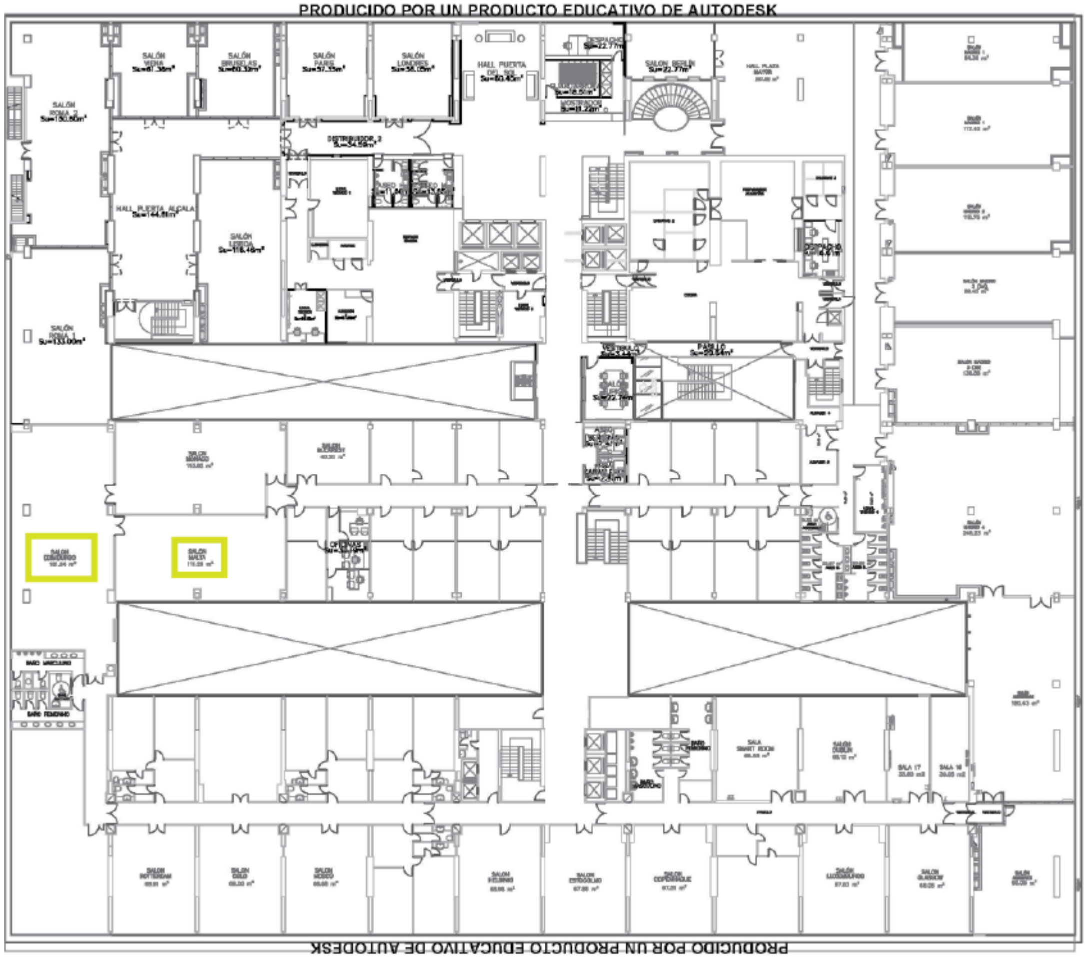
Second Security, Stability, and Resiliency Review (SSR2)

ICANN

Plenary Meeting 11 | Madrid Face-to-Face
Day 2: 15 May 2017

Meeting Logistics

- Observers may join in-room or online
- Restrooms:
  - Exit salon Edinburgo, restrooms immediately on your right
- Breaks (Salon Malta next door):
  - 10:30 – 10:40 coffee
  - 12:30 – 13:15 working lunch
  - 15:15 – 15:30 coffee



Review of Agenda – Day Two

1 08:30 – 10:00
Proposed SSR2 Work Approach (James Gannon)

