS is used over UDP. The lower computing power consumption offers a significant advantage, especially for battery-powered devices.

The Root KSK DNSSEC Practice Statement (DPS) provides guidance on key length and key rollover.[98] The DPS says nothing, however, about how changes to the digital signature algorithm may be performed. Recent guidance from the US National Security Agency recommends using 3072 bits for RSA.[99] ECDSA seems to offer a better alternative than very large RSA keys.

Post Quantum Cryptography

Most people had not heard of quantum computing a decade ago, but in recent years, it has captured the public's imagination. Part of this interest comes from the unique computational power of a quantum computer. The US National Academy of Sciences recently issued a report

[97] 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>.

[98] "DNSSEC Practice Statement for the Root Zone KSK Operator," RZ KSK PMA, 1 October 2016, https://www.iana.org/dnssec/icann-dps.txt.

[99] National Security Agency/Central Security Service Information Assurance Directorate, "Commercial National Security Algorithm Suite and Quantum Computing FAQ," MFQ U/OO/815099-16, January 2016, https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/cnsa-suite-and-quantum-computing-faq.cfm.

on “Quantum Computing: Progress and Prospects,”[100] with the high-level conclusion that now is the time to start preparing for a quantum-safe future.

DigiCert has estimated that it takes several quadrillion years to factor a 2048-bit RSA key[101] using classical computing technology. In the future, if a large-scale quantum computer is invented, it can break the same key much faster, perhaps 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 that are used to secure the Internet.

Progress towards a large-scale quantum computer must track not only the scaling rate of the number of physical quantum bits or “qubits” computers have, but also error rates. Error rates are important because they have a significant impact on the number of physical qubits required to make a logical qubit. Physical qubits are the individual quantum systems that represent 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 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[102], which is working with researchers around the world to develop new cryptographic primitives that are not susceptible to attack by quantum computers. 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.[103] However, the signatures are quite large, and a private key can only be used to 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.

[100] Emily Grumbling, Mark Horowitz, eds., *Quantum Computing: Progress and Prospects*, (The National Academies Press, 2019), https://doi.org/10.17226/25196.

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

[102] Project website for Post-Quantum Cryptography, NIST: Information Technology Laboratory: Computer Security Resource Center, created 3 January 2017, last updated 22 October 2019, https://csrc.nist.gov/projects/post-quantum-cryptography.

[103] Crypto Forum Research Group, Internet Research Task Force (IRTF), last modified 7 April 2019, https://irtf.org/cfrg.

SSR2 Recommendation 27: Update the DPS and Build Consensus Around future DNSKEY Algorithm Rollovers

27.3. PTI operations should update the DPS to facilitate the transition from one digital signature algorithm to another, including an anticipated transition from the RSA digital signature algorithm to ECDSA or to future post-quantum algorithms, which will create a more resilient DNS while providing the same or greater security.

27.4. As 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.

Name Collision

Rationale and Findings

While ICANN org provides detailed education on name collision, there is no restriction of registrants utilizing a unique identifier for a private zone that collides with a public zone. There is no reporting and alerting mechanism allowing the community to file reports that may reveal sensitive data and security threats resulting from the collision.

With the known instances of these attack vectors, the SSR2 RT feels the name collision problem is present and must be explored, diagnosed, and acted upon through careful study and action. Among the findings of "MitM attack by name collision: Cause analysis and vulnerability assessment in the new gTLD era"[104] were that the last round of gTLDs measurably exacerbated this problem.

SSR2 Recommendation 28: Develop a Report on the Frequency of Name Collisions and Propose a Solution

28.4. ICANN org should produce findings that characterize the nature and frequency of name collisions and resulting concerns. The ICANN community should implement a solution before the next round of gTLDs.

28.5. ICANN org should facilitate this process by initiating an independent study of name collisions through to its eventual completion and adopt or account for the implementation or non-adoption of any resulting recommendations. By "independent," SSR2 RT means that ICANN org should ensure that the SSAC Name Collision Analysis Project (NCAP) work party research and report evaluation team's results need to be vetted by parties that are free of any financial interest in TLD expansion.

28.6. ICANN org should enable community reporting on instances of name collision. These reports should allow appropriate handling of sensitive data and security threats and should be rolled into community reporting metrics.

[104] 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.

Privacy

Rationale and Findings

Privacy and WHOIS Conflicts

One of the challenges the SSR2 RT faced in this investigation was the lack of clear policies and linkages to dated documents related to the topic. While there are many resources on the ICANN org website on the subject of privacy, the SSR2 RT was unable to locate one comprehensive page that addresses the topic substantially and included references to current documents on the subject area. According to ICANN org,

> *Discussion of privacy laws and the transfer of personal data always accompany WHOIS discussions. Some policy discussions center on changing the WHOIS policy to restrict the amount of information available through the display of a WHOIS record. … Laws change over time, and it may be difficult to identify how privacy laws apply to the flow of information and data across borders.*
>
> *As a result, there is the possibility of conflicts between national laws and the terms and conditions applicable to WHOIS. Registrars and registries must abide by applicable law. ICANN has developed procedures for addressing issues where conflicts arise between compliance with ICANN policy and compliance with national laws.*[105]

The SSR2 RT evaluated the concept of privacy within the context of the introduction of new global requirements that address privacy and data protection. The connection between WHOIS enquiries—a resource tool for law enforcement, academia, and other public policy practitioners—and security considerations was also considered during this review. The SSR2 RT undertook both a desk review and the submission of specific enquiries to ICANN staff to develop the recommendations relating to privacy.

One of the conclusions made from the information discovered was that while ICANN org has developed various documents in response to the challenges arising from WHOIS conflicts and privacy, it was still evident that there was an unnecessarily limited interpretation taken by ICANN staff, including the Contract Compliance Unit, on their role in ensuring contracted parties adhere to the Service Level Agreements, including addressing the investigation of complaints about inaccurate WHOIS information.[106] For example, WHOIS Guidance on WHOIS and Privacy Law and also on Privacy and Proxy Services does not reflect the current discussions and on the web page the notification only indicates:[107]

> *NOTICE, DISCLAIMERS AND TERMS OF USE:*

[105] ICANN's Current Issues page on Privacy, accessed on 27 December 2019, https://whois.icann.org/en/privacy.

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

[107] "Privacy and Proxy Services," ICANN, accessed on 27 December 2019, https://whois.icann.org/en/privacy-and-proxy-services.

> *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.*

In this regard, ICANN org has included on its web page information related to the Temporary Specification[108] some guidance. The SSR2 RT did not find any updates linked to the page on the current policy position since its adoption by the Board in May 2018 and reaffirmation in January 2019.[109]

More specifically to contract obligations, ICANN, according to Section 4.6(e)[110] of the Bylaws, is only required, subject to applicable laws, to "***use commercially reasonable efforts** to enforce its policies relating to registration directory services*," including by working with stakeholders to "*explore structural changes to improve accuracy and access to generic top-level domain registration data*," "a*s well as consider[ing] safeguards for protecting such data.*" In relation to privacy, while ICANN does have a privacy policy, in an explanatory note released in February 2019, an explanatory note released by ICANN org in February 2019 stated "*ICANN's role is very limited, and it is not responsible for many issues associated with the Internet, such as financial transactions, Internet content control, spam (unsolicited commercial email), Internet gambling, or* ***data protection and privacy." (emphasis added)***[111] ICANN org, in having a privacy policy that covers registration information and having bylaws that requires it enforce its own policies, is in conflict with their statement that ICANN org is not responsible for data protection and privacy.

The SSR2 RT also notes that ICANN org's mission and mandate, as stated in ICANN's Bylaws, highlights the role of ICANN in the Registration Data Access Protocol (**RDAP**)[112] and the need for adaptability when external regulations such as the EU GDPR are issued.

Service Level Agreements

The Contractual Compliance Unit indicated in response to questions on the treatment of complaints on WHOIS that they saw no need to change the Registrar Accreditation Agreement to respond to complaints of inaccurate WHOIS. Further, it was apparent during the review that ICANN Contractual Compliance is responsible for enforcing Specification 10 of the RA directly with the registry operators, as Registry Service Providers (RSPs) are not ICANN org contracted parties and, therefore, out of ICANN org's contractual authority for enforcement of RA obligations. Registry operators are subject to Service Level Agreement monitoring and, for Registration Data Directory Services (RDDS), DNS and DNSSEC failures. They would receive automated compliance Escalated Notices when they meet certain downtime thresholds, as well as compliance notices when data escrow failures occur. Upon resolution of the downtime, ICANN Contractual Compliance follows up with the registry operator for additional information and preventative actions. Registry operators often provide information from their RSPs in

[108] "Temporary Specification for gTLD Registration Data," ICANN, effective date 25 May 2018, https://www.icann.org/resources/pages/gtld-registration-data-specs-en.

