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

SSAC Meeting

11 February @ 15:00 UTC

ICANN

Security, Stability, and Resilience

SSR is one of 4 bylaw-mandated community reviews identified as key transparency and accountability safeguard post IANA transition

'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").' -- Section 4.6(c)

SSR Assessments **shall** include:

- the extent to which ICANN 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
- 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.

SSR Assessments **may** also include:

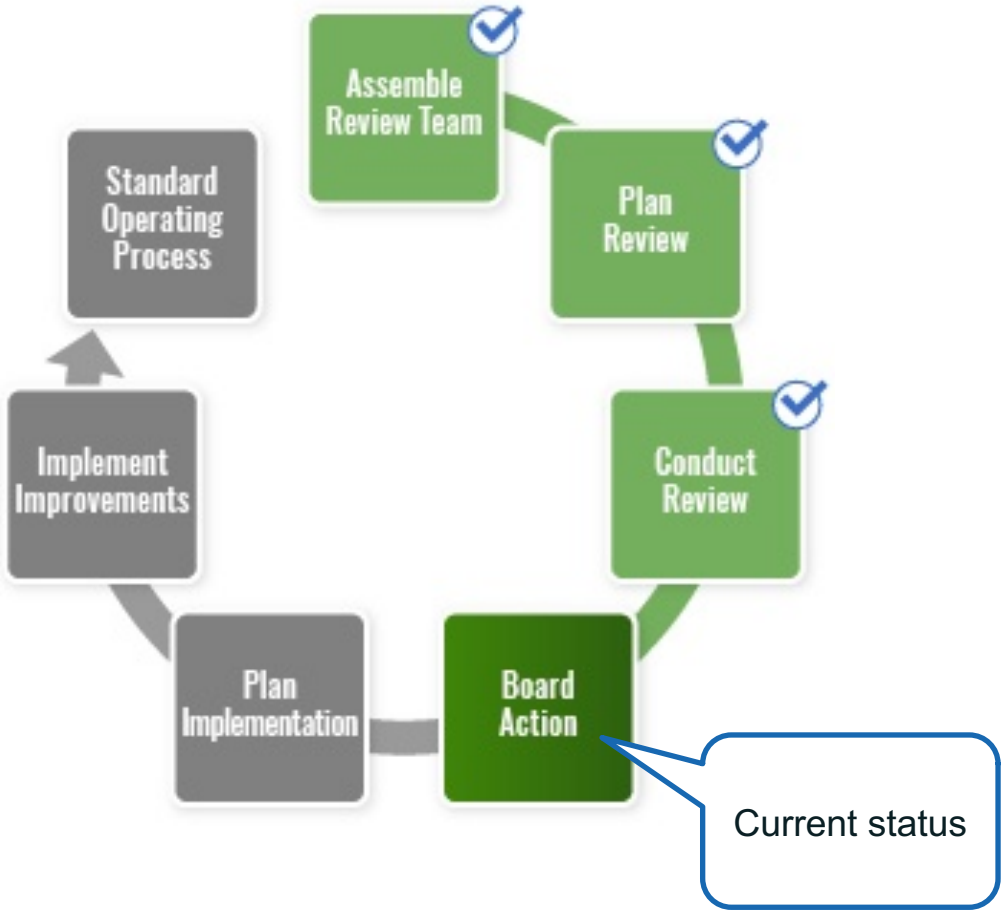
- security, operational stability and resiliency matters, both physical and network, relating to the coordination of the Internet's system of unique identifiers;
- conformance with appropriate security contingency planning framework for the Internet's system of unique identifiers; and
- maintaining clear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

SSR2 Review Team

RT Member	SO / AC Affiliation	Region
Alain Aina	ccNSO	AF
Noorul Ameen	GAC	AP
Kerry-Ann Barrett	GAC	LAC
KC Claffy	SSAC	NA
Russ Housley (Chair)	SSAC	NA
Danko Jevtovic	Board	EUR
Žarko Kecić	ccNSO	EUR
Boban Krsic	ccNSO	EUR
Jabhera Matogoro	ALAC	AF
Scott McCormick	GNSO	NA

RT Member	SO / AC Affiliation	Region
Denise Michel (Vice-Chair)	GNSO	NA
Eric Osterweil (Vice-Chair)	RSSAC	NA
Ramkrishna Pariyar	ALAC	AP
Rao Naveed bin Rais	GNSO	AP
Kaveh Ranjbar	Board	EUR
Norm Ritchie	GNSO	NA
Laurin Weissinger (Vice-Chair)	ALAC	EUR

Review Process



ICANN Strategic Plan

See:
https://www.icann.org/resources/pages/strategic-engagement-2013-10-10-en

SSR2 Recommendations are tied back to the 2021-2025 ICANN Strategic Plan

SSR2 RT Focus Areas

1

Workstream 1:

SSR1 implementation and impact

2

Workstream 2:

Key security, stability, and resiliency issues within ICANN

3

Workstream 3:

Security, stability, and resilience of the DNS

4

Workstream 4:

Future challenges

Public Consultation

Public Comment (24 January 2020 through 20 March 2020) resulted in 371 comments

https://www.icann.org/public-comments/ssr2-rt-draft-report-2020-01-24-en

Results

- Significant restructuring of the document
- Clarification and consolidation of many of the recommendations

Every comment received a response. See Appendix H in the final report for a link to the public comment response.