10:30 – 10:40 Break

2 10:40 – 12:30
Work Plan and Timeline

12:30 – 13:15 Review Team Lunch

3 13:15 – 15:15
Subgroup Discussions

15:15 – 15:30 Break

4 15:30 – 16:30
Outreach Plan and Next Steps

5 16:30 – 17:10
Items Requiring Additional Discussion and AOB

6 17:10 – 17:30
Recap of Action Items and Closing Remarks

ICANN Expected Standards of Behavior

Those who take part in ICANN's multistakeholder process, including Board, staff and all those involved in SO and AC councils, undertake to:

Act in accordance with ICANN's Bylaws. In particular, participants undertake to act within the mission of ICANN and in the spirit of the values contained in the Bylaws.

Adhere to ICANN's conflict of interest policies.

Treat all members of the ICANN community equally, irrespective of nationality, gender, racial or ethnic origin, religion or beliefs, disability, age or sexual orientation; members of the ICANN community should treat each other with civility both face-to-face and online.

Respect all members of the ICANN community equally and behave according to professional standards and demonstrate appropriate behavior. ICANN strives to create and maintain an environment in which people of many different backgrounds and cultures are treated with dignity, decency and respect. Specifically, participants in the ICANN process must not engage in any type of harassment. Generally, harassment is considered unwelcome hostile or intimidating behavior -- in particular, speech or behavior that is sexually aggressive or intimidates based on attributes such as race, gender, ethnicity, religion, age, color, national origin, ancestry, disability or medical condition, sexual orientation or gender identity.

Protect the organization's assets and ensure their efficient and effective use.

Act fairly and in good faith with other participants in the ICANN process.

Conduct themselves in accordance with ICANN policies.

Support the maintenance of robust mechanisms for public input, accountability, and transparency so as to ensure that policy development and decision-making processes will reflect the public interest and be accountable to all stakeholders.

Listen to the views of all stakeholders when considering policy issues. ICANN is a unique multistakeholder environment. Those who take part in the ICANN process must acknowledge the importance of all stakeholders and seek to understand their points of view.

Work to build consensus with other stakeholders in order to find solutions to the issues that fall within the areas of ICANN's responsibility. The ICANN model is based on a bottom-up, consensus-driven approach to policy development. Those who take part in the ICANN process must take responsibility for ensuring the success of the model by trying to build consensus with other participants.

Promote ethical and responsible behavior. Ethics and integrity are essential, and ICANN expects all stakeholders to behave in a responsible and principled way.

Facilitate transparency and openness when participating in policy development and decision-making processes.

Act in a reasonable, objective and informed manner when participating in policy development and decision-making processes. This includes regularly attending all scheduled meetings and exercising independent judgment based solely on what is in the overall best interest of Internet users and the stability and security of the Internet's system of unique identifiers, irrespective of personal interests and the interests of the entity to which individuals might owe their appointment.

Proposed SSR2 Work Approach

James Gannon

SSR2 Work Breakdown Structure - Bylaws

https://community.icann.org/pages/viewpage.action?pageId=64076120&preview=/64076120/64949020/SSR2-Plenary-SubTeams-20150508V0.2-JG-DRAFT%5B1%5D.docx

The following areas are identified as ‘may assess’ under the Bylaws, Section 4.6(c),

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

> 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.

SSR2 Work Breakdown Structure - Bylaws

The following areas are identified as 'shall assess' under the Bylaws, Section 4.6(c),

"(iii) The SSR Review Team shall also assess 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."

"(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."

