From SSR2 RT Face-to-Face Meeting Madrid 15 May 2017
20170522 Draft 1.0

SSR2 Topics

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	1. Complete the assessment of the implementation of SSR1 recommendations, the impact of the implementation, how the post implementation is being managed and what implications for the SSR2 review. 2. With regards to SSR1, implementation of Rec 7, 10, 11 and 27, to see to what extent the current OCTO research feeds into the risk management framework especially in relation to the SSR of unique identifier space. 3. Risk Assessment and Management relevant to SSR 4. What are the indicators for "successful" implementations and intended effects? 5. What are the key performance indicators? 6. How do we get an understanding of what SSR1 recommendations have been implemented? 7. Which extent of SSR1 recommendations implemented? 8. How does ICANN compliance impact SSR? 9. Define a set of metrics to measure the effectiveness of the implementation 10. Note about SO/AC recommendations on security including R/SSAC?
Team Members	Denise, Alain
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	1. Scope of ICANN's SSR responsibilities: action zone, influence zone, coordination zone. 2. Effectiveness of ICANN's SSR framework, SSR Plan and its implementation. 3. Physical security requirements in place and enforcement of minimum security specification for DNSSEC key storage Facility. 4. Level of compliance requirement for registrars agreements 5. SLAM and performance indicators 6. ICANN's role in helping to mitigate DDoS 1. Operational 2. Other (Lroot, zone ICANN is resp for, domain name contractual obligations/compliance, security training) 7. Measures and metrics (incorporate in all topics and subteams) - What are, and how can the community measure the relevant DNS abuses - The evidence base: DNS health index and abuse data. What the evidence tells us; access to information (risks and benefits) 8. ICANN's internal security, stability and resiliency operations: - Allocation of resources and priority within the organisation (includes budget and staffing) - Outreach and public information role (training, vulnerability disclosure, system attack mitigation etc) - Risk management, compliance with relevant frameworks. 9. White-hat operations - What are the white-hat operations that are taken in ICANN space that may need exceptional handling (gratis for registering sink-holes, etc.) (can this be included in improving security of unique identifiers/threat mitigation?) 10. 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. 11. Due to ICANN's orientation to ISO/IEC 27001 (and ISO 22301? - BCMS) I would recommend to provide a gap-analysis to the normative requirements of the management part and Annex A of the ISO standard based on the SoA (Scope). 12. Perform interviews and review descriptions and evidence of: * ISMS / BCMS Scope * Information security policy * Information risk assessment

	and risk treatment processes * Information security objectives * Information security roles and responsibilities * ISMS internal audit program and results of conducted audits * Operational planning and control documents * Evidence of top management reviews of the ISMS (Note: Gap assessment only) 13. Various others from the Annex A like rules for acceptable use of assets, access control policy, operating procedures, confidentiality or non-disclosure agreements, secure system engineering principles, information security policy for supplier relationships, etc. (Note: Gap assessment only) 14. Categorize and prioritize the outcome of the analysis 15. Develop a short-, medium- and long-term schedule to implement different controls in accordance to the requirements 16. Define a set of metrics to measure the effectiveness of the implementation (Note: Items 12 – 16 linked) 17. Analyze policies and procedures that are essential to ICANN identifier systems activities 18. Analyze ICANN internal procedures essential for SSR of the organization and global operations 19. Business continuity planning 20. Security Framework 21. Incident response planning 22. Coordinated Vulnerability Disclosure Process 23. Assess ICANNs ability to respond to strategic threats to the unique identifiers it coordinates.' 24. Vetting process for EBERO operators. 25. ICANN processes around vetting registry operators - Nick Shorey observer 26. Corporate Data Security and/or Business Systems 27. What is the scope of ICANN's threat modeling? 28. How effective it is ICANN risk management? 29. If I how ICANNs security efforts related to the DNS? 30. How ICANN measures the effectiveness as security efforts? 31. What are ICANN's security efforts? (x2) 32. Review ICANN security procedures. 33. How are we distinguishing operational stability and security from measures that stem from compliance issues? 34. What does "interoperable security processes" mean? 35. What is the current state of ICANN and disaster and operational recovery planning? 36. What is the appropriate security contingency planning framework? 37. What is ICANN doing in the area of interoperable security STDs to monitor? (ITHI)
Team Members	James, Denise, Boban, Noorul Ameen, Kerry-Ann
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	1. Universal resolvability: Can identifiers be uniquely resolved and consumed? – Alternate root – Name collisions (status and remediations) – Universal resolvability and the internet of things – IPv6 / CGN complexity (query the role of ICANN on this?) – Nation state firewalls 2. ICANN role in Improving the security of unique identifiers (includes threat mitigation) – Authoritative domain name servers – Domain name registration data, registries, registrars, and registrants – IP addresses and autonomous system numbers (ASNs) employed by the global Internet routing system (Note: Will continue to flesh out exact role of ICANN) 3. DNSSec (progress, Key rollover) 4. Domain name abuse mitigation as it affects SSR issues (Note: More info on ICANN's specific role is needed) 5. Universal acceptance: Can identifiers be consumed by clients – IDNs and new gTLDs – Platforms, approaches, and status 6. Proactive measures (Advisories, Technical alerts) 7. Analyze universal accessibility and resolution of unique identifiers systems 8. Assess DNS threat landscape, domain abuse, and mitigation relevant to ICANN's role 9. What are the actual and potential challenges and threats? 10. Which portion of the Internet systems of unique identifiers does ICANN not coordinate? 11. What are the SSR issues with new gTLD's?
Team Members	Emily, Alain, Cathy, Matogoro, Ram Krishna, Geoff, Mohamad Amin Hasbini
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	1. How do we assess ”Future challenges to security and stability a DNS?” 2. Explore forecasting research on the Internet unique identifiers 3. What has been, or could be, the impact of the evolution and the number and types of devices in the DNS? 4. How effective are ICANN’s security efforts to known threats and preparation for future threats? 5. What emerging technologies are trends should we consider?
Team Members	Emily, Kerry-Ann, Matogoro, Mohamad Amin Hasbini
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	1. What are the changes to ICANN SSR with the IANA transition? 2. Business continuity plan for new IANA functions operator (Note: C7.3 replacement)
Team Members	Cathy, James
Rapporteur	

Other

Topic	Other
Related Bylaw	
Skillset	
Description of activity	
Work Items	1. What are the indicators the SSR2 would want to use to measure “success” of security efforts? 2. Collect input from the community on how ICANN should improve on SSR 3. How effective is ICANN’s coordination effort with IETF and others?
Team Members	
Rapporteur	

Orphan topics (not assigned to any of the above categories):

1. Analyze the possibilities for faster exchange of information on methods of abuse of Internet unique identifiers and recommendations for mitigation
2. What are the benchmarks and good practices for successful security efforts? (note duplicates)
3. How can we measure “the extent” of ICANN’s success in implementing security efforts?
4. How the end-user feel secure, reliable, instable (Note: avoid duplication of CCT research)
5. Root server stability, security