Final Report

Recommendations

- Recommendations are significantly revised and consolidated
- Recommendations are written according to the SMART criteria where possible: *specific, measurable, assignable, relevant, and trackable*.

  Making the recommendations fully SMART will require thought and action from the implementation.
- Total number of recommendations:

  24 groups of recommendations, resulting in 63 specific recommendations
- Full consensus achieved

Revised Document Structure

C. SSR1 Implementation (1 specific recommendation)

D. Key Stability Issues within ICANN (21 specific recommendations)

E. Contracts, Compliance, and Transparency around DNS Abuse (25 specific recommendations)

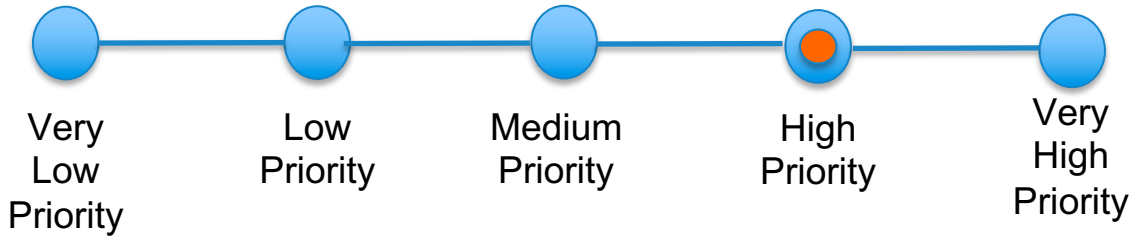
F. Additional SSR-Related Concerns Regarding the Global DNS (16 specific recommendations)

- Extensive Appendixes

Prioritization

- SSR2 RT members polled via Qualtrics for their inputs on recommendation priority

  Available scale: Very Low Priority, Low Priority, Medium Priority, High Priority, to Very High Priority.



- Of the 24 groups of recommendations

  27 specific recommendations = High

  9 specific recommendations = Medium-High

  18 specific recommendations = Medium

  8 specific recommendations = Low

SSR1 Implementation

SSR1 Implementation

- Bylaw-mandated goal: 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.*"
- All SSR1 recommendations remain relevant; none were implemented fully.
- SSR1 Recommendations were difficult to measure

SSR2 Rec 1: Further Review of SSR1

#	Recommendation	Owner	Priority
1.1	The ICANN Board and ICANN org should perform a further comprehensive review of the SSR1 Recommendations and execute a new plan to complete the implementation of the SSR1 Recommendations (see Appendix D: Findings Related to SSR1 Recommendations).	ICANN Board and ICANN org	Low

Key Stability Issues within ICANN

Key Stability Issues within ICANN

- Considered in this section:

  security, operational stability, and resiliency matters, both physical and network, relating to the coordination of the Internet's system of unique identifiers;

  security contingency planning framework for the Internet's system of unique identifiers;

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

- Resulting recommendations considered:

  Org structure

  Budgets and Reporting

  Risk management

  Business Continuity and Disaster Recovery

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

#	Recommendation	Owner	Priority
2.1	ICANN org should create a position of a Chief Security Officer (CSO) or Chief Information Security Officer (CISO) at the Executive C-Suite level of ICANN org and hire an appropriately qualified individual for that position and allocate a specific budget sufficient to execute this role's functions.	ICANN org	Medium-High
2.2	ICANN org should include as part of this role's description that this position will manage ICANN org's security function and oversee staff interactions in all relevant areas that impact security. This position should be responsible for providing regular reports to the ICANN Board and community on all SSR-related activities within ICANN org. Existing security functions should be restructured and moved organizationally to report to this new position.	ICANN org	Medium-High

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

#	Recommendation	Owner	Priority
2.3	ICANN org should include as part of this role's description that this position will be responsible for both strategic and tactical security and risk management. These areas of responsibility include being in charge of and strategically coordinating a centralized risk assessment function, business continuity (BC), and disaster recovery (DR) planning (see also SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures) across the internal security domain of the organization, including the ICANN Managed Root Server (IMRS, commonly known as L-Root), and coordinate with other stakeholders involved in the external global identifier system, as well as publishing a risk assessment methodology and approach.	ICANN org	Medium-High
2.4	ICANN org should include as part of this role's description that this role will be responsible for all security-relevant budget items and responsibilities and take part in all security-relevant contractual negotiations (e.g., registry and registrar agreements, supply chains for hardware and software, and associated service level agreements) undertaken by ICANN org, signing off on all security-related contractual terms.	ICANN org	Medium-High

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

- **Implemented**: ICANN org has created and filled the role of Chief Security Officer with responsibilities as defined in the recommendations.
- **Effective**: ICANN org centralizes security responsibilities such that ICANN org can demonstrably coordinate SSR activities and budget and speak to security issues at the appropriate management level.

