
ICANN
ANNUAL GENERAL
66
MONTRÉAL
2–7 November 2019

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

Community Engagement Session @ ICANN66

3 November 2019

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 may include:

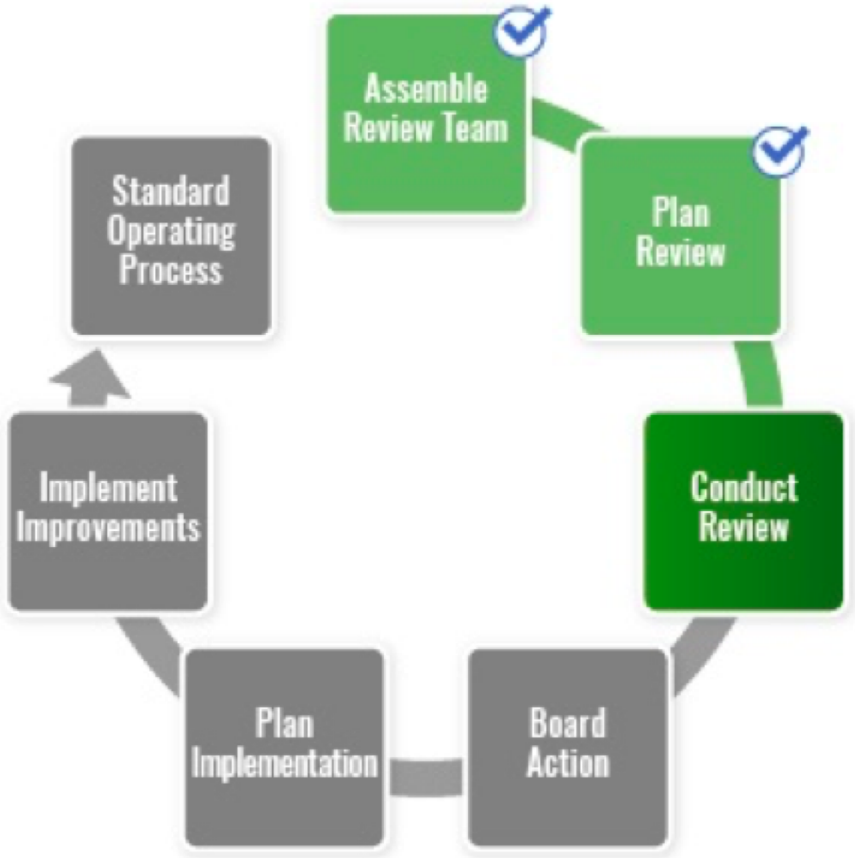
1. security, operational stability and resiliency matters, both physical and network, relating to the coordination of the Internet's system of unique identifiers;
2. conformance with appropriate security contingency planning framework for the Internet's system of unique identifiers;
3. maintaining clear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

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

Workstream 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

Workstream 1

SSR1 Implementation & Impact

Review of SSR1 Recommendations

Covered by ICANN Bylaw 4.6(c) …

- 28 SSR1 Recommendations evaluated
- 27 SSR1 recommendations still relevant
  - Most relevant recommendations are not fully implemented

SSR1 Implementation and Impact

ICANN org should continue its work to implement all relevant SSR1 Recommendations

- Complete the implementation of all relevant SSR1 recommendations. The SSR2 Review Team's observations of the status and the road to implement the recommendation will be detailed in the report (where the original guidance was not sufficiently measurable.)

Workstream 1

SSR2 Recommendations Expanding on Original SSR1 Recommendations

Expanded SSR1 Recommendation 9

Information Security Management Systems and Security Certifications

- Establish a road map of industry standard security audits and certification activities that are being undertaken, including milestone dates for obtaining each certification and continuous improvement
- Put together a plan for certifications and training requirements for roles in the organization, track completion rates, provide reasoning for their choices, and document how the certifications fit into ICANN org's security and risk management strategies
- Provide reasoning for their choices, demonstrating how they fit into its security and risk management strategies
- Implement an Information Security Management System and undergo a third party audit and certification
- Be audited and certified along the lines of industry security standards, and assess certification options with commonly accepted international standards (e.g., ITIL, ISO 27001)