[109] "ICANN Board Reaffirms Temporary Specification for gTLD Registration Data," ICANN Announcements, 29 January 2019, https://www.icann.org/news/announcement-2019-01-29-en.

[110] ICANN, Bylaws Article 4, "Accountability and Review," as amended 28 November 2019, https://www.icann.org/resources/pages/governance/bylaws-en/#article4.

[111] "FAQs for Registrations: About ICANN," accessed on 27 December 2019, https://www.icann.org/resources/pages/about-icann-faqs-2019-02-25-en.

[112] "Registry Data Access Protocol (RDAP)," ICANN, n.d., https://www.icann.org/rdap.

support of their responses. Failure to remediate noncompliance for these functions can result in ICANN Contractual Compliance issuing a notice of breach against the registry operator and transitioning the top-level domain to an emergency back-end registry operator (EBERO). However, when the SSR2 RT explicitly asked ICANN Contractual Compliance about auditing, the response indicated that the frequency of an audit of a contracted party varies based on the systemic issues and the audit scope and criteria.

The conclusion based on the analysis of the team is that if contracts are negotiated only between contracted parties and ICANN org, which no representation of consumer harm, this deprioritization of SSR is a guaranteed outcome. Further, as it relates to privacy concerns, the results of the investigation did not reveal sufficient information on a deliberate and coordinated approach to substantively address the issues. Therefore, the SSR2 RT targeted their recommendations in the areas of security and privacy towards raising the need to include additional measures to ensure that security and privacy are balanced and prioritized.

SSR2 Recommendation 29: Focus on Privacy and SSR Measurements and Improving Policies Based on Those Measurements

29.5. ICANN org should monitor and regularly report on the privacy impact of technologies like DoT (DNS over TLS) and DoH (DNS over HTTPS).

29.6. ICANN org's consensus policies and agreements with registry operators and registrars should, therefore, have clauses to reflect compliance with these while ensuring that the DNS is not fragmented because of the need to maintain/implement minimum requirements governing the 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.

29.7. ICANN org should:

29.7.1. Create specialized units within the contract compliance function that focus on 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 evolving RDAP framework.

29.7.2. Monitor relevant and evolving privacy legislation (e.g., CCPA and legislation protecting personally identifiable information (PII)) and ensure that ICANN org's policies and procedures are aligned and in compliance with privacy requirements and the protection of personally identifiable information as required by relevant legislation and regulation.[113]

29.7.3. Develop and keep up to date a policy for the protection of personally identifiable information. The policy should be communicated to all persons involved in the processing of personally identifiable information. Technical and organizational measures to appropriately protect PII should be implemented.

29.7.4. Conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they, at a minimum, have procedures in place to address privacy breaches.

29.8. ICANN org's DPO should also be responsible for external DNS PII. The DPO should provide guidance to managers and stakeholders regarding responsibilities and procedures and monitor and report on relevant technical developments.

[113] The Review Team is aware of the ICANN org Charter outlining approach to government engagement https://www.icann.org/en/system/files/files/proposed-org-engagement-govt-standards-charter-25feb19-en.pdf and the Legislative report (the Tracker) https://www.icann.org/legislative-report-2019. However we would like a more specific focus on privacy and data protection.

Research and Briefings

Rationale and Findings

An enormous amount of activity is now occurring in the academic research community related to SSR issues of 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 itself and the community it serves stay aware of these developments.

SSR2 Recommendation 30: Stay Informed on Academic Research of SSR Issues and Use That Information to Inform Policy Debates

30.1. 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 S&P, as well as the operational security conferences APWG, M3AAWG, and FIRST, and publish a report for the ICANN community summarizing implications of publications that are relevant to ICANN org or contracted party behavior.

30.1.1 These reports should include 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.

30.1.2. These reports should also include recommendations for additional study to confirm peer-reviewed findings, a description of what data would be required to execute additional recommended studies, and how ICANN can offer to help broker access to such data, e.g., CZDS.

DNS-over-HTTPS

Rationale and Findings

The introduction of DNS over encrypted protocols was intended to solve DNS privacy concerns.[114] However, DNS-over-HTTPS (DoH) does not protect DNS privacy at the endpoints, and introduces security risks that some consider more serious than the privacy risks it mitigates. An alternative to DoH, DNS over TLS (DoT) operates over port 853, which means that network operators can still track (though not observe the contents of) transactions on their networks. By contrast, DoH uses port 443 where even the presence of DNS traffic hides within the flux of the HTTPS web traffic. DoH, shifts network operators' controls by moving important security and stability into the hands of software vendors. In the degenerative case, DoH creates a single point of failure. More generally, DoH lets application software diffuse DNS resolution in ways that transport networks can neither control nor inspect. For example, a third-party app on a

[114] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

phone could unilaterally elect to use a third-party DoH resolution infrastructure that could effectuate selective intercept without the knowledge of even the app vendor (who installed it).

Another DoH consideration relates to DNSSEC, which enforces cryptographic integrity of the mapping from domain name to IP addresses. By allowing third parties to tunnel encrypted DNS resolution inside HTTP, users give external parties the opportunity to selectively bypass DNSSEC. This is a particular concern when the selected resolver does not properly perform DNSSEC validation. A less conscientious choice of resolution infrastructure amounts to users installing a more systematic form of the ‘DNSpionage’ campaign attacks for themselves.

The DoH protocol facilitates the danger posed by this operational trend. For some applications, DoH will mandate centralized resolution among a few large providers. For others, resolution choices can establish covert or non-negotiable resolution paths without user control or awareness. Either case will hide traffic from network operator and remove user choice from DNS resolution behavior. Additional concerns exist around application vendors selecting diverse HTTPS resolution infrastructures, thereby allowing per-application intervention in resolution and selective enforcement of DNSSEC.

SSR2 Recommendation 31: Clarify the SSR Implications of DNS-over-HTTPS

31.1. ICANN org should commission an independent investigation(s) into the SSR-related implications of DoH deployment trends, as well as implications for the future role of IANA in the Internet ecosystem. The intended outcome is to ensure that all stakeholders have the opportunity to understand the SSR-related implications of these developments, and the range of alternatives (or lack thereof) various stakeholders have to influence the future.

Appendix A: 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 RT) operated under the following definitions:[115]

- 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"[116]
- Internet Identifier Systems Security, Stability, and Resiliency (IIS-SSR) Framework – Another name for IS-SSR Framework
- 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

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

[116] "Identifier Systems Security, Stability and Resiliency Framework–FY 15-16," ICANN, September 2016, https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf.

- 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.
- 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[117]

Acronyms

- BC – Business Continuity
- CISO – Chief Information Security Officer
- CSO – Chief Security Officer
- CZDS – Centralized Zone Data Service[118]
- DAAR – Domain Abuse Activity Reporting[119]
- DNS - Domain Name System
- DNSSEC – the DNS Security Extensions (specified in RFCs 4033, 4034, and RFC 4035)
- DoH – DNS over HTTPS
- DoT – DNS over TLS
- DPS – DNSSEC Practice Statement
- DR – Disaster Recovery
- EBERO - Emergency Back-End Registry Operator
- FSM - Finite-State Machine
- gTLD - generic Top-Level Domain
- HTTP – HyperText Transfer Protocol
- HTTPS – HyperText Transfer Protocol Secure

[117] "Defining the Role and Function of IETF Protocol Parameter Registry Operators," RFC 6220, April 2011, https://www.rfc-editor.org/info/rfc6220.

[118] "Centralized Zone Data Service (CZDS)," ICANN, accessed on 30 December 2019, https://www.icann.org/resources/pages/czds-2014-03-03-en.

[119] "Domain Abuse Activity Reporting," ICANN, accessed on 30 December 2019, https://www.icann.org/octo-ssr/daar.