SSR2 Rec 3: Improve SSR-Related Budget Transparency

#	Recommendation	Owner	Priority
3.1	The Executive C-Suite Security Officer (see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management) should brief the community on behalf of ICANN org regarding ICANN org's SSR strategy, projects, and budget twice per year and update and publish budget overviews annually.	ICANN org	High
3.2	The ICANN Board and ICANN org should ensure specific budget items relating to ICANN org's performance of SSR-related functions are linked to specific ICANN Strategic Plan goals and objectives. ICANN org should implement those mechanisms through a consistent, detailed, annual budgeting and reporting process.	ICANN Board and ICANN org	High
3.3	The ICANN Board and ICANN org should create, publish, and request public comment on detailed reports regarding the costs and SSR-related budgeting as part of the strategic planning cycle.	ICANN Board and ICANN org	High

SSR2 Rec 3: Improve SSR-Related Budget Transparency

- **Implemented**: when ICANN org moves all relevant functions and budget items under the new C-Suite position.
- **Effective**: ICANN community has a transparent view of the SSR-related budget.

SSR2 Rec 4: Improve Risk Management Processes and Procedures

#	Recommendation	Owner	Priority
4.1	ICANN org should continue centralizing its risk management and clearly articulate its Security Risk Management Framework and ensure that it aligns strategically with the organization's requirements and objectives. ICANN org should describe relevant measures of success and how to assess them.	ICANN org	High
4.2	ICANN org should adopt and implement ISO 31000 "Risk Management" and validate its implementation with appropriate independent audits. ICANN org should make audit reports, potentially in redacted form, available to the community. Risk management efforts should feed into BC and DR plans and procedures (see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures).	ICANN org	High

SSR2 Rec 4: Improve Risk Management Processes and Procedures

#	Recommendation	Owner	Priority
4.3	ICANN org should name or appoint a dedicated, responsible person in charge of security risk management that will report to the C-Suite Security role (see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management). This function should regularly update, and report on, a register of security risks and guide ICANN org's activities. Findings should feed into BC and DR plans and procedures (see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures) and the Information Security Management System (ISMS) (see SSR2 Recommendation 6: Comply with Appropriate Information Security Management Systems and Security Certifications).	ICANN org	High

SSR2 Rec 4: Improve Risk Management Processes and Procedures

- **Implemented**: ICANN org's risk management processes are sufficiently documented as per international standards (e.g., ISO 31000), and the organization has established a cycle of regular audits for this program that include the publication of audit summary reports.
- **Effective**: ICANN org has a strong, clearly documented risk management program.

SSR2 Rec 5: Comply with Appropriate Information Security Management Systems and Security Certifications

#	Recommendation	Owner	Priority
5.1	ICANN org should implement an ISMS and be audited and certified by a third party along the lines of industry security standards (e.g., ITIL, ISO 27000 family, SSAE-18) for its operational responsibilities. The plan should include a road map and milestone dates for obtaining certifications and noting areas that will be the target of continuous improvement.	ICANN org	High
5.2	Based on the ISMS, ICANN org should put together a plan for certifications and training requirements for roles in the organization, track completion rates, provide rationale for their choices, and document how the certifications fit into ICANN org's security and risk management strategies.	ICANN org	High

SSR2 Rec 5: Comply with Appropriate Information Security Management Systems and Security Certifications

#	Recommendation	Owner	Priority
5.3	ICANN org should require external parties that provide services to ICANN org to be compliant with relevant security standards and document their due diligence regarding vendors and service providers.	ICANN org	High
5.4	ICANN org should reach out to the community and beyond with clear reports demonstrating what ICANN org is doing and achieving in the security space. These reports would be most beneficial if they provided information describing how ICANN org follows best practices and mature, continually-improving processes to manage risk, security, and vulnerabilities.	ICANN org	High

SSR2 Rec 5: Comply with Appropriate Information Security Management Systems and Security Certifications

- **Implemented**: ICANN org has an ISMS oriented alongside accepted standards (e.g., ITIL, ISO 27000 family, SSAE-18), with regular audits that validate the appropriate security management and management procedures.
- **Effective**: ICANN org has an Information Security Management System that is thoroughly documented and adequately addresses current security threats and offers plans to address potential future security threats.

