

Questions on FY14 Framework

ICANN appears to have vested the primary implementation of SSR-related activities within the Security team. Some comments received suggest that this may be too narrowly based and that a more appropriate strategy is for the matrix organization scheme to be adjusted to incorporate SSR functions. How will ICANN ensure SSR-related enhancements are applied appropriately to the organization as a whole?

Given the large area encompassed by ICANN's SSR-related efforts and a limitation on resources, prioritization of activities becomes a critical issue. What concrete mechanisms exist or are planned to allow for prioritization in an open, transparent, and accountable fashion?

The Framework tends to have a much greater focus on DNS issues rather than security/stability/resiliency of the Internet's unique identifier system as a whole. For example, page 7 "The Challenge" speaks of "attacks against the DNS and global networks" and "DNS attacks target [everybody]", the trends mentioned on page 8 and 9 are exclusively DNS oriented, the "Relationships in SSR" mentioned on page 12-13 discuss domain name registration processes, etc. In terms of openness, transparency, and accountability, how was this focus chosen?

Some definitions used within the Framework appear to have come from discussions in large part DNS Security Symposia. Who participated in those symposia? How were attendees selected? Is this an ongoing series of meetings? Who organizes the meetings?

What efforts are being undertaken by ICANN to identify and mitigate particularly vulnerable sectors of the Internet's system of unique identifiers (e.g., operationally vulnerable ccTLDs)? How is that identification and mitigation done in an open, transparent, and accountable manner?

Questions on Recommendation Status:

Rec	Question(s)
1	Can a pointer to a summary of change requests (based on public comments) and revisions to the "single statement of [ICANN's] remit and limited technical mission" be provided?
2	Has a review been done? If so, can a pointer to the schedule and process of the review of ICANN's definition and implementation of its SSR remit and limited technical mission" be provided along with a summary of feedback received and how ICANN determined consensus?
24	What is the charter of the "Chief Security Office Team"? What process was used to establish that charter? Is there a more full description of the roles and responsibilities of the team members?
18	When is the operational review performed?

7	My interpretation of this recommendation is that ICANN should establish a clear set of SSR objectives and prioritize according to those objectives. What is the process by which those SSR objectives are established? Have those objectives been defined? If so, what mechanism was used to establish priorities?
8	What is ICANN currently doing to maintain/drive DNS availability? How have the Strategic Plan objectives been refined to continue that effort?
17	What is the internal process for showing how activities relate to SSR Framework defined goals? What are the reporting timeframes? What will be reported and how?
20	Status of publication of information relating to current and future budget/organization related to SSR implementation?
21	Can ICANN provide preliminary information regarding the underlying cost-benefit analysis?
9	Webtrust is relevant to DNSSEC but not to corporate certification. Can a pointer be provided to the “clear roadmap” towards certification?
10	Can a pointer be provided that documents the resources provided to contractual compliance enforcement? Can a pointer be provided which describes the “structured process for monitoring compliance issues and investigations”?
11	Can a pointer be provided to the SSR-related program objectives for finalized measures of success for new gTLDs and fast track IDNs? Can a pointer be provided that describes the measurements for effectiveness to mitigate domain name abuse?
22	Can a pointer be provided to where the organization and budget resources needed to manage new gTLD SSR issues has been published? What mechanisms are in place to monitor new gTLD SSR issues? Can a pointer be provided to the documentation related to documentation and their updates related to new gTLD SSR-related issues?
25	Can a description of mechanisms for identifying near- and long-term risks and strategic factors related to Risk Management be provided?
26	Can a project plan with milestones for ICANN’s Risk Management Framework be provided?
27	--
15	Can a pointer be provided to documents that list ICANN’s actions as “facilitator in responsible disclosure/dissemination of DNS security threats and mitigation techniques”?
28	Can a pointer be provided to documents that list ICANN’s root zone monitoring, threat detection and mitigation efforts? Is ICANN engaging in detection and mitigation of threats outside of the DNS? Can a pointer be provided to documentation describing ICANN’s efforts in distributing threat and incident information?
3	Can a pointer be provided to the definitions ICANN uses for its terminology and descriptions? Can the schedule of training and training materials be provided?

4	Can a project plan with milestones be provided for the definition and documentation effort? Can ICANN describe how it will provide “a single focal point for understanding the interdependencies between organizations”?
5	Can a pointer be provided to a comprehensive list of SSR goals, the SSR relationships associated with those goals, and how ICANN is maintaining effective working relationships?
14	Can a pointer be provided to documentation that details what outreach activities are being done and how that has changed over time?
16	Can a pointer be provided to documentation that describes input derived from outreach efforts? What is the process for obtaining “systematic input” from other parties?
6	Can a project plan with milestones be provided for the publication of the document outlining SSAC and RSSAC roles and responsibilities?
12	Can a pointer be provided to documentation that lists SSR-related best practices? Beyond the revised new gTLD registry agreement, what agreements, MOUs and other mechanisms have been modified to support those best practices?
13	Can a pointer be provided to documentation that details actions by ICANN to encourage each Supporting Organization to develop and publish SSR-related best practices?
19	Can a project plan with milestones be provided for the deployment of the Dashboard?
23	Can a pointer be provided to the inventory of SSR-related working groups an AC activities?

appendix b

global security engagement: url for proceedings? attendees? open attendance?

collaboration (RIPE Atlas): form of contribution?

collaboration (root zone automation): cost/timeframe/etc.?

collaboration (lea/opsec training): materials?

mechanisms by which folks can request training/etc.?