Working Document

SSR2 Topics

Overarching matters include:

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

Sub Topic 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, Ram Krishna
Rapporteur	Alain

Sub Topic 2 – ICANN SSR

Topic	ICANN SSR
Related Bylaw	4.6 (c)(ii)(A) 4.6 (c)(ii)(B) 4.6 (c)(iii)
Skillset	Information Security Management (ISM), Audit (AUD), Risk Management (RM), Business Continuity Management (BCM), Legal (LG)
Description of activity	The sub team will be responsible for reviewing the completeness and effectiveness of ICANNs internal security processes, the effectiveness of the ICANN security framework, and SSR activities performed or led by ICANN.

Work Items - Key Action Steps	1. Perform a comprehensive assessment of ICANN's internal security, stability and resiliency operations processes. This includes, but is not limited to:
	- Allocation of resources and priority within the organization (includes budget and staffing)
	- GDD Operations
	- Centralized Zone Data Service
	- SLAM (Arias)
	- [get list from Staff of additional items, include all public facing services]
	- Outreach and public information role (training, vulnerability disclosure, system attack mitigation etc)
	
	2. Perform a comprehensive assessment of ICANN's Information Security Management System - best practices, standards and certification-related processes (e.g SOC 2/3, ISO 27001). This includes, but is not limited to:
	- Definition of a scope - based on a service-oriented view
	- Perform a gap-analysis (interviews and review descriptions / evidence) based on best-practices, etc.
	  - Leadership, roles and responsibilities
	  - Risk management and risk treatment
	  - Resources, competence, awareness and communication
	  - Access control and Cryptography
	  - Physical and environmental security
	  - Operational security
	  - System acquisition, development and maintenance
	  - Supplier relationships
	  - Categorize and prioritize the outcome of the analysis
	- Summarize all the (non)conformities and write an audit report
	
	3. Perform a comprehensive assessment of ICANN's Business Continuity Management System - best practices, standards and certification-related processes (e.g SOC 2/3, ISO 22301). This includes, but is not limited to:
	- Definition of a scope - based on a service-oriented view
	- Perform a gap-analysis that covered the following domains:
	  - Business Continuity Objectives and Plans
	  - Operational planning and control
	  - Business Continuity Strategies
	  - Prioritised Activity Recovery Strategy
	  - Resource Recovery Strategy

	- BC Procedures - Incident Response Structure - Business Continuity Plans (BCP) - Evaluation of Business Continuity Procedures - Categorize and prioritize the outcome of the analysis - Summarize all the (non)conformities and write an audit report 4. Perform an assessment how effectively ICANN has implemented its Security Incident Management Process to reduce (pro-active) the probability of DNS-related incidents. - List general categories of incidents, eg DoS, etc. - ICANN operational responsibilities - L-Root - ICANN is resp for, domain name contractual obligations/compliance - security training - Action: Conduct gap analysis, document lessons learned 5. Perform an assessment how effectively ICANN has implemented its Security Incident Response Process relating to a global incident?: - assist / conduct interested parties - Action: Conduct gap analysis, document lessons learned 6. Perform an assessment how effectively ICANN has implemented its processes around vetting registry services. This includes, but is not limited to: - Back-End Registry Operator (BERO) - Emergency Back-End Registry Operator (EBERO) - Registry Data Escrow (RyDE) - Data Escrow Agent (DEA) - Centralized Zone Data Service (CZDS) - Bulk Registration Data Access (BRDA) - SLA Monitoring System (SLAM) - Categorize and prioritize the outcome of the analysis - Summarize all the (non)conformities and write an audit report 7. [new item] Registrar-related SSR - ICANN Compliance sub-items (Level of compliance requirement for registrars agreements) 8. [new item] IDNs - The evidence base: DNS health index and abuse data. What the evidence tells us; access to information (risks and benefits)

	9. WHOIS issues - Accuracy, Privacy and Proxy Services - VPNs,TORs,VPS 10. Root server Security Issues (Need discussion) - RFC 2870 Compliance - Issues with anycast servers

Team Members	James, Denise, Boban, Noorul Ameen, Kerry-Ann, Žarko, Norm, Eric
Rapporteur	Boban

Sub Topic 3 – DNS SSR

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\zxccvbbbnmmmnnnw? - 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	Alain, Cathy, Matogoro, Ram Krishna, Geoff, Amin Hasbini, Žarko, Eric, Don, Boban
Rapporteur	Geoff

Sub Topic 4 – Future Challenges

Sub Topic 4 – Future Challenges	
Topic	Future 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.
Topics for Consideration	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? [new items to discuss] : ● ICANN OCTO Middleware research ● ICANN Emerging Technologies (ask ICANN) ● Internet Governance issues ● Privacy regulation i.e. GDPR