SSR2 Rec 6: SSR Vulnerability Disclosure and Transparency

#	Recommendation	Owner	Priority
6.1	ICANN org should proactively promote the voluntary adoption of SSR best practices and objectives for vulnerability disclosure by the contracted parties. If voluntary measures prove insufficient to achieve the adoption of such best practices and objectives, ICANN org should implement the best practices and objectives in contracts, agreements, and MOUs.	ICANN org	High
6.2	ICANN org should implement coordinated vulnerability disclosure reporting. Disclosures and information regarding SSR-related issues, such as breaches at any contracted party and in cases of critical vulnerabilities discovered and reported to ICANN org, should be communicated promptly to trusted and relevant parties (e.g., those affected or required to fix the given issue). ICANN org should regularly report on vulnerabilities (at least annually), including anonymized metrics and using responsible disclosure.	ICANN org	High

SSR2 Rec 6: SSR Vulnerability Disclosure and Transparency

- **Implemented**: ICANN org promotes the voluntary adoption of SSR best practices for vulnerability disclosures by contracted parties and implements associated vulnerability disclosure reporting.
- **Effective**: ICANN org and the contracted parties have adopted SSR best practices and objectives for vulnerability disclosure.

SSR2 Rec 7: Improve Business Continuity and Disaster Recovery Processes and Procedures

#	Recommendation	Owner	Priority
7.1	ICANN org should establish a Business Continuity Plan for all the systems owned by or under the ICANN org purview, based on ISO 22301 "Business Continuity Management," identifying acceptable BC and DR timelines.	ICANN org	Medium-High
7.2	ICANN org should ensure that the DR plan for Public Technical Identifiers (PTI) operations (i.e., IANA functions) includes all relevant systems that contribute to the security and stability of the DNS and also includes Root Zone Management and is in line with ISO 27031. ICANN org should develop this plan in close cooperation with the Root Server System Advisory Committee (RSSAC) and the Root Server Operators (RSO).	ICANN org	Medium-High
7.3	ICANN org should also establish a DR Plan for all the systems owned by or under the ICANN org purview, again in line with ISO 27031.	ICANN org	Medium-High

SSR2 Rec 7: Improve Business Continuity and Disaster Recovery Processes and Procedures

#	Recommendation	Owner	Priority
7.4	ICANN org should establish a new site for DR for all the systems owned by or under the ICANN org purview with the goal of replacing either the Los Angeles or Culpeper sites or adding a permanent third site. ICANN org should locate this site outside of the North American region and any United States territories. If ICANN org chooses to replace one of the existing sites, whichever site ICANN org replaces should not be closed until the organization has verified that the new site is fully operational and capable of handling DR of these systems for ICANN org.	ICANN org	Medium-High
7.5	ICANN org should publish a summary of their overall BC and DR plans and procedures. Doing so would improve transparency and trustworthiness beyond addressing ICANN org's strategic goals and objectives. ICANN org should engage an external auditor to verify compliance with these BC and DR plans.	ICANN org	Medium-High

SSR2 Rec 7: Improve Business Continuity and Disaster Recovery Processes and Procedures

- **Implemented**: ICANN org's BC and DR plans and processes are thoroughly documented according to accepted industry standards, including regular audits that those processes are being followed, and when a non-US, non-North American site is operational.
- **Effective**: ICANN org can demonstrate how they can handle incidents that impact the whole US or North America.

Contracts, Compliance, and Transparency around DNS Abuse

Contracts, Compliance, and Transparency around DNS Abuse

- Considered ICANN's role and influence regarding SSR in the global DNS
- Recommendations covered:
  - Unachieved Safeguards for the New gTLD Program
  - Challenges: Definitions and Data Access
  - PDP Alternatives
  - Privacy and Data Stewardship

SSR2 Rec 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties

#	Recommendation	Owner	Priority
8.1	ICANN org should commission a negotiating team that includes abuse and security experts not affiliated with or paid by contracted parties to represent the interests of non-contracted entities and work with ICANN org to renegotiate contracted party contracts in good faith, with public transparency, and with the objective of improving the SSR of the domain name system for end-users, businesses, and governments.	ICANN org	Medium

SSR2 Rec 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties

- **Implemented**: ICANN org has included abuse and security specialists in these negotiations and the management of the domain name system aligns with public safety and consumer interests, and not just those of the domain name industry.
- **Effective**: a broader and more balanced set of stakeholders are able to have direct input into the contracts negotiated with contracted parties.

SSR2 Rec 9: Monitor and Enforce Compliance

#	Recommendation	Owner	Priority
9.1	The ICANN Board should direct the compliance team to monitor and strictly enforce the compliance of contracted parties to current and future SSR and abuse related obligations in contracts, baseline agreements, temporary specifications, and community policies.	ICANN Board	High
9.2	ICANN org should proactively monitor and enforce registry and registrar contractual obligations to improve the accuracy of registration data. This monitoring and enforcement should include the validation of address fields and conducting periodic audits of the accuracy of registration data. ICANN org should focus their enforcement efforts on those registrars and registries that have been the subject of over 50 complaints or reports per year regarding their inclusion of inaccurate data to ICANN org.	ICANN org	High
9.3	ICANN org should have compliance activities audited externally at least annually and publish the audit reports and ICANN org response to audit recommendations, including implementation plans.	ICANN org	High
9.4	ICANN org should task the compliance function with publishing regular reports that enumerate tools they are missing that would help them support ICANN org as a whole to effectively use contractual levers to address security threats in the DNS, including measures that would require changes to the contracts.	ICANN org	High

SSR2 Rec 9: Monitor and Enforce Compliance

- **Implemented**: audits are happening regularly and summaries published.
- **Effective**: ICANN org has completed an audit successfully and reported out to the community.
- **Special Considerations**: this recommendation requires action from the ICANN Board and ICANN org. The Board might have to update its stance and instructions after completion of the anti-abuse Expedited Policy Development Process (EPDP) (see SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements).