Expanded SSR1 Recommendations 12, 15, and 16

SSR Strategy and Framework

- Address security issues clearly, publicly, and promote security best practices across all contracted parties
- Work with the community to develop and continuously update an overarching SSR strategy and framework; capture SSR-related best practices in a consensus document; establish clear, measurable, and trackable objectives; implement the practices in contracts, agreements, and MOUs
- Implement coordinated vulnerability disclosure reporting
- 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

Expanded SSR1 Recommendation 20 and 22

Budget Transparency and Budgeting SSR in new gTLDs

- Be more transparent with the budget for parts of ICANN org related to implementing the SSR Framework and performing SSR-related functions, including those associated with the introduction of new gTLDs

Expanded SSR1 Recommendation 27

Risk Management

- Centralize and strategically coordinate ICANN's Risk Management Framework
- Clearly articulate their risk framework and strategically align the framework against the requirements and objectives of the organization, describe relevant measures of success, and how these are assessed

Workstream 2

Key SSR Issues within ICANN

Recommendations Areas for Workstream 2

Covered by ICANN Bylaw 4.6(c) (ii) A, 4.6(c) (ii) B as well as 4.6(c) (iii)

Topics covered include:

- C-Suite Security Position
- Security Risk Management
- Business Continuity Management
- Disaster Recovery Planning

C-Suite Security Position

- Create the position then hire or appoint an individual responsible for both strategic and tactical security and risk management across the security domain of the organization and the global identifier system

  - position would fulfil the responsibilities of a chief security officer and chief information security officer
  - position should manage ICANN org's Security Function, oversee the interactions of security staff in all relevant areas, provide regular reports to the community
  - position 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, feeding into all security-related contractual terms

Security Risk Management

- Clearly articulate and strategically align the Security Risk Management Framework against the requirements and objectives of the organization, describe relevant measures of success, and how these are to be assessed
    - Adopt and implement ISO 31000 “Risk Management”, the ISO/IEC 27000 family “Information Security Management Systems”, and ISO 22301 Business Continuity Management, and validate with appropriate independent audits
    - Security risk matrix and registers should be created / updated and used to prioritize and guide the activities of the ICANN org. Findings should feed into BC/DR and the ISMS
    - ICANN should name or appoint a dedicated, responsible person in charge of security risk management
    - The report from the DNS Risk Framework Working Group and the 2016 Identifier Systems Security, Stability and Resiliency Framework for FY15-16 should be considered for the development of the Security Risk Management Framework

Business Continuity Management

- Establish a Business Continuity Plan (BCP) for Public Technical Identifiers (PTI) operations (IANA functions)
  - includes all relevant systems that contribute to the Security and Stability of the DNS and also Root Zone Management, in line with ISO 22301 “Business Continuity Management”
- Establish a BCP for the systems owned by, or under the purview of ICANN org, based on ISO 22301 “Business Continuity Management”
- Publish evidence (e.g., a summary of their BCP and Provisions)
- Engage an external auditor to verify compliance aspects of the implementation of the resulting BCP

Disaster Recovery Planning

- 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
- Establish a DR Plan for all the systems owned by, or under the purview of ICANN org, also in line with ISO 27031 “Guidelines for information and communication technology readiness for business continuity”
- 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, specifically outside of the United States and its territories and the North American region, including a plan for implementation
- Publish evidence, e.g., a summary, of their overall disaster recovery plans and provisions
- Engage an external auditor to verify compliance aspects of the implementation of these DR plans

Workstream 3

Security, Stability, and Resilience of the DNS

Recommendations Areas for Workstream 3

Covered by ICANN Bylaw 4.6(c) (ii) A, 4.6(c) (ii) B, 4.6(c) (ii) C, and 4.6(c) (iii)

- Abuse and Compliance
  - Abuse Definitions & Reporting
  - DAAR
  - Policies, Agreements, Activities with Registrars and Registries
  - Contracts/Agreements
  - Incentivization
  - Abuse Report Portal
  - Compliance Function
- Abusive Naming
- Key Rollover
- Root Server Operations
- Root Zone Data and IANA Registries