- IANA - Internet Assigned Numbers Authority
- IMRS – ICANN Managed Root Server
- ISMS – Information Security Management System
- ISO - International Organization for Standardization
- OCTO - Office of the Chief Technology Officer
- PII – Personally Identifiable Information
- PTI - Public Technical Identifiers
- RAA – Registrar Accreditation Agreement
- RDAP – Registration Data Access Protocol
- RDDS - Registration Data Directory Services
- RSSAC - Root Server System Advisory Committee
- SADAG - Statistical Analysis of DNS Abuse in gTLDs
- SLA – Service Level Agreement
- SMART - specific, measurable, assignable, relevant, and trackable
- SOP – Strategic and Operating Plans
- SSAC - Security and Stability Advisory Committee
- SSR – Security, Stability, and Resiliency
- SSR1 - first SSR review process
- SSR2 RT – SSR2 Review Team
- TLS – Transport Layer Security

Appendix B: Further Suggestions

Suggestion 1

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 RT suggests that ICANN org should create an email mailing list for announcements about public comment periods upon their closing. At the moment, finding information about public comments can be quite challenging. Implementing this suggestion will serve to increase awareness among mailing list subscribers of public comment periods as they close, 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 RT 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 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 comment period. In addition, the SSR2 RT 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 2

ICANN should implement a continuous function to track the progress of review team recommendations and also provide quarterly reports to the members of the review team that produced the recommendations. This function should include a web page that provides information about implementation progress to the whole community. This function should allow review team members to provide feedback on whether the implementation is as intended, avoiding questions from the next generation of the review team when they assess the implementation and whether it had the intended effect.

Suggestion 3

To avoid misunderstanding and broken expectations, ICANN Staff should develop a clear written process for obtaining contracted resources for review teams, including milestones and points for review team approval.

Suggestion 4

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

Suggestion 5

ICANN org should establish a system to track review team recommendation implementation over time to enable future review teams to assess the implementation status.

Appendix C - Process and Methodology

Process and Methodology for the Review of SSR1 Recommendations

The assessment process of the SSR2 RT 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. The team also used outreach sessions 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 RT also 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 RT 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, and providing evidence and documentation to satisfy to the team that implementation had been completed successfully. 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. For each recommendation, the report provides a list of all documents used by the SSR2 team and answered questions by ICANN org staff.

In order to allocate its time and resources efficiently, the team first performed research and investigation based on these available or provided materials in 2017. Then, the team focused its further efforts on specific SSR issues and open questions identified by this initial 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 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?
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 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 RT conducted a series of interviews with ICANN staff. Questions focused on the completeness and effectiveness of ICANN org's security processes and the effectiveness of the ICANN org security framework.

The SSR2 RT 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 mapping the resulting data to the relevant ICANN component(s), procedures, and policies.

Within Workstream 4 regarding future challenges for SSR, the SSR2 RT 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 RT recognized that this workstream was dependent on the emerging themes from the other dependent areas. More specifically, in addition to commonly identified 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. As noted in 'Workstream 1: Review of SSR1 Implementation and Impact,' the SSR2 RT 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 also 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.

54

SSR2 Conclusion: This recommendation remains relevant; further work is needed to bring this process to closure, especially because of the inconsistencies between different versions of the remit.[120]

[120] See, for example, clause 7.3 of the Registry Agreement, https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.docx.

Rationale:

- The team observes that a statement exists[121], and it was updated as a result of a review by the community[122]. Despite the existence of this statement, the use of definitions remains inconsistent. For example, the definitions of Security and Stability contained in ICANN org's agreements with contracted parties are different.
- No metrics were provided to evaluate whether the implementation had its intended effect; while the statement exists, given the discrepancies in how it is used, it did not have the impact expected.

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: As above, this recommendation remains relevant and can be correlated to SSR1 Recommendation 1.

Rationale:

- The implementation of this recommendation is incomplete, mainly because the concept of community input needs to be part of a clear framework that is adopted by community consensus.
- The definitions of Security and Stability contained in ICANN org's agreements with contracted parties are different. In recent years, while some updates to the IS-SSR Framework received community review, this was not done for every update.
- Regular reviews of the SSR remit have not happened. There have been no opportunities to comment specifically on the remit and mission statement since 2013. Current definitions make it difficult to assess the implementation

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.

[121] "SSR Role & Remit," https://www.icann.org/resources/pages/ssr-role-remit-2015-01-19-en.

[122] "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.

SSR2 Conclusion: This recommendation is still relevant. The SSR2 RT noted a correlation between this recommendation (SSR1 Recommendation 3) and SSR1 Recommendations 1 and 2. As pointed out above, the team observes that a statement exists, and it has been reviewed by the community. A blog post from July 2013 lists ICANN org's security terminology available to the whole community;[123] however, these definitions do not appear to be consistently integrated into other SSR-related documents. Therefore, it is clear that the definitions of Security and Stability contained in ICANN org's agreements with contracted parties are not entirely consistent and so the implementation cannot have had its intended effect.

Further work would include updating current definitions where needed, publicize them appropriately, and establishing procedures to ensure consistency. ICANN org should develop a public glossary for the ICANN community, and then develop procedures that ensure the terms in the glossary are used in all material and communications, and revisited - and if necessary updated - yearly, with document control in place to make changes trackable. This process should have an owner within ICANN org who would also be responsible for providing clarification of terms when needed.

Rationale:

- 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 has not been updated since February of 2014. For example, the definitions of Security and Stability contained in ICANN org's agreements with contracted parties diverge. Further, there are no references to SSR, its remit, or mission in the publicly available glossary.
- The team did not find procedures that are employed to ensure that the defined terms are used in all material and communications; however, the team did find evidence of inconsistencies.

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 and did not have its intended effect. Whenever questions about ICANN's SSR remit and relevant relationships arise, there should be a comprehensive and informative focal point for understanding SSR's relationships with other organizations in- and outside the ICANN community.

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

Further work is needed to update the document that defines the nature of the SSR relationships. This document should be kept up to date. It should indicate what relationships exist, what aspects they cover, and how they are maintained in contrast to the current form where no indicative information is given for the majority of entries. If information is to be omitted in the public-facing document, the information should still be filed.

Rationale:

- Whereas the key document for tracking ICANN SSR-related roles and responsibilities lists every organization with which ICANN org has ever had a formal relationship, a pointer to the document that underpins that relationship, and a description of the SSR components of that relationship,[124] many of the references listed cannot be located online. Furthermore, while there are additional documents that provide small pieces of evidence, the single focal point called for in the recommendation does not exist. In addition, the document often shows the SSR components of the relationships as "unknown."
- ICANN org reports that many SSR relationships have been defined and publicized.[125] As part of the OCTO SSR Team Strategic and Operating Plans (SOP), these are supposed to be updated periodically.[126] Memorandums of Understanding (MOUs) have been signed with numerous entities.[127] It was expected that SSR-related portions of these MOUs would be extracted and cataloged; however, ICANN org reports that some relationships are sensitive, and thus they are not disclosed. As pointed out above, the team observes that a statement of SSR-related roles and responsibilities exists, and it has been reviewed by the community.

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. Reporting on ICANN org's progress toward SSR-related critical success factors (CSFs) and key performance indicators (KPIs) involving SSR relationships is part of the OCTO SSR Team Strategic and Operating Plans (SOP), and they can be found in regular project management reporting, operating plans, the IS-

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

[125] "Supporting a Healthy, Resilient Internet," version 1.0, 1 April 2013, https://www.icann.org/sites/default/files/assets/security-2000x1295-30jul13-en.png.

[126] IS SSR Update, "ICANN Identifier System SSR Update – 2H 2014," 21 January 2015, https://www.icann.org/en/system/files/files/is-ssr-update-s2-2014-21jan15-en.pdf.

[127] "Partnership Memorandums of Understanding," ICANN, https://www.icann.org/resources/pages/governance/partnership-mous-en.

SSR Framework, and SSR quarterly reports. ICANN org should be encouraged to do routine SSR reports and ensure that the sections related to relationships with other external organizations are highlighted and kept up to date. Where possible, insight into these relationships should be provided in an easily accessible format. Lastly, the recommendation specifically mentions maintenance, making this is a constant process.