SSR2 Rec 10: Provide Clarity on Definitions of Abuse-related Terms

#	Recommendation	Owner	Priority
10.1	ICANN org should post a web page that includes their working definition of DNS abuse, i.e., what it uses for projects, documents, and contracts. The definition should explicitly note what types of security threats ICANN org currently considers within its remit to address through contractual and compliance mechanisms, as well as those ICANN org understands to be outside its remit. If ICANN org uses other similar terminology—e.g., security threat, malicious conduct—ICANN org should include both its working definition of those terms and precisely how ICANN org is distinguishing those terms from DNS abuse. This page should include links to excerpts of all current abuse-related obligations in contracts with contracted parties, including any procedures and protocols for responding to abuse. ICANN org should update this page annually, date the latest version, and link to older versions with associated dates of publication.	ICANN org	High

SSR2 Rec 10: Provide Clarity on Definitions of Abuse-related Terms

#	Recommendation	Owner	Priority
10.2	Establish a staff-supported, cross-community working group (CCWG) to establish a process for evolving the definitions of prohibited DNS abuse, at least once every two years, on a predictable schedule (e.g., every other January), that will not take more than 30 business days to complete. This group should involve stakeholders from consumer protection, operational cybersecurity, academic or independent cybersecurity research, law enforcement, and e-commerce.	ICANN org	High
10.3	Both the ICANN Board and ICANN org should use the consensus definitions consistently in public documents, contracts, review team implementation plans, and other activities, and have such uses reference this web page.	ICANN org	High

SSR2 Rec 10: Provide Clarity on Definitions of Abuse-related Terms

- **Implemented**: ICANN org publishes the web page that includes the first output of the CCWG as well as the process for keeping the web page up to date.
- **Effective**: ICANN org is able to offer increased transparency and accountability with respect to accepted and community-vetted descriptions and clarity to community discussions and interpretation of policy documents, thus enabling other stakeholders to define codes of conduct around DNS abuse.

SSR2 Rec 11: Resolve CZDS Data Access Problems

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

SSR2 Rec 11: Resolve CZDS Data Access Problems

- **Implemented**: ICANN org and the community makes access to CZDS data available in a timely manner and without unnecessary hurdles to requesters.
- **Effective**: ICANN org reports a decrease in the number of zone file access complaints and improves the ability for researchers to study the security-related operations of the DNS.
- **Special Considerations**: This recommendation aims to establish proper access to the security-relevant zone file data used by academics and security specialists. This recommendation requires action from the ICANN Board, ICANN org, and the GNSO.

SSR2 Rec 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review

#	Recommendation	Owner	Priority
12.1	ICANN org should create a DNS Abuse Analysis advisory team composed of independent experts (i.e., experts without financial conflicts of interest) to recommend an overhaul of the DNS Abuse Reporting activity with actionable data, validation, transparency, and independent reproducibility of analyses as its highest priorities.	ICANN org	Medium
12.2	ICANN org should structure its agreements with data providers to allow further sharing of the data for non-commercial use, specifically for validation or peer-reviewed scientific research. This special no-fee non-commercial license to use the data may involve a time-delay so as not to interfere with commercial revenue opportunities of the data provider. ICANN org should publish all data-sharing contract terms on the ICANN web site. ICANN org should terminate any contracts that do not allow independent verification of methodology behind blocklisting.	ICANN org	Medium

SSR2 Rec 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review

#	Recommendation	Owner	Priority
12.3	ICANN org should publish reports that identify registries and registrars whose domains most contribute to abuse. ICANN org should include machine-readable formats of the data, in addition to the graphical data in current reports.	ICANN org	Medium
12.4	ICANN org should collate and publish reports of the actions that registries and registrars have taken, both voluntary and in response to legal obligations, to respond to complaints of illegal and/or malicious conduct based on applicable laws in connection with the use of the DNS.	ICANN org	Medium

SSR2 Rec 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review

- **Implemented**: ICANN org's DNS Abuse Analysis efforts introduce metrics that produce actionable, accurate, and trustworthy data.
- **Effective**: all of the data available to ICANN org is also available to the community and independent researchers, perhaps with a time delay, to provide validation and feedback.