SSR2 Work Breakdown Structure – Work Structure

Sub Teams – Work Methods

- Sub teams may be proposed in addition to the groupings listed below
- Sub teams structure and activities will be agreed at the plenary of the SSR2 Review Team in Madrid
- Sub teams will be populated by a call for volunteers lasting 1 week from the date of
- sub teams should comprise of a minimum of 3 members of the SSR2 RT
- Sub teams will be required to appoint a rapporteur who will act as the ‘pen holder’ and will guide the sub team through their work and will be responsible for reporting back the progress of the review team to the plenary
- Sub team meetings will be convened by the rapporteur as soon as possible to commence its deliberations and is expected to report back to the full CWG on a regular basis
- Sub teams will at a defined period of time submit its status and proposed language for inclusion in the relevant section of the draft SSR2 review team document and recommendations, for review by the plenary SSR2 RT
- If accepted by the SSR2 RT plenary, the agreed language will be included into the final review team outcomes and recommendations document

Sub Team 1 – SSR1 Review

Topic	Review of Implementation of SSR1 Report
Related Bylaw	4.6 (c)(iv)
Skillset	ICANN, Policy, SSR1
Description of activity	The sub team will be responsible for reviewing the implementation of the SSR1 RTs work and drafting a document outlining the effectiveness of said implementation.
Work Items	
Team Members	
Rapporteur	

Sub Team 2 – ICANN Security

Topic	ICANN Internal Security Processes
Related Bylaw	4.6 (c)(ii)(A) 4.6 (c)(ii)(B) 4.6 (c)(iii)
Skillset	IT Security, Audit, Risk Management, Disaster Recovery
Description of activity	The sub team will be responsible for reviewing the completeness and effectiveness of ICANNs internal security processes and the effectiveness of the ICANN security framework.
Work Items	
Team Members	
Rapporteur	

Sub Team 3 – DNS Security

Topic	ICANN DNS Security Coordination Processes
Related Bylaw	4.6 (c)(ii)(A) 4.6 (c)(ii)(C)
Skillset	DNS Security, RIR, IETF, Risk Management
Description of activity	The sub team will be responsible for reviewing ICANNs role in the broader security of the DNS and unique identifiers system, including its role in mitigating threats to the DNS and other unique identities it coordinates.
Work Items	
Team Members	
Rapporteur	

Sub Team 4 – Future Threats

Topic	Future Threats and Challenges
Related Bylaw	4.6 (c)(iii)
Skillset	Threat Intel, Policy, Cybersecurity, IETF,
Description of activity	The sub team will be responsible for reviewing the long term strategy of ICANN to plan for and mitigate potential threats to the secure and resilient operation of the unique identifiers systems it coordinates.
Work Items	
Team Members	
Rapporteur	

Sub Team 5 – IANA Transition

Topic	IANA Transition Impact
Related Bylaw	4.6 (c)(ii)(B) 4.6 (c)(iii)
Skillset	IANA, CCWG, IETF, RIR, Risk Management
Description of activity	The sub team will be responsible for reviewing the impact of the IANA transition on the security of ICANN and the unique identifier systems it coordinates.
Work Items	
Team Members	
Rapporteur	

Timeline (Based on v3 Terms of Reference)

- February-May 2017: agree Terms of Reference and work plan
- May-September 2017: Fact finding and assembling materials
- October 2017: Assemble findings and consult with ICANN community
- November 2017-January 2018: Socialize draft recommendations with community
- February 2018: Publish draft report for public comment
- March-April 2018: Review input received and incorporate as appropriate
- June 2018: Send final report to ICANN Board
- June 2018: Socialize final recommendations with community

Work Plan & Timeline

ICANN Board Resolution

03 Feb 2017
Appointment of Board Designees for New Specific Reviews: Second Security, Stability, and Resiliency of the Domain Name System

Resolved (2017.02.03.11), the Board hereby appoints Kaveh Ranjbar to serve as a member of the Second SSR Review Team, and requests that this team develop and deliver to the Board their approved Terms of Reference and Work Plan by the 30th of March, to ensure that the team's scope and timeline is consistent with the requirements of the ICANN Bylaws.

https://www.icann.org/resources/board-material/resolutions-2017-02-03-en#1.g

Work Plan & Timeline

- v2 draft Work Plan: https://community.icann.org/pages/viewpage.action?pageId=64076120&preview=/64076120/64081761/SSR2%20Draft%20Work%20Plan%20-%20April%202017%20-%20EO.docx

- Should outline key areas for discussion, data elements to be considered, milestones to be achieved and timelines for producing both findings and recommendations.