Abuse Definitions & Reporting

- Undertake the following short-term and long-term actions to address the definition and application of DNS abuse; elicit feedback from the ICANN community
  - ICANN org and Board: implement the CCT Review and RDS (WHOIS) Review recommendations, and other security-related actions based on current, community vetted abuse definitions, without delay
  - ICANN Board: adopt the additional term and evolving external definition of "security threat"—a term used by the ICANN DAAR project, the GAC (in its Beijing Communique and for Spec 11), and the Convention on Cybercrime -- to use in conjunction with ICANN DNS Abuse definition
    - ICANN Board: entrust SSAC and PSWG to work with eCrime and abuse experts to evolve the definition of DNS Abuse, taking into account the processes and definitions outlined in the Convention on Cybercrime ETS No. 185
- Minimize ambiguous language and reach a universally acceptable agreement on abuse, SSR, and security threats in its contracts with contracted parties and implementation plans

DAAR

- The ICANN Board and ICANN org: work with the gNSO, ccNSO, and ccTLDs to improve DAAR and incorporate ccTLD data tracking and reporting in DAAR and integrate pricing data into DAAR
- Identify entities with persistently very high abuse domain registrations
- Publish DAAR reports that identify registries and registrars that most contribute to abuse
- Publish reports that include machine-readable formats of the data, in addition to the graphical data in current reports

Contracts and Agreements

- Incorporate measures to mitigate “DNS abuse” and “security threats” in agreements with contracted parties, including Registry Agreements (base and individual) and the RAA, as necessary contract obligations
- Make SSR requirements mandatory on contract or baseline agreement renewal
- Include SSR concerns and SSR2 recommendations in these negotiations
- Attract and collaborate with ccTLDs and the ccNSO to address DNS abuse and security threats in ccTLDs. Some ccTLDs are creating and using best practices, while others have domain portfolios with unacceptably high levels of abuse
- ICANN Board, community and staff: work with the ccNSO to advance data tracking and reporting, an assessment of DNS abuse and security threats in ccTLDs, and a ccNSO plan to support ccTLDs in further mitigating DNS abuse and security threats

Incentivization

- Create incentives for contracted parties to mitigate abuse and security threats; impose such changes unilaterally and immediately
- Incentivize the mitigation of abuse and security threats utilizing measures where take downs are performed within an appropriate period after registration (e.g., 30 days after the domain is registered)
- Institutionalize training and certifications for contracted parties and key stakeholders -- Registries, Registrars, Privacy/Proxy Service Providers, Internet Service Providers -- in areas identified by DAAR and other sources on common methods of abuse, and mitigation efforts

Abuse Report Portal

- Establish and maintain a central DNS Abuse complaint portal for all complaints that automatically directs all abuse reports to relevant parties
  - It should be mandatory for all gTLDs; ccTLDs should be invited to join

Compliance Function

- Ensure ICANN org's compliance activities are neutral and effective:
  - Have compliance activities audited externally, and hold them to a high standard
  - ICANN Board: empower the Compliance Office to react to complaints and require Compliance to initiate investigation and enforce contractual obligations against those aiding and abetting systemic abuse, as defined by the SLA
  - Default approach used by the Compliance Office should involve SLAs on enforcement and reporting, clear and efficient, processes, a fully informed complainant, measurable satisfaction, and maximum public disclosure

Abusive Naming

- Build upon the current activities to investigate typical misleading naming, in cooperation with researchers and stakeholders, wherever applicable
- When misleading naming rises to the level of abusive naming, include this type of abuse in their DAAR reporting, and develop policies and mitigation best practices
- Measure the number of abusive naming complaints made at the portal and shared that information with the community in a form that allows independent third parties to analyze, mitigate, and prevent harm from use of such domain names
- The current "Guidelines for the Implementation of IDNs" should be updated to include a section on names containing trademarks, TLD-chaining and the use of (hard-to-spot) typos; contractually enforce "Guidelines for the Implementation of IDNs" for gTLDs and recommend that ccTLDs do the same; the guidelines should apply to IDNs and all other names to avoid pure ASCII domains to be abused due to being visually indistinguishable