Rationale:

- The team expects the IS-SSR Framework to include information on how the key relationships[128] called for in SSR1 Recommendation 4 are used to achieve SSR goals; however, this information is not readily available.
- While evidence has been presented that ICANN org has taken various steps to forge relationships, little evidence is available regarding what these relationships entail and whether they are effective. Therefore, the SSR2 team cannot assess if working relationships are functional. There is some evidence, however, that ICANN org has succeeded in establishing relationships with relevant actors.

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

SSR2 Conclusion: This recommendation remains relevant; implementation was started but has not been completed. The roles and responsibilities for SSAC and RSSAC are captured in a document.[129] 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 RT could not locate the final document.

Guidance on how to complete this recommendation is included below; it is not new work but should be considered in the context of completing SSR1.

The ICANN community should update the draft document from March 2015 that describes SSAC and RSSAC responsibilities to resolve the comments from SSAC and RSSAC, and then the public comment should be resumed or repeated. Once consensus is reached, ICANN org

[128] “SSR Relationships,” https://www.icann.org/en/system/files/files/ssr-relationships-fy17-23jan17-en.pdf.

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

should produce a final document with a stable URL to publicly clarify and define the functions of SSAC and RSSAC.

Rationale:

- 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 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.*

- ICANN org uses the web site (https://www.icann.org/public-comments) to manage the public comment process. However, the web site does not capture information about calls for public comment in a way that is easy to search. It is especially challenging to gather history, including any final consensus, for public comments that happened many years ago.

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. It is apparent that the Strategic and Operating Plans (SOP) were informed by the IS-SSR Framework and include SSR priorities, objectives, and activities. SSR-related activities are reported on regularly as part of SOP, including in ICANN's regular portfolio management reporting[130] and SSR quarterly reports.[131] The process for updating SSR-related documents has been redesigned, and the SSR mission and approach was published in 2015. However, there is a lack of community input and a clear framework of how strategy informs SSR activities. Clear frameworks and objective setting are key tools needed to attain security and resiliency goals. While specific and implementation-related planning is likely well-served by specialists, the community should be able to provide input into these key strategies, as they relate strongly to ICANN's core mission. Therefore, further work is needed.

[130] "ICANN Strategic Plan for Fiscal Years 2021 – 2025," ICANN, last updated 29 March 2019, https://www.icann.org/public-comments/strategic-plan-2018-12-20-en.

[131] 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.

Rationale:

- Strategic planning for security, stability, and resiliency issues appear to be centered on the Office of the CTO (OCTO), and it is apparent that a level of planning exists within the OCTO. However, the level of detail and planning envisioned in the recommendation does not seem to be provided in public discussions. Furthermore, there remains no obvious way for the ICANN community to provide input on the objectives, initiatives, and priorities of activities related to SSR beyond high-level documents.

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**: This recommendation remains relevant today. As with SSR1 Recommendation 7, the ICANN community has regular opportunities to comment and discuss priorities and objectives at a high level, as published in its strategic plan. The chief concern is the level of detail related to SSR activities. The Strategic and Operating Plans (SOP) were informed by the IS-SSR Framework and reflect SSR priorities, objectives, and activities. However, 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. It would be useful to undertake a more detailed and public objective setting with prioritization done via public, community input processes. Furthermore, these objectives would have to be written in a way that allows them to feed into applicable and measurable SSR activities.

Rationale:

- Available documents indicate that SSR guidance is included and addressed in relevant reports, strategies, and procedures. However, available reports do not provide sufficient insight into SSR activities and lack detail regarding the implementation and the execution of SSR activities. While advisory committees, namely SSAC and RSSAC, exist, there is little opportunity for other parts of the community to provide input (or even learn about SSAC input) on the objectives, initiatives, and priorities of activities related to SSR.

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.

Specific guidance regarding additional action on this recommendation is offered in Section "SSR1 Recommendation 9 - Information Security Management Systems and Security Certifications".

SSR2 Conclusion: This recommendation remains relevant and was not fully implemented. 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. 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. ICANN org also reports that all information security staff are trained using SANS offerings. Lastly, ICANN org reports that the outcomes of internal audits are reported to the Board only. Thus, ICANN org has not published a document that could be used as a roadmap for SSR process certification, making community review impossible. Therefore, it is not apparent how ICANN org assessed certification options as a result of SSR1. In any case, ICANN org has not published “a clear roadmap towards certification.”

ICANN may find it useful to create a road map of what certification activities are being undertaken and what certifications ICANN is aiming to achieve. ICANN should also provide reasoning for their choices, demonstrating how they fit into its security and risk management strategies. The road map would communicate expectations for organizational and individual audits and certifications and explain how their expectations and plans are appropriate. For example, ICANN org should explain which certifications or training are relevant to which roles in the organization and track completion rates.

Rationale:

- While ICANN org has undertaken some steps towards certification, a clear roadmap and an overarching strategy are not apparent. This conclusion was reached by assessing publicly available material and submitting questions to ICANN staff. At this point in time, ICANN org has undertaken various steps towards training staff, and in some cases, pursued organizational certifications. While the recommendation calls for a “clear roadmap,” there is no evidence available publicly or to the SSR2 RT that such a roadmap has been created. ICANN org seems to follow an ad hoc approach, rather than organizing and tracking its activities in this area. Besides, ICANN org has not followed industry best practice, e.g., by not rotating auditors regularly, and has failed to demonstrate that all certification activities feed into relevant risk and information security frameworks and strategies.
- While ICANN org runs specific infrastructure that some standards might struggle to capture appropriately, there is value in pursuing individual and organizational certifications, particularly if these goals are organized and planned appropriately. Therefore, this recommendation is still relevant, and further work is needed. ICANN org can, and should, be audited and certified along the lines of various standards and should

assess certification options with commonly accepted international standards (e.g., ITIL, ISO, SSAE-16) for its operational responsibilities and report on their procedure and the standards' suitability. ICANN org should publish a clear roadmap towards achieving relevant certifications.

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: There is no doubt that ICANN Compliance has stepped up considerably since 2011 (when the SSR1 recommendations were made). ICANN now produces monthly reports about its compliance enforcement work. However, it is not clear the extent to which SSR issues are handled within the compliance process. Note that more than 80% of complaints against registrars in August 2018 related to WHOIS inaccuracy.[132]

Further work would be to drill down into greater detail on specific security, stability, and resiliency issues such as those outlined in ICANN org's SLA monitoring system, along with details on follow-up and any enforcement action. Additional recommendations around Compliance and Enforcement are available in Workstream 3: Abuse and Compliance.

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.[133] Regular public reporting of compliance activities 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 13-month period; and metrics and data as explicitly requested by different working groups. Some Compliance auditing and outreach programs are now in place. New positions in ICANN org were created after the SSR1 Review to ensure the fulfillment of goals and objectives in this area.
- Complaints mechanisms were updated by migrating to the ICANN org website, automating, and launching a bulk complaint tool. Additionally, a Pulse Survey was implemented. With specific respect to WHOIS, an inaccuracy qualities check was

[132] ICANN Contractual Compliance Dashboard for August 2018, ICANN, August 2018, https://features.icann.org/compliance/dashboard/0818/report.

[133] The SSR1 implementation report is available at https://community.icann.org/download/attachments/54691765/SSR%20Recs%201-28.pdf?api=v2 (slides 28-30) 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.

launched. WHOIS accuracy reporting has been underway since the 2012 WHOIS Review Team recommended the action.

- While acknowledging the efforts made, there still is work to be done to fully implement this recommendation. For instance, compliance enforcement reports for 2017 and 2016 contain little evidence of SSR enforcement actions. However, the new gTLD base registry agreement (July 2017) contains specific obligations on contracted parties relating to security and stability and may assist further implementation.[134] It still remains unclear 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 Services, Registry Services, the DNS, or the Internet.
- Despite other requirements for Compliance improvements, such as those arising from the first WHOIS Review, and the Accountability and Transparency Review Team's (ATRT) first and second reports advocating a strengthening of ICANN Compliance, much improvement work remains to be done.

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: While actions have been taken to mitigate domain name abuse, the implementation did not have its intended effect. SSR1 Recommendation 11 was aimed at embedding SSR considerations into the expansion of the DNS space (either through the new gTLD program or the ccTLD IDN Fast Track[135]) through appropriate metrics and risk mitigation measures. No measures for success, including measurements for the effectiveness of mechanisms to mitigate domain name abuse, have been defined in a document that has community consensus.