SSR2 Rec 13: Increase Transparency and Accountability of Abuse Complaint Reporting

#	Recommendation	Owner	Priority
13.1	ICANN org should establish and maintain a central DNS abuse complaint portal that automatically directs all abuse reports to relevant parties. The system would purely act as an inflow, with ICANN org collecting and processing only summary and metadata, including timestamps and types of complaint (categorical). Use of the system should become mandatory for all gTLDs; the participation of each ccTLD would be voluntary. In addition, ICANN org should share abuse reports (e.g., via email) with all ccTLDs.	ICANN org	High
13.2	ICANN org should publish the number of complaints made in a form that allows independent third parties to analyze the types of complaints on the DNS	ICANN org	High

SSR2 Rec 13: Increase Transparency and Accountability of Abuse Complaint Reporting

- **Implemented**: ICANN org simplifies the process of submitting and receiving abuse complaints and offers insight into the number of complaints and some metadata (e.g., type of abuse reported, dates, time to resolution) for researchers and community members. This recommendation can be considered complete when the portal is up and running.
- **Effective**: contracted parties have to spend less time on misdirected complaints, and the research community as well as the broader ICANN community can see and study the associated data about those complaints.
- **Special Considerations**: Due to the complexity of this enterprise, this recommendation is expected to take several years (at least three) after the ICANN Board approves the implementation of this recommendation.

SSR2 Rec 14: Create a Temporary Specification for Evidence-based Security Improvements

#	Recommendation	Owner	Priority
14.1	ICANN org should create a Temporary Specification that requires all contracted parties to keep the percentage of domains identified by the revised DNS Abuse Reporting (see SSR2 Recommendation 13.1) activity as abusive below a reasonable and published threshold.	ICANN org	High
14.2	To enable anti-abuse action, ICANN org should provide contracted parties with lists of domains in their portfolios identified as abusive, in accordance with SSR2 Recommendation 12.2 regarding independent review of data and methods for blocklisting domains.	ICANN org	High
14.3	Should the number of domains linked to abusive activity reach the published threshold described in SSR2 Recommendation 14.1, ICANN org should investigate to confirm the veracity of the data and analysis, and then issue a notice to the relevant party.	ICANN org	High

SSR2 Rec 14: Create a Temporary Specification for Evidence-based Security Improvements

#	Recommendation	Owner	Priority
14.4	ICANN org should provide contracted parties 30 days to reduce the fraction of abusive domains below the threshold or to demonstrate that ICANN org's conclusions or data are flawed. Should a contracted party fail to rectify for 60 days, ICANN Compliance should move to the de-accreditation process.	ICANN org	High
14.5	ICANN org should consider offering financial incentives: contracted parties with portfolios with less than a specific percentage of abusive domain names should receive a fee reduction on chargeable transactions up to an appropriate threshold.	ICANN org	High

SSR2 Rec 15: Launch an EPDP for Evidence-based Security Improvements

#	Recommendation	Owner	Priority
15.1	After creating the Temporary Specification (see SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements), ICANN org should establish a staff-supported EPDP to create an anti-abuse policy. The EPDP volunteers should represent the ICANN community, using the numbers and distribution from the Temporary Specification for gTLD Registration Data EPDP team charter as a template.	ICANN org	High
15.2	The EPDP should draw from the definition groundwork of the CCWG proposed in SSR2 Recommendation 10.2. This policy framework should define appropriate countermeasures and remediation actions for different types of abuse, time-frames for contracted party actions like abuse report/response report timelines, and ICANN Compliance enforcement actions in case of policy violations. ICANN org should insist on the power to terminate contracts in the case of a pattern and practice of harboring abuse by any contracted party. The outcome should include a mechanism to update benchmarks and contractual obligations related to abuse every two years, using a process that will not take more than 45 business days.	ICANN org	High

SSR2 Recommendations 14 and 15

- **Implemented**: ICANN Compliance has the tools to appropriately respond to contracted parties failing to respond to DNS abuse, specifically the existence of anti-abuse related obligations in all relevant contracts and agreements.
- **Effective**: ICANN Compliance uses those tools to deal with egregious policy violations on the part of contracted parties.
- **Special Considerations**: The intended outcome of SSR2 Recommendations 14 and 15 is to empower ICANN Compliance to deal with the worst offenders when it comes to DNS abuse, which the ICANN Compliance team has stated it lacks sufficient tools to do.

SSR2 Rec 16: Privacy Requirements and RDS

#	Recommendation	Owner	Priority
16.1	ICANN org should provide consistent cross-references across their website to provide cohesive and easy-to-find information on all actions—past, present, and planned—taken on the topic of privacy and data stewardship, with particular attention to the information around the RDS.	ICANN org	Medium
16.2	ICANN org should create specialized groups within the contract compliance function that understand privacy requirements and principles (such as collection limitation, data qualification, purpose specification, and security safeguards for disclosure) and that can facilitate law enforcement needs under the RDS framework as that framework is amended and adopted by the community (see also SSR2 Recommendation 11: Resolve CZDS Data Access Problems).	ICANN org	Medium
16.3	ICANN org should conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they have procedures in place to address privacy breaches.	ICANN org	Medium

SSR2 Rec 16: Privacy Requirements and RDS

- **Implemented**: ICANN org's actions regarding privacy and their management of the RDS are properly documented, and specifically assigned resources within ICANN org keep the organization in line with current best practices and legal requirements in this space.
- **Effective**: ICANN org can demonstrate ongoing compliance with best practices and legal requirements in data handling and privacy.