DNS Testbed

- Complete the development of a suite for DNS regression testing
- Perform functional testing of different configurations and software versions

Key Rollover

- 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, full control-flow, etc.
  - Verification of the key rollover process should include posting the programmatic procedure (program, FSM, etc.) for public comment, and community feedback should be incorporated
  - Have empirically verifiable acceptance criteria at each stage, which should be fulfilled for the process to continue
  - Create a group of stakeholders involving relevant personnel (from ICANN org and/or the community) to periodically run table-top exercises that follow the Root KSK rollover process

Root Server Operations

- Develop baseline security best practices for root server operators and operations (in close cooperation with RSSAC and other relevant stakeholders)
    - Include: change management, verification procedures, and sanity check procedures, and should also include hardening strategies of L-Root
- Develop relevant KPIs to measure these best practices and requirements, and ensure yearly reporting on how these KPIs are met by RSOs and other relevant parties including ICANN org
- Ensure that L-Root uses a vulnerability disclosure process, security reports and intelligence, and communicate to researchers and RSSAC wherever applicable

Root Zone Data and IANA Registries

- Create a list of statistics and metrics for 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, 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
- Produce KPIs as summaries over both the previous year and longitudinally (to illustrate baseline behavior)
- Community feedback should be requested annually, considered, publicly summarized after each report, and should be incorporated into follow-on reports

Workstream 4

Future Challenges

Recommendations Areas for Workstream 4

Covered by ICANN Bylaw 4.6(c) (iii)

- Cryptography
- Name Collision
- Privacy
- Research and Briefings
- DNS-over-HTTPS (DoH)

Cryptography

- PTI should update the DPS to facilitate 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
- PTI should work with other root zone partners and the global community to develop a consensual plan for root DNSKEY algorithm rollover

Name Collision

- Produce findings that characterize the nature and frequency, and any relevant concerns, regarding the issue of name collisions
  - a solution be implemented before the next round of gTLDs be launched
- Support 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
  - Publish planned milestones and (with associated start/end dates) for these studies, and link to their results from the published plan
  - NCAP should be allowed to complete all three of its studies

Privacy

- Create specialized units within the contract compliance function that focuses and understands privacy requirements and principles (such as collection limitation, data qualification, purpose specification and security safeguards for disclosure) but can facilitate law enforcement needs under the WHOIS framework as it is amended and adopted by the community
- Monitor relevant and evolving privacy legislation (e.g., CCPA and legislation protecting personal identifiable information (PII)) and ensure that policies and procedures are aligned and in compliance privacy and the protection of personally identifiable information is ensured as required by relevant legislation and regulation
- Develop and keep up to date a policy for the protection of PII; communicate policy to all persons involved in the processing of personally identifiable information; implement appropriate technical and organizational measures to protect PII
- ICANN's DPO: be responsible for external DNS PII; provide guidance to managers and stakeholders regarding responsibilities and procedures, and monitor and report on relevant technical developments
- Conduct periodic audit of adherence to privacy policies implemented by registrars to ensure that they at a minimum have procedures in place to address privacy breaches

Research and Briefings

- Track developments in the peer-reviewed research community, focusing on networking and security research conferences, including at least ACM CCS, ACM IMC, Usenix Security, CCR, SIGCOMM, IEEE S&P, APWG, M3AAWG, and publish to the ICANN community an action report about any publications that are relevant
    - Reports should include either recommendations or situational awareness for SSR-impacting changes to contracted parties and other ICANN community stakeholders

DNS-over-HTTPS (DoH)

- DoH enables application vendors to choose the resolution infrastructure, thereby allowing the vendors per-application overrides of administrator or user choice of DNS resolution and selective enforcement of DNSSEC
- Commission investigation(s) into DoH adoption, and focus particular attention to the reduced resilience in the DNS ecosystem and security concerns from the DoH protocol enhancements
    - *This recommendation is still under active discussion within SSR2*

Wrap Up

Thank You and Questions

Visit our wiki at **https://community.icann.org/x/AE6AAw**
Email (publicly archived): input-to-ssr2rt@icann.org