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. Coordinated vulnerability disclosure reporting would be an excellent project for ICANN org to progress. It is difficult to assess the status of this initiative as the link included in the staff report goes to a document from

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

[135] "IDN ccTLD Fast Track String Evaluation Request System," ICANN, accessed on 27 December 2019, https://forms.icann.org/en/idn.

2013. Also, a clear communication plan on how it reports this to the community-at-large would be a useful tool as well.

Rationale:

- No measures for success, including measurements for the effectiveness of mechanisms to mitigate domain name abuse, have been defined in a document that has community consensus. This lack of measurable criteria has also been noted in the recent CCT's report and recommendations[136]. It appears that despite the new gTLD and IDN fast track programs that have been in existence (or in an advanced planning stage) since the SSR1 report was published, the SSR objectives required by SSR1 Recommendation 11 remain 'to be defined'.
- 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. Unfortunately, no metrics for evaluating compliance with these obligations appear to exist.
- Security and stability reviews under the IDN ccTLD Fast Track process[137] have been ineffective. All applications that have passed through the security and stability panel have been found not to create a technical SSR risk. The Extended Process Similarity Review Process (EPSRP) mechanism in the staff report has been criticized by community members and ICANN staff as expensive and ineffective.[138]

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.

Specific guidance regarding additional action on this recommendation is offered in Section "SSR1 Recommendations 12,15, and 16 - SSR Strategy and Framework, Metrics, and Vulnerability Disclosures."

SSR2 Conclusion: SSR1 Recommendation 12 remains particularly relevant today. Cybersecurity threats are becoming more acute, and several countries are now adopting specific cybersecurity strategies. Maintaining and improving the security, stability, and resiliency

[136] "Competition, Consumer Trust, and Consumer Choice: Final Report," https://www.icann.org/en/system/files/files/cct-rt-final-08sep18-en.pdf

[137] "IDN ccTLD Fast Track String Evaluation Request System," https://forms.icann.org/en/idn.

[138] Working Group EPSRP, ICANN ccNSO, accessed on 27 December 2019, https://ccnso.icann.org/en/workinggroups/epsrp.htm.

of the domain name system is a limited but essential part of ensuring the security and stability of the entire network. This recommendation appears to have driven ICANN SSR Team—now ICANN OCTO SSR Team—to continue to build their engagement both on an individual networking level, and to engage heavily with ICANN's GSE (Global Stakeholder Engagement) department. The OCTO Team has worked with GSE since this recommendation. This SSR1 Recommendation has had partial implementation through the accumulation of other initiatives in OCTO. It is not apparent that any attempt was made to implement the specific goals of this Recommendation.

In addition, 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.

Further work is needed to fulfill the objectives of the recommendation and bring ICANN org forward to a proactive position in working through the community to improve SSR. ICANN org should work with the community to identify SSR-related best practices, and then implement the practices through contracts, agreements, MOUs, and other mechanisms.

Rationale:

- While SSR-related interactions with SOs and ACs are documented through the regular ICANN org processes, they are not flagged in any way beyond meetings at ICANN being labeled as of interest for those in the community with a security interest. One such effort could be OCTO SSR team member participation in the ccNSO TLD-OPS discussions list, but again, these are not documented by the OCTO SSR team.
- The report entitled "Identifier System Attack Mitigation Methodology" is dated February 2017.[139] The paper sets out suggestions said to have been generated 'within ICANN and by Identifier System security experts throughout the Community.' However, it is not clear what process was followed in arriving at the best practices set out in the document. In any event, 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 that has been put forth for consideration within ICANN. 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 resource locator page linked to has not been updated since 2014. The 'additional information' links to the SSR annual reports page (which does not mention best practices, at least on its face), and the other link does not resolve.

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

- SSR2's review found no evidence of staff periodically informing SO/ACs of best practices or inviting them to identify additional best practices.
- Another deliverable is that staff is to address SSR-related responsibilities and best practices in Regional Engagement Strategies. In examining the ICANN org Middle East Engagement Strategy, a single action is related to SSR initiatives: conducting contingency and coordination exercises to prepare for threats to DNS and prepare CERTs.[140] In the Latin American and Caribbean Strategy document only action 2.2.1 (a roadshow) is related to SSR.[141] In the African Strategic Plan, two strategic projects touch on SSR: project 2, Developing and Improving African Expertise; and project 4, encouraging resiliency of local DNS infrastructure.[142] While these appear in the Regional Engagement Strategy documents – and while the IS-SSR team reports on meetings in these regions – it is not evident that the outreach being done by the IS-SSR team is a coordinated response to strategic regional engagement documents.
- 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 is an advisory from APWG on "What to Do if Your Website Has Been Hacked by Phishers," but it was produced prior to SSR1. Other than Phishing Trends Surveys and Reports, APWG does not seem to have released a new recommendation or report from its Internet Policy Committee. While there is a report from the 4th Global DNS Stability, Security and Resiliency Symposium held in Puerto Rico in 2012, the ICANN web site does not appear to have a set of recommendations for web application protection and development of resources for security awareness.[143]

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—SSR objectives need to be followed and applied throughout ICANN org in order to be effective—but is not measurable. Work is reported to be ongoing within ICANN org, though only one example of a successful publication was found from 2012.[144] The SSR2 RT recommends ICANN to develop a concise

[140] MEAC Strategy Working Group (MEAC-SWG), ICANN Middle East Working Group, last modified 4 November 2019, https://community.icann.org/pages/viewpage.action?pageId=59642230.

[141] "LAC Year in Review 2017," ICANN Engagement Center for Latin America and the Caribbean, 2017, https://www.icann.org/en/system/files/files/lac-year-in-review-2017-en.pdf.

[142] Pierre Dandjinou, Yaovi Atohoun, Bob Ochieng, "Five Years of Africa Strategy Implementation 2012-2017," ICANN, 3 May 2018, https://www.icann.org/en/system/files/files/africa-strategy-implementation-2012-2017-03may18-en.pdf.

[143] "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.

[144] "Identifier Systems Security, Stability and Resiliency (IS-SSR)," ICANN, 24 November 2014, https://www.icann.org/resources/pages/is-ssr-2014-11-24-en.

and consistent process that helps all SO/AC to develop and implement a model for publishing SSR-related best practices. ICANN org should document and report all such efforts made in this respect.

Rationale:

- ICANN org considers work on this recommendation ongoing and reports as part of the Strategic and Operating Plan (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 RT cannot assess if this recommendation was implemented, as there is no available evidence whether this was done or not. 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 Organization." 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. The SSR communities are a non-stationary set and are always evolving; staying in-step and plugged in with them is critical. Having some machinery in place that tracks communities and assesses their relevance to ICANN org's SSR is an important ongoing activity that does not appear to be addressed.

Rationale:

- The Engagement Interface (https://features.icann.org/events-near-you) did not directly address how the outreach activities "evolve" to remain relevant. 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.

Specific guidance regarding additional action on this recommendation is offered in Section "SSR1 Recommendations 12,15, and 16 - SSR Strategy and Framework, Metrics, and Vulnerability Disclosures"

SSR2 Conclusion: The motivations behind SSR1 Recommendation 15 remain relevant today. The SSR2 RT considers it necessary for ICANN org to provide an appropriate and proportionate level of insight into the vulnerability disclosure process and its efficacy. 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. Therefore, while a process exists "on paper," it is not possible to assess if that process is functional and effective. ICANN org should provide anonymized metrics of the vulnerability disclosure process on a regular and timely basis.

Rationale:

- ICANN org has implemented a Vulnerability Disclosure Program for ICANN's public-facing assets. 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).
- 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.

Specific guidance regarding additional action on this recommendation is offered in Section "SSR1 Recommendations 12,15, and 16 - SSR Strategy and Framework, Metrics, and Vulnerability Disclosures"

SSR2 Conclusion:
This recommendation remains relevant and was only partially implemented.   The SSR space is very dynamic and needs to support both evolution and maintenance. New and relevant actors are appearing regularly and should be engaged. It seems that the ongoing involvement in related communities has accomplished the "participation" objective, but it is not clear how information is "systematic[ally]" incorporated. This recommendation envisions greater public engagement with SSR initiatives, including the Frameworks and Annual Reports. This recommendation resulted in no obvious changes to the way the IS-SSR Framework and Annual

Reports are created. It is not readily apparent how changes to the organization or processes related to SSR activities have expanded participation and input.