Work Plan & Timeline

- Is there any further information ICANN organization can provide us to inform our work?
- What additional data do we need?
- Do we need additional support (consultant)?
- How can the RT work best effectively and efficiently?
- What are our key milestones?
- What are the barriers to meeting key milestones?
- How can we ensure we stay on target with the review timeline?

Subgroup Discussions

Subgroup Discussions

- Confirm group topics and identify group members
- What are the next steps for each?

ICANN58 Brainstorming

Ii: Shall Review 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.

Measures and evaluations of security efforts

- What is the scope of ICANN's threat modeling?
- Is DNSSEC an ICANN security effort?
- How effective it is ICANN risk management?
- Study the DNS abuse lifecycle
- If I how ICANNs security efforts related to the DNS?
- How ICANN measures the effectiveness as security efforts?
- What are ICANN's security efforts? (x2)
- What are the benchmarks and good practices for successful security efforts?
- Evaluate the DNS abuse threat mitigation measures/Deficiencies processing speed
- Recommend upgrade and revision of security and stability procedures and action plans.
- Review ICANN security procedures.

*Extracted from the SSR2 scope brainstorming session at ICANN58

Organizational

- What are the indicators for "successful" implementations and intended effects?
- Are SSAC recommendations automatically considered as ICANN efforts towards SSR?
- What are the changes to ICANN SSR with the IANA transition?
- How to interact with outside organizations?
- What are the key performance indicators
- How can we measure "the extent" of ICANN's success in implementing security efforts?
- What is the significance of "both internal and external, that directly affect and/or affected by…"?

Future challenges

- Explore forecasting research on the Internet capacity/performance(DD OS).
- Should SSR2 consider the future?
- How do we assess "Future challenges to security and stability a DNS?"
- What are the actual and potential challenges and threats?

ICANN58 Brainstorming

*Extracted from the SSR2 scope brainstorming session at ICANN58

Iii: Shall review 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.

Approach to Assessing

- How can we assess the efforts of prior recommendations?
- SSR1 implementation, what were the impacts for results of each successfully implemented recommendation?
- How do we get an understanding of what SSR1 recommendations have been implemented?
- Which implementation measures from what were critical are deemed insufficient?
- Are there measures in place to assess SSRI one work?
- Which extent of SSR1 recommendations implemented?
- Review and grade importance and way it is implemented
- What are the indicators the SS are too would want to use to measure “success” of security efforts?
- How are we distinguishing operational stability and security from measures that stem from compliance issues?
- How can we work on global policies?

Post Transition Factors

- Which recommendations are still critical for SSR since the transition?

Uncategorized

- Collect input from the community on how ICANN should improve on SSR

ICANN58 Brainstorming

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

Definitions

- What does security, stability, resiliency mean? (x4)
- What do we mean by unique identifiers? (x2)
- What is meant by "both physical and network"?
- What does "interoperable security processes" mean?

Scope

- What has been, or could be, the impact of the evolution and the number and types of devices in the DNS?
- What are the parameters to secure the DNS?
- Which portion of the Internet systems of unique identifiers does ICANN not coordinate?
- Where is the best source to determine most pertinent aspects? (e.g. networking scope is wide and covers many actors in the community)
- What is the main responsibility of SSR2 review team?

*Extracted from the SSR2 scope brainstorming session at ICANN58

Procedures

- UI procedures?
- Interoperable security processes – how is this currently addressed in DN, protocols, addresses?
- What is the current state of ICANN and disaster and operational recovery planning?
- Identity and access management?
- Operational impact on security and stability?
- What is ICANN's internal level of risk and how it minute and how is it managed? (vulnerability reporting bug bounty, future?)
- Conduct performance indicators and benchmarks of SSR.

Uncategorized

- Explore DNS analysis opportunities (malware)
- Is the assessment limited to those organizations ICANN has policy inputs to?
- Physical security? Should we consider KSK signing physical security? ICANN headquarters?
- How can we ensure the security reliable unique data fires?
- How do out organizations policies affect assessment?