Additional SSR-Related Concerns Regarding the Global DNS

Additional SSR-Related Concerns Regarding the Global DNS

- Addressed a variety of other SSR-related issues observed over the course of the review
- Recommendation topics:
  - Name collision
  - Research and Briefings
  - DNS Testbed
  - Root Zone and Registry Concerns
  - Emergency Back-End Registry Operator (EBERO)

SSR2 Rec 17: Measuring Name Collisions

#	Recommendation	Owner	Priority
17.1	ICANN org should create a framework to characterize the nature and frequency of name collisions and resulting concerns. This framework should include metrics and mechanisms to measure the extent to which Controlled Interruption is successful in identifying and eliminating name collisions. This could be supported by a mechanism to enable protected disclosure of name collision instances. This framework should allow the appropriate handling of sensitive data and security threats.	ICANN org	Medium
17.2	The ICANN community should develop a clear policy for avoiding and handling new gTLD-related name collisions and implement this policy before the next round of gTLDs. ICANN org should ensure that the evaluation of this policy is undertaken by parties that have no financial interest in gTLD expansion.	ICANN community and ICANN org	Medium

SSR2 Rec 17: Measuring Name Collisions

- **Implemented**: ICANN org produces a framework to produce findings that characterize the nature and frequency of name collisions and resulting concerns by identifying metrics and devising mechanisms to measure the extent to which the Controlled Interruption mechanism is successful.
- **Effective**: ICANN org and the community are able to detect, act on, and ultimately minimize the existence of name collisions and respond to evolving name collision scenarios.
- **Special Considerations**: This recommendation must be completed before the next round of gTLDs.

SSR2 Rec 18: Informing Policy Debates

#	Recommendation	Owner	Priority
18.1	ICANN org should track developments in the peer-reviewed research community, focusing on networking and security research conferences, including at least ACM CCS, ACM Internet Measurement Conference, Usenix Security, CCR, SIGCOMM, IEEE Symposium on Security and Privacy, as well as the operational security conferences and FIRST, and publish a report for the ICANN community summarizing implications of publications that are relevant to ICANN org or contracted party behavior.	ICANN org	Low
18.2	ICANN org should ensure that these reports include relevant observations that may pertain to recommendations for actions, including changes to contracts with registries and registrars, that could mitigate, prevent, or remedy SSR harms to consumers and infrastructure identified in the peer-reviewed literature.	ICANN org	Low
18.3	ICANN org should ensure that these reports also include recommendations for additional studies to confirm peer-reviewed findings, a description of what data would be required by the community to execute additional studies, and how ICANN org can offer to help broker access to such data, e.g., via the CZDS.	ICANN org	Low

SSR2 Rec 18: Informing Policy Debates

- **Implemented**: ICANN org creates and maintains a public archive of digests or readouts from various networking and security research conferences

- **Effective**: the information coming from the research community on SSR-related issues is more accessible to people who are making policy decisions.

SSR2 Rec 19: Complete Development of the DNS Regression Test Suite

#	Recommendation	Owner	Priority
19.1	ICANN org should complete the development of a suite for DNS resolver behavior testing.	ICANN org	Low
19.2	ICANN org should ensure that the capability to continue to perform functional testing of different configurations and software versions is implemented and maintained.	ICANN org	Low

SSR2 Rec 19: Complete Development of the DNS Regression Test Suite

- **Implemented**: ICANN org finishes developing a publicly accessible test suite for community testing and research into resolver behavior.
- **Effective**: there is a test suite available with an annual update cycle that helps ensure the DNS's integrity and availability globally.

SSR2 Rec 20: Formal Procedures for Key Rollovers

#	Recommendation	Owner	Priority
20.1	ICANN org should establish a formal procedure, supported by a formal process modeling tool and language to specify the details of future key rollovers, including decision points, exception legs, the full control-flow, etc. Verification of the key rollover process should include posting the programmatic procedure (e.g., program, finite-state machine (FSM)) for public comment, and ICANN org should incorporate community feedback. The process should have empirically verifiable acceptance criteria at each stage, which should be fulfilled for the process to continue. This process should be reassessed at least as often as the rollover itself (i.e., the same periodicity) so that ICANN org can use the lessons learned to adjust the process.	ICANN org	Medium
20.2	ICANN org should create a group of stakeholders involving relevant personnel (from ICANN org or the community) to periodically run table-top exercises that follow the Root KSK rollover process.	ICANN org	Medium

SSR2 Rec 20: Formal Procedures for Key Rollovers

- **Implemented**: ICANN org develops formal process and verification that offers verification of the key rollover process after each key rollover, and when ICANN org begins to run regular tabletop exercises to test and familiarize participants with the key rollover process.
- **Effective**: the SSR of the process by which DNSSEC protections are maintained during Root zone Key Signing Key (Root KSK) during key rollovers are formally verifiable.
- **Special Considerations**: This recommendation must be completed in conjunction with each key rollover.

