FY 11 Update to ICANN Plan for Security, Stability & Resiliency (SSR)

Summary and Analysis of Comments

ICANN conducted a public comment period on the *FY 11 Update to the Plan for Enhancing Internet Security, Stability and Resiliency (SSR)* from 13 September to 13 October 2010. Based on an informal request from the At Large community, the comment period was extended on 4 October 2010 to 3 November 2010. Seven comments were received in the forum, along with 4 questions and responses from a briefing to the At Large community conducted on 18 October 2010.

In addition, staff conducted briefings on the SSR Plan and ICANN activities in SSR during the comment period on the following dates:

- Security & Stability Advisory Committee – 9 September 2010, 22 October 2010
- RIPE NCC Regional Meeting (Moscow, Russian Federation) – 29 September 2010
- Commercial Stakeholders Group (Washington, DC) – 12 October 2010
- At Large community (remote briefing) – 18 October 2010
- Internetdagarna (Stockholm, Sweden) – 26 October 2010
- Organization of The Islamic Conference-CERT meeting (Kuala Lumpur, Malaysia) – 28 October 2010

Summary of Comments

ICANN received input on the FY 11 SSR Plan from individuals in DNS and academic research communities, top-level domain registry operators, Internet organizations, and business users. A detailed analysis of these comments is provided below. Revisions will be made to the FY 11 SSR Plan based on the comments received.

ICANN also received input during the briefings listed above, which included a suggestion that ICANN clarify the title as it may be perceived as overreaching beyond ICANN's role, and that ICANN provide a definition for resiliency in a future version of the SSR Plan. Commenters suggested several citation updates and corrections so that the plan would be consistent with current work (such as reports related to root scaling, possible revisions to the Registrar Accreditation Agreement, an inventory of WHOIS service requirements, RPKI, and DNSSEC implementation).

Main Themes

1. Commenters generally supported the description of ICANN's role in security, stability and resiliency of the unique identifier system, but asked for clarification that ICANN does not expand beyond its mission. Commenters suggested that ICANN focus on its mission on core threats to the DNS itself.
2. Corrections should be made to the Contractual Compliance section to clarify that compliance remains a priority and that ICANN will work with the broader community, rather than only contracted parties.

3. Commenters stated there is a real need for a system-wide risk assessment, threat analysis and to assess how best to embed DNS expertise in the existing computer and network security response capability.
4. Several commenters noted ICANN work in DNSSEC implementation and in DNS capacity building initiatives as positive examples of ICANN's work in DNS security, stability