ICANN58 Brainstorming

iB: May assess conformance with appropriate security contingency planning framework for the Internet's system of unique identifiers

*Extracted from the SSR2 scope brainstorming session at ICANN58

How Do We Assess

- Definition of scope of "Internets system of unique identifiers?"
- When it says conformance, to what extent?
- Overall process the implication of security, stability, and resiliency of DNS as per bylaws?
- What are the key point who address secure reliable and stable DNS?
- How can we address the "operational issue?"

IANA Transition

- What is the impact of moving the IANA services to PTI? How will this be monitored?
- What contingency planning has taken place as a result of the CWG/CCWG

Contingency planning

- What measures are taken to ensure relevance and applicability of the contingency plan?
- Contingency planning framework, what does that mean four, DN, protocols, addresses?
- What is the appropriate security contingency planning framework?
- Who is responsible for the current contingency plan?
- What is meant by "the appropriate security contingency planning framework"?

Uncategorized

- What is ICANN doing in the area of interoperable security STDs to monitor? (ITHI)
- How the end-user feel secure, reliable, instable
- Does this review look only internally and ICANN process?
- Who is responsible for the maintenance and upkeep of the [unreadable]

ICANN58 Brainstorming

iC: May assess maintaining clear and globally interoperable security processes for those portions of the Internet's system of unique identifiers that ICANN coordinates.

Definitions

- What is meant by "globally interoperable security processes"?
- What aspects of the unique identifier space is relevant to the definition of quote "security processes"?
- This is IETF, No?

Abuse (gTLD and ccTLD)

- gTLD abuse mitigation
- Global abuse policies recommendations
- How does ICANN compliance impact SSR?

gTLD compliance analysis

- What are the SSR issues with new GTLD's?
- ccTLD abuse mitigation

*Extracted from the SSR2 scope brainstorming session at ICANN58

Assess effectiveness

- How effective is ICANN's coordination effort with IETF and others?
- How effective or ICANN's security efforts to known threats and preparation for future threats?

Emerging Trends

- What emerging technologies are trends should we consider?

Uncategorized

- Root server stability, security
- How DNS works with secure reliable and stable [look up text]

Outreach Plan & Next Steps

Outreach Plan & Next Steps

- Review current outreach mechanisms, objectives, draft outreach target list
- Based on work plan, what groups should the RT outreach to and what's the objective?
- What opportunities should we use for outreach efforts, eg. conference calls, meetings?

Draft Outreach List

https://community.icann.org/pages/viewpage.action?pageId=64076120&preview=/64076120/64078800/SSR2%20Draft%20Outreach%20List%2028March17.docx

- ICANN Groups
  - Security Stability Advisory Committee (SSAC)
  - Governmental Advisory Committee (GAC)
  - GAC's Public Safety Working Group (PSWG)
  - Root Server System Advisory Committee (RSSAC)
  - At-Large Advisory Committee (ALAC)
  - Generic Names Supporting Organization(GNSO) constituencies (see list on website)
  - Country Code Names Supporting Organization (ccNSO)
  - Address Supporting Organization (ASO)
  - Board
  - Board Technical Experts Group (TEG)

Draft Outreach List (cont.)

- SSR1 Review Team
- Internet Engineering Task Force (IETF)
- IAB
- World Wide Web Consortium (W3C)
- Regional Internet Registries (RIRs)
    - African Network Information Center (AFRINIC)
    - Asia-Pacific Network Information Centre (APNIC)
    - American Registry for Internet Numbers (ARIN)
    - Latin American and Caribbean Network Information Centre (LACNIC)
    - Réseaux IP Européens Network Coordination Centre (RIPE NCC)

Draft Outreach List (cont.)

- Regional country code top-level domain organizations
  - African TLD Organization (AFTLD)
  - Council of European National TLD Registries (CENTR)
  - Asia Pacific TLD Organization (APTLD)
  - Latin American and Caribbean TLD Organization (LACTLD)

- Anti-Phishing Working Group (APWG)

- Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG)

Items Requiring Additional Discussion & AOB

Recap of Action Items & Closing Remarks