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

#	Recommendation	Owner	Priority
21.1	ICANN org and PTI operations should accelerate the implementation of new RZMS security measures regarding the authentication and authorization of requested changes and offer TLD operators the opportunity to take advantage of those security measures, particularly MFA and encrypted email.	ICANN org and PTI	Medium

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

- **Implemented**: ICANN org and PTI have a next-generation RZMS that involves a robust and secure authentication and authorization model for submission and approval of the requests as well as additional functionality that would enhance the security and stability of the global DNS system.
- **Effective**: ICANN org mitigates the potential for security and stability issues that involve the misuse of the RZMS through improved identity management procedures.

SSR2 Rec 22: Service Measurements

#	Recommendation	Owner	Priority
22.1	For each service that ICANN org has authoritative purview over, including root-zone and gTLD-related services as well as IANA registries, ICANN org should create a list of statistics and metrics that reflect the operational status (such as availability and responsiveness) of that service, and publish a directory of these services, data sets, and metrics on a single page on the icann.org web site, such as under the Open Data Platform. ICANN org should produce measurements for each of these services as summaries over both the previous year and longitudinally (to illustrate baseline behavior).	ICANN org	Low
22.2	ICANN org should request community feedback annually on the measurements. That feedback should be considered, publicly summarized after each report, and incorporated into follow-on reports. The data and associated methodologies used to measure these reports' results should be archived and made publicly available to foster reproducibility.	ICANN org	Low

SSR2 Rec 22: Service Measurements

- **Implemented**: ICANN org makes the operational status metrics on the services ICANN org supports available to the community.
- **Effective**: the community sees an increase in the transparency of ICANN org SSR-related operations.

SSR2 Rec 23: Algorithm Rollover

#	Recommendation	Owner	Priority
23.1	PTI operations should update the DNSSEC Practice Statement (DPS) to allow the transition from one digital signature algorithm to another, including an anticipated transition from the RSA digital signature algorithm to other algorithms or to future post-quantum algorithms, which provide the same or greater security and preserve or improve the resilience of the DNS.	PTI	Medium
23.2	As a root DNSKEY algorithm rollover is a very complex and sensitive process, PTI operations should work with other root zone partners and the global community to develop a consensus plan for future root DNSKEY algorithm rollovers, taking into consideration the lessons learned from the first root KSK rollover in 2018.	PTI	Medium

SSR2 Rec 23: Algorithm Rollover

- **Implemented**: PTI updates the DPS to allow the transition from one digital signature algorithm to another and develops a consensus plan for future root DNSKEY algorithm rollovers.
- **Effective**: ICANN org is prepared for more advanced algorithms to be used for key signing, including any increases of key length and timing for key rollover.

SSR2 Rec 24: Improve Transparency and End-to-End Testing for the EBERO Process

#	Recommendation	Owner	Priority
24.1	ICANN org should coordinate end-to-end testing of the full EBERO process at predetermined intervals (at least annually) using a test plan that includes datasets used for testing, progression states, and deadlines, and is coordinated with the ICANN contracted parties in advance to ensure that all exception legs are exercised, and publish the results.	ICANN org	Medium
24.2	ICANN org should make the Common Transition Process Manual easier to find by providing links on the EBERO website.	ICANN org	Medium

SSR2 Rec 24: Improve Transparency and End-to-End Testing for the EBERO Process

- **Implemented**: ICANN org coordinates annual end-to-end testing of the full EBERO process with public documentation for the outcome.
- **Effective**: ICANN org is able to validate that the EBERO process functions as intended, protecting registrants and providing an additional layer of protection to the DNS.

Extensive Appendixes

Extensive Appendixes

- Included suggestions to improve the process of future reviews
- Detailed descriptions of the review processes and methodologies
- Full findings related to the SSR1 evaluation
- Research on DNS Abuse, relevant cryptography issues
- Mapping of SSR2 recommendations against relevant Bylaws and ICANN strategic plan goals
- Responses to 100+ public comments received on the draft report

Wrap Up

Implementation Shepherds

- Kerry-Ann Barrett
- KC Claffy
- Russ Housley
- Laurin Weissinger

- Implementation Shepherds are the first contact for any questions or clarifications the Board seeks as it considers the recommendations, and ICANN org seeks once the implementation is underway.

Next Steps

- Public Comment is open until 9 March 2021.
- The Board will consider the Public Comment submissions received, and a feasibility analysis and impact assessment of the implementation of recommendations,
- The Board will take action on SSR2 recommendations within six months of receipt of the report, by 25 July 2021.

Additional Links

ICANN ByLaws – Section 4, “Accountability and Review”

- https://www.icann.org/resources/pages/governance/bylaws-en/#article4

SSR2 Final Report & Public Comment

- https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf
- https://www.icann.org/public-comments/ssr2-final-report-2021-01-28-en

Thank You and Questions

Visit our wiki at **https://community.icann.org/x/AE6AAw**
Email (publicly archived): input-to-ssr2@icann.org