ICANN org needs to develop an overarching SSR strategy that includes measurable or trackable objectives on the acquisition of external feedback and outreach to relevant non-community as well as community stakeholders. This should incorporate some of the observations made under the review of previous recommendations.

Rationale:

- 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.
- There is no evidence of a process for “systematic[ally]” incorporating other ecosystem participants.
- The recommendation specifically asks for a more systematic process for getting input from other ecosystem participants. This makes the final deliverable seem out of place.
- The Implementation Report says that staff would “support a variety of capability building initiatives by the Security Team.” It is not immediately evident how these capability-building initiatives would affect greater engagement in the development of the IS-SSR Frameworks or Annual Reports. It is also not evident from the public record what those capability building initiatives were or when they were conducted.

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:

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.

Clear processes for SSR-related issues remain relevant. Like other SSR1 Recommendations where the target was greater community participation in the development of objectives and priorities, SSR1 Recommendation 17 requires better metrics for evaluating the success of the implementation, processes for community integration and feedback, and finally, a clear relation to strategic plans, policies, and goals.

Rationale:

- The most recent Annual Report 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 obvious. 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 RT. 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. Due to a lack of trackable indicators, the status of implementation is impossible to ascertain from publicly available materials.

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: On the surface, this has been completed annually except for FY15-16. The team cannot assess the status of FY18, since it is not yet on the web site. However, 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. While this may be taking place informally, there is no public reporting or mechanism for input on an SSR-related operational review.

Rationale:

- While there might be an informal or undocumented internal process, the implementation did not provide 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. There may be data available that could be used to support the implementation of SSR1 Recommendation 19, but the formal process was never initiated in this regard except publishing the annual IS-SSR framework. Hence, the RT concludes that the intended effect has not been achieved since there currently is no mechanism to track the implementation of the IS-SSR Framework effectively. As in other SSR1 Recommendations, this remains relevant for the purposes of transparency and accountability of the ICANN organization. As with a number of other SSR1 Recommendations, a functional procedure and reporting structure needs to be developed and implemented with community feedback and should be accessible to the community.

Rationale:

- ICANN org reports that the publication of the annual IS-SSR Framework[145] 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.
- The SSR2 RT also notes that SSR1 Recommendation 19 suggested that information be provided information with "enough clarity." However, this does not seem to be measurable in its entirety.

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.

Specific guidance regarding additional action on this recommendation is offered in Section "SSR1 Recommendation 20 and 22 - Budget Transparency and Budgeting SSR in new gTLDs"

SSR2 Conclusion: This recommendation was partially implemented, and, for the purposes of transparency and accountability, continues to have relevance today. SSR-related activities do appear in ICANN's annual budget but at a very high level. SSR1's Recommendation 20 seems to have intended a greater degree of granularity for examination and public comment on SSR-related budget items. The implementation did not have the full, intended effect. The assessment was conducted based on publicly available information, the SSR1 implementation report, and an SSR2 briefing. ICANN org should increase the transparency of information about the

[145] IS-SSR Document Archive, ICANN, accessed 27 December 2019, https://www.icann.org/ssr-document-archive.

organization and the budget related to implementing the IS-SSR Framework and performing SSR-related functions.

Rationale:

- The SSR1 implementation report is available here (slides 58-60), and the SSR2 RT briefing on this recommendation here (slides 30-37). Work was done in two phases. Phase I included a planning framework and process 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. Periodic SSR activity reporting augments this public information.[146] 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 here.
- Staff also developed an after-event-report that includes budget and resource impacts related to managing an event. No after-event reports have been published yet, although they should be published annually starting FY18. A template for a public version of these reports can be found here. ICANN also publishes an information security event log here.
- ICANN org reported that the department spending on the Emergency Back-end Registry Operator (EBERO) provider for FY17 totaled $2.3m, and supported work on the following items: data escrow services ($930k); WHOIS studies (ARS design/analysis, parsing, accuracy testing, ARS phase 3; $638k); EBERO services ($353k); Background checks for registrar accreditation ($100k); and miscellaneous or smaller items ($300k).
- Annual reporting on SSR-related activities does take place in the Framework documents and Annual Reports. However, the very high-level budget line items should be accompanied by greater specificity and inclusion in ICANN's regular project management reporting to improve transparency. 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 staff implementation report says that ICANN will "Integrate SSR Framework and reports on SSR activities and expenditures into planning framework and process to provide public information about SSR-related plans, budgets and activities." 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. Unfortunately, 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

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

expenditures across multiple ICANN departments," indicating a further work is needed 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.

SSR2 Conclusion: This is very similar to SSR1 Recommendation 20; the SSR1 findings about the budget process made in SSR1 Recommendation 20 above are equally applicable here.

The SSR1 Recommendation calls for a more structured internal process for showing how the organization and budget decisions relate to the IS-SSR Framework, including the underlying cost-benefit analysis. While there is more information available, the goal of the SSR1 Recommendation was a mechanism for showing, specifically, how organizational and budgetary decisions relate to the IS-SSR Framework; this has either not been done or is not visible to the ICANN community.

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; and
    - 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. The link to the template does not resolve. 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 as, as yet, 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. In fact, 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.

Specific guidance regarding additional action on this recommendation is offered in Section "SSR1 Recommendation 20 and 22 - Budget Transparency and Budgeting SSR in new gTLDs"

SSR2 Conclusion:
This is very similar to SSR1 Recommendations 20 and 21. The difference is that the documentation requested is the budget, resources, and activities related to SSR impacts of the new gTLD program. The staff report simply echoes the previous deliverables (for SSR1 Recommendations 20 and 21) without providing any evidence or any specific work related to the new gTLD program. Thus, in the staff report for implementation, there is no new information that would help determine if this Recommendation was implemented. Like SSR1 Recommendations 20 and 21, for the purposes of transparency and accountability, the recommendation continues to have relevance today.

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

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 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 September 30, 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: It is not clear that this recommendation was implemented. While the recommendation remains relevant, it is unclear how to assess this recommendation given the wording. The recommendation requires reconceptualization, as described in the Rationale below. A recommendation related to this topic included later in the report.

Rationale:

- The SSR1 report provided a few examples of SSR-related WGs within ICANN (the Board DNS Risk Management Working Group and the DNS Security and Stability Analysis Working Group (DSSA-WG) specifically). It also provided examples of two SSR-related Advisory Committees: SSAC and RSSAC.
- The DSSA-WG no longer exists, but there is a final report for this group.[147] Section 4 of that report talks about planned steps for the next phase of this work, but it is unclear as to whether those planned steps ever happened. It is also not clear whether that working group had the appropriate resources required to complete their work. The rest of this commentary will restrict itself to SSAC and RSSAC.
- 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 RT to the 2015 budget as an example.[148] 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

[147] "DNS Security and Stability Analysis Working Group (DSSA) Final Report," ICANN, November 2013, https://ccnso.icann.org/sites/default/files/filefield_42587/dssa-final-08nov13-en.pdf.

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

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:

> *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 precisely echoes circumstances and concerns over the last couple of years, especially in the context of the KSK roll in October 2018, during which SSAC struggled to be responsive to requests for advice on short time frames with inadequate data/research available to inform the debate.[149] 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 other 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 being subsidized by their employer for their time to participate (and thus not "free from external pressure"). The SSR2-RT does not believe that just throwing budget at the problem is sufficient to address this concern; rather, it will require a rethinking of the structure and expectations of not just these committees, but of ICANN itself.

- A concrete example is the recent NCAP activities, where SSAC proposed a $3M budget to outsource some research they thought would be needed, which the ICANN Board thought was too expensive, or at least did not have sufficient justification, because SSAC had not performed a gap analysis from previous studies, which itself is research that requires resources that SSAC does not have. In the case of NCAP, the work also required a level of independence that SSAC did not have since most members of the WG were in some way financially conflicted with the new gTLD program. Contributing to the challenge is the fact that ICANN's approach to self-managing conflict of interest is transparency (i.e., publishing "Statements of Interest") rather than follow a formal conflict-of-interest policy. This structure compromises the integrity of the work products since the balance of participation is weighted toward organizations with sufficient capital and financial incentive to participate, and there are no formal checks and balances to compensate.
- The lack of metrics and monitoring of success or failure of the new gTLD program indicates this multi-stakeholder approach is not "free of external pressures." The CCT RT report on DNS abuse in new gTLDs has found metrics to rigorously apply, through

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

which it is impossible to conclude that the 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.