Definitions	**Assets** – What are we trying to protect. Attackers can use an Identifier System(s) to target and attack property, information, or people, e.g., by using the DNS to implement denial of service attacks. They can also attack aspects of an Identifier System by using it in a manner that is abusive or malicious, for example, by using fraudulent registration information or hijacking names or addresses. Importantly, these forms of attacks can be executed in tandem. Each of these assets performs a different critical function; a specific attack against one may threaten the security, stability, or resiliency of the Identifier System as a whole. These assets include: ● Authoritative domain name servers and recursive and stub resolvers, as well as domain name registration data, registries, registrars, and registrants. ● IP addresses and autonomous system numbers (ASNs) employed by the global Internet routing system, along with associated network infrastructure components (e.g., routers, switches, address management systems) and regional Internet registries. Protocol parameters and the implementations of the associated protocols that make use of those parameters, both individually and within the context of larger systems that incorporate those protocols and protocol parameters. **Vulnerabilities –** Weaknesses or gaps that can be exploited. Vulnerabilities may be flaws within Identifier System assets themselves, or within measures intended to protect them. These vulnerabilities include design defects, coding errors, configuration mistakes, and other gaps that weaken an asset's attack resistance, stability, or resiliency. **Threats –** What we're trying to protect against. Threats include both entities and events which may exploit an asset's vulnerabilities. Threats to Identifier System assets include attacks against domain name servers and name resolvers, or network elements such as routers or switches. The threat landscape includes attacks against domain and address registration services as well as natural disasters such as storms that trigger

	power and network outages which degrade Identifier System operations. **Risk –** The probability that threats will exploit vulnerabilities to obtain, damage or destroy assets. In this document, we attempt to identify high-risk types of attacks against Identifier System assets. To do so, we focus on high-impact vulnerabilities that are being actively exploited by threats, as well as new vulnerabilities at high risk of exploitation.

Work Items/ Areas of Focus	**Top Identifier System Attacks** ● Route Insertion Attacks ○ As it affects the unique ID system (what could happen, how it could be prevented, etc.) ● Coalescence of registry/backend operators for multiple TLDs ○ Multitudes of victims for one high-value compromise/outage/etc. ■ DNS Denial of Service Attacks (coordinate w/other Sub-Topics) ■ DNS DDoS Attacks ■ Web Services Attacks impacting Identifier Resources ■ Software ■ Resource Registration Account Compromises ● Identifier Hijacking via Social Engineering ● DNS Zone File Attacks ○ ? ● Parallel Root Name System Risks ○ Namespace ambiguity/competition/etc ● DNS and Surveillance Attacks ○ Undermining DNS' utility and perceived trustworthiness ● DNS Misuse as Covert Channel ○ How the attacks (TTPs) are evolving to use identifier spaces in new ways ○ Empower ICANN to investigate attacks that are using new and more sophisticated TTPsBo **New dependencies:** ● New crytpo-systems in DNSSEC ○ Can DNSSEC continue to offer security in the future and evovle where it needs to (e.g. PQ) ● New uses for DNS (IoT, etc.) ○ Can the DNS evolve as new systems use it ● ~~Threat Intelligence blindspots~~ ○ ~~When technologies like QName Minimisation [sic] and DNS over TLS hide necessary telemetry from whitehats, miscreants have more latitude~~ ● Alternate naming systems (interactions, conflicts, etc.) ○ Namecoin, ● Censoring

	● Loss of confidence in standards bodies ● Adoption of systems that don't adhere to standards **Performance security (SSR2 scope):** *Issue high level recommendations towards ICANN technologies(routing, switching, computing environments, DNS related services) resources utilization (Traffic, processing/power/memory utilization, ...)* ● Identify a list of the types of technologies used by ICANN ● Recommend forecasting techniques to be used by ICANN to determine future utilization ● ICANN role in return: Recommendations need to be considered in future technological planning or architecture designs by ICANN. **Technology selection security (SSR2 scope):** ● Vendor security technology evaluation process (how to test solutions) ● Vendor security technology selection process (how to select a solution) ● Vendor security technology implementation process (what vendors need to do when deploying solutions) ● Vendor security maintenance process (how vendors should maintain their solutions) ● Vendor responsibilities and SLAs (patching vulnerabilities, technology development/deployment) ● Vendor accountability for security problems ● ICANN role in return: Selection recommendations need to be considered in future technology selection processes employed by ICANN **Threat intelligence (SSR2 scope):** ● The need for an ICANN threat intelligence team ● The need for ICANN to have established communication with top threat intelligence sources to know about the latest threats ● The need for adapting threat intelligence internally, to identify attacks and threats accordingly ● ICANN role in return: Threat intelligence recommendations to be adapted by ICANN towards enhancing blocking of cyber-attacks, identifying causes of new breaches, and knowing about the latest threats endangering similar organizations.

	NB1:Recommendations provided should be vendor/technology neutral, as to be valid for future utilization NB2: issues of DDOs, route injection all fall under “Sub Topic 3 – DNS SSR” as they are issues probably currently being dealt with. What is not dealt with, is how they could be used in the future, which falls under threat intelligence. I do not believe should predict protocols misuse options through new vulnerabilities, which has an unlimited scope.

Team Members	Kerry-Ann, Matogoro, Amin Hasbini, Noorul Ameen, Eric, Denise
Rapporteur	Kerry-Ann

Sub Topic 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, Geoff, Eric
Rapporteur	James

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