- The SSR2 RT also notes that 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 deliberations are all confidential for security reasons.[150] The same appears true for RSSAC and RZERC, but in these two cases, the committees are architected such that each person represents a stakeholder. This structure is not a reliable recipe for ICANN to be in a position to "ensure" decisions are made in an objective manner, free from external or internal pressures. ICANN staff do participate in the SSAC and RSSAC, which provides visibility into the committee dynamics and an opportunity to identify and attempt to mitigate such pressures. It also bears noting that important stakeholders are consistently missing from these SSR2-related advisory committees (e.g., victims of identifier abuse, academic researchers, law enforcement, policymakers). This gap is not intentional, but it is by the nature of the charters of these groups, and it does affect the balance of pressures from various stakeholders.
- With respect to RSSAC, a review of RSSAC's operations occurred in 2017-2018 in accordance with ICANN's bylaws that also raised questions about RSSAC's accountability. The final report includes several recommendations relevant to this recommendation:[151]

> *Recommendation 2*
>
> *Resolve the apparent mismatch between the charter and operational procedures of the RSSAC and the requirements and expectations of the ICANN Board and Community for interaction with the root server system.* (The report footnotes that *"the publication of RSSAC037, "A Proposed Governance Model for the DNS Root Server System", (https://www.icann.org/resources/files/1216341-2018-06-15-en), is a clear and welcome first step in the direction suggested by this Recommendation."*)
>
> *Recommendation 3*
>
> *Formalize the responsibilities of the RSSAC to the ICANN Board and*

[150] "SSAC Operational Procedures Version 5.1," ICANN Security and Stability Advisory Committee, 27 February 2019, https://www.icann.org/en/system/files/files/operational-procedures-27feb18-en.pdf.
[151] "Independent Review of the ICANN Root Server System Advisory Committee (RSSAC) Final Report," https://www.icann.org/en/system/files/files/rssac-review-final-02jul18-en.pdf.

> *Community in a work plan that is periodically reviewed and published, and hold the RSSAC accountable for work plan deliverables.*
>
> *Recommendation 6*
>
> *Clarify the role and responsibility of the RSSAC with respect to other groups with adjacent or overlapping remits, including the SSAC, the RZERC, and the RSSAC Caucus.*

- RSSAC's June 2018 publication, "A Proposed Governance Model for the DNS Root Server System", mentioned above, would require significant resources to implement. It is not clear if or how ICANN intends to implement this model. RSSAC currently has similar technical staff support from ICANN as SSAC does.

SSR1 Recommendation 24

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

SSR2 Conclusion: To the extent that the articulation of roles and responsibilities were intended to enable community understanding and evaluation of ICANN's SSR activities, this description of roles and responsibilities is too vague to support such understanding. The SSR2 RT recommends that this list include a set of metrics by which one could evaluate progress on execution of these responsibilities, as well as periodic (at least annual) reports that report these metrics and provide details on SSR2-related accomplishments within ICANN. The SSR2 RT believes that ICANN should staff a full-time person that will coordinate across all SSR-related constituencies: Compliance, CCT, GDD. Details on this recommendation are covered in the SSR2 Recommendation "C-Suite Security Position."

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.[152] The web page for this team describes the mission of this team in high-level terms, and links to a page of SSR "activities."[153] 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:

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

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

  - 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, multi-stakeholder effort to improve cybersecurity and mitigate cybercrime.
- The 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: A regular review of near and long-term SSR-related risks remains relevant. While some material about near and long-term risk related to SSR is published, the mechanism for feeding this information into ICANN’s Strategic Plans is not obvious. It is necessary to consider the mechanisms to support a regular review of near- and long-term SSR-related risks. In particular, ICANN org must pay attention to how risk identification is performed and how findings would translate or feed into relevant policies and risk management frameworks. This recommendation is expanded in more detail in the SSR2 Recommendation “Security Risk Management.”

Rationale:

- A Risk Management Framework was accepted by the 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 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 correlates to SSR1 Recommendations 25 and 27 but is not relevant today. Rather than a timely completion, it is important for risk management practices and procedures to stay up to date, and for it to be reviewed regularly by the community, and findings and recommendations feed back into the Risk Management Framework. Furthermore, procedures that ensure measures are tracked and reviewed should be established, as discussed in SSR1 Recommendation 25.

Rationale:

- A Risk Management Framework was accepted by the board in 2013,[154] having received community input during ICANN50 and ICANN51. A more detailed response for this recommendation is addressed under the assessment for Recommendation 27.
- Notably, given that the term "timely" does not a connate any specificity in what was intended or acceptable, it cannot be assessed if the intended effect was achieved.

SSR1 Recommendation 27

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

Specific guidance regarding additional action on this recommendation is offered in Section "SSR1 Recommendation 27 - Risk Management."

SSR2 Conclusion: This review is still relevant. The SSR2 noted that there is a correlation between SSR1 Recommendations 25, 26, and 27. During the review, the SSR2 RT concluded that there is a Risk Management Framework in place. However, in the absence of a definition of "comprehensive" by SSR1 or metrics for evaluation, it was very difficult to assess whether this recommendation has been fully implemented.

The SSR2 RT recommends evaluating this recommendation against more specific language that captures the original intent of SSR1: If one were to rephrase this Recommendation, the SSR2 RT believes what was meant was '*ICANN's Risk Management Framework should be clearly articulated, aligned strategically against the requirements and objectives of the Organization, describe relevant measures of success and how these are to be assessed.'*

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

The SSR2 RT also notes the conclusion of the DNS Risk Framework Working Group, its report, and the 2016 IS-SSR Framework for FY 15-16.[155,156] ICANN org should consider these documents when developing the Risk Management Frameworks.

Rationale:

- In doing the review, the SSR2 RT discussed, among other things, 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 RT 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 RT 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.
- 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.
- The SSR2 RT also took note of the conclusion of the DNS Risk Framework Working Group and its report and the 2016 Identifier Systems Security, Stability and Resiliency Framework – for FY 15-16 and recommends that these be taken into account as resource documents for the development of any Risk Management Frameworks.[157, 158]

[155] "DNS Security and Stability Analysis Working Group (DSSA) Final Report," https://ccnso.icann.org/sites/default/files/filefield_42587/dssa-final-08nov13-en.pdf.

[156] "Identifier Systems Security, Stability and Resiliency Framework–FY 15-16", https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf.

[157] "DNS Risk Management Framework Report," https://www.icann.org/public-comments/dns-rmf-final-2013-08-23-en.

[158] "Identifier Systems Security, Stability, and Resiliency Framework – FY 15-16", https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf.

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 today and is related to SSR1 Recommendations 15 and 24. While the SSR2 RT is confident that the OCTO SSR team plays a coordinating role in distributing threat intelligence to involved parties and regularly engages with law enforcement, there is little or no public evidence that this has occurred. Furthermore, 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 conducts threat detection, including SSAC, RSSAC, TLDOPS, ccNSO incident response WG, and PSWG. The OCTO SSR team coordinates with these groups.

Rationale:

- The SSR2 RT 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.

Appendix E - Bylaws and Strategic Plan sections most relevant to SSR2 Recommendations

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

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

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

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

2.1. Address the increasing needs of inclusivity, accountability and transparency, while at the same time ensuring that work gets done and policies are developed in an effective and timely manner
2.2 Strengthen ICANN's multistakeholder decision-making process.
2.3 Strengthen the inclusivity and openness of ICANN's multistakeholder model by improving and sustaining diverse representation and active, effective participation.

3. Strategic Objective: Evolve the unique identifier systems to continue to serve the needs of the global Internet user base.

3.1 Encourage readiness for Universal Acceptance, IDN implementation, and IPv6 by increasing awareness to enable more end users to use the Internet.
3.2 Improve understanding of and responsiveness to new technologies by greater engagement with industry, academia, standards development organizations, and other relevant parties.
3.3 Continue to deliver and enhance the IANA functions with operational excellence. 3.4 Plan a properly funded, managed, and risk-evaluated new round of gTLDs.

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

4.1 Further develop early warning systems, such as ICANN org's Legislative/Regulatory Development Reports, to identify and address global needs and threats, demonstrating ICANN's trustworthiness in resolving the challenges within its remit in a timely manner.

4.2 Continue to build alliances in the Internet ecosystem and beyond to raise awareness, and equip stakeholders from around the world to become active participants in ICANN's policy making.

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

5.1 Enhance ICANN's understanding of the domain name marketplace.
5.2 Strengthen cost management and financial accountability mechanisms.
5.3 Enhance ICANN's financial planning model to better balance economic changes and stakeholders' needs.

Appendix F: 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[159], and mobile malware attacks nearly doubled from 2017 to 2018 to over 116 million[160].
- Digital Certificate Fraud: APWG reports that phishers are increasingly using digital certificates to make attacks look legitimate and to defeat browser fraud detection warnings.[161] 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.[162]
- 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.

[159] AMR, "Kaspersky Security Bulletin 2018: Statistics," 4 December 2018, https://securelist.com/kaspersky-security-bulletin-2018-statistics/89145/.

[160] Victor Chebyshev, "Mobile Malware Evolution 2018," 5 March 2019, https://securelist.com/mobile-malware-evolution-2018/89689/.

[161] APWG, "APWG Phishing Activity Trends Report 3rd Quarter 2018," 11 December 2018, https://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf.

[162] 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.

> "*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."*[163]

- Business Email Compromise: The US 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 United 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.[164]
- 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 AU$11.8 million in losses in 2019.[165] Domain names used to perpetrate online scams very typically infringe on brand or business name. Scammers register these names with little or no controls 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.[166] 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.[167]
- 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.[168]

> *"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*

[163] APWG Phishing Activity Trends Report 3rd Quarter 2018.

[164] "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.

[165] ScamWatch, Australian Competition and Consumer Commission, https://www.scamwatch.gov.au/about-scamwatch/scam-statistics.

[166] "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.

[167] "Spamhaus Botnet Threat Report 2019," Spamhaus Malware Labs, n.d., https://www.spamhaustech.com/botnet-threat-report-2019/

[168] "Email and Spam Data," Cisco Talos Intelligence Group, https://www.talosintelligence.com/reputation_center/email_rep.

> *techniques, such as phishing and malicious links and attachments, adversaries need only to sit back and wait for unsuspecting users to activate their exploits."*[169]

- DDoS Attacks: Distributed denial of service (DDoS) attacks increased by 40% from mid-2017 to mid-2018.[170] 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.[171] 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.[172] Additionally, the "Internet of Things" (IoT) is a growing concern for DDoS attacks because these connected 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.[173]

From reports, it is evident that some accredited registrars established a practice to process domain registrations by the thousands that are then used for many of the criminal activities highlighted earlier.[174] Alpnames, among the most egregious registrar as highlighted by the CCT Review report, offered cheap bulk registrations and at times over 80% of its portfolio was identified as abusive domains.[175] ICANN Compliance failed to address this ongoing, systemic abuse. After ICANN org became aware of the "discontinuance of [Alpnames] operations," ICANN Compliance de-accredited it and simply transferred the abuse-laden portfolio to other registrars. Abuse-harboring registrars are not an anomaly. Spamhaus (among others) tracks the most abused registrars, and certain registrars have been repeatedly identified year after year.

Spamhaus (among others) tracks the most abused TLDs registries manage, and certain registries have been repeatedly identified year after year.

[169] "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.

[170] "H1 2018 DDOS Trends Report," Corero Network Security, n.d., https://info.corero.com/report-2018-half-year-ddos-trends-report-download.html.

[171] 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.

[172] "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/.

[173] 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.

[174] ICANN, "Statistical Analysis of DNS Abuse in gTLDs (SADAG) Report," 13 October 2017, https://www.icann.org/public-comments/sadag-final-2017-08-09-en.

[175] ICANN CCT Review Team, "Competition, Consumer Trust, and Consumer Choice Review," September 2018, p 96, https://www.icann.org/en/system/files/files/cct-final-08sep18-en.pdf.

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

#	Recommendation	Strategic Objective and Goal
1	Complete the implementation of all relevant SSR1 recommendations.	Strategic Objectives 1,2, and 3
2	SSR1 Recommendation 9 - Information Security Management Systems and Security Certifications	Strategic Objective 1
3	SSR1 Recommendations 12,15, and 16 - SSR Strategy and Framework, Metrics, and Vulnerability Disclosures	Strategic Objectives 1, 2, 3, and 4; and Strategic Goals 1.1, 1.2, 1.3, and 4.1
4	SSR1 Recommendation 20 and 22 - Budget Transparency and Budgeting SSR in new gTLDs	Strategic Objectives 1, 2, 3, and 5; and Strategic Goals 2.1 and 3.4
5	SSR1 Recommendation 27 - Risk Management	Strategic Objectives 1, 4 and 5
6	Create a Position Responsible for Both Strategic and Tactical Security and Risk Management	Strategic Objectives 1, 3, and 4
7	Further Develop a Security Risk Management Framework	Strategic Objectives 1, 2, 3, 4, and 5
8	Establish a Business Continuity Plan Based on ISO 22301	Strategic Objectives 1,3, potentially 4.
9	Ensure the Disaster Recovery Plan is Appropriate, Functional, and Well Documented	Strategic Objectives 1, 3, and 4; and also Strategic Goals 1.1, 1.4, and 3.3
10	Improve the Framework to Define and Measure Registrar & Registry Compliance	Strategic Objective 1; and Strategic Goals 1.1, 1.3, and 3.3
11	Lead Efforts to Evolve Definitions Around Abuse and Enable Reporting Against Those Definitions	Strategic Objective 1; and Strategic Goals 1.1, 1.3, and 3.3
12	Create Legal and Appropriate Access Mechanisms to WHOIS Data	TBD
13	Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program	Strategic Objectives 1, 2, 3, 4, and 5
14	Enable Rigorous Quantitative Analysis of the Relationship Between Payments for Domain Registrations and Evidence of Security Threats and Abuse	Strategic Objectives 1 and 3; and Strategic Goals 1.1, 1.2, 1.3, and 1.4

15	Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse	Strategic Objectives 1 and 3; and Strategic Goals 1.1, 1.2, 1.3, and 1.4
16	Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats	Strategic Objectives 1 and 3; and Strategic Goals 1.1, 1.2, 1.3, and 1.4
17	Establish a Central Abuse Report Portal	Strategic Objectives 1 and 3; and Strategic Goal 2.1
18	Ensure that the ICANN Compliance Activities are Neutral and Effective	Strategic Objectives 1, 2, and 3; and Strategic Goal 2.1
19	Update Handling of Abusive Naming	Strategic Objective 1
20	Complete Development of a DNS Regression Testing	Strategic Objective 1; and Strategic Goals 1.1, 1.2, 1.3, and 1.4
21	Implement the Recommendations from SAC063 and SAC073 and Establish Formal Procedures for Key Rollovers	Strategic Objectives 1, 2, and 4; and Strategic Goal 1.4
22	Establish Baseline Security Practices for Root Server Operators and Operations	Strategic Goals 1.1, 1.2, 1.4, and 3.3
23	Accelerate the Implementation of the New-Generation RZMS	Strategic Objective 1, and Strategic Goal 3.3
24	Create a List of Statistics and Metrics Around the Operational Status of the Unique Identifier Systems	Strategic Objectives 1, 2, 3, 4, and 5; and Strategic Goals 1.1, 1.2, 2.1, 3.2, 3.4, and 4.1
25	Ensure the Centralized Zone File Data Access is Consistently Available	TBD
26	Document, Improve, and Test the EBERO Processes	TBD
27	Update the DPS and Build Consensus Around future DNSKEY Algorithm Rollovers	Strategic Objectives 1 and 3
28	Develop a Report on the Frequency of Measuring Name Collisions and Propose a Solution	Strategic Objectives 1, 3, and 4; and Strategic Goal 3.4
29	Focus on Privacy and SSR Measurements and Improving Policies Based on Those Measurements	Strategic Objectives 1, 3, and 5
30	Stay Informed on Academic Research of SSR Issues and Use That Information to Inform Policy Debates	Strategic Objectives 1, 3, and 4; and Strategic Goal 3.2
31	Clarify the SSR Implications of DNS-over-HTTP	Strategic Objectives 1 and 3; and Strategic Goals 1.3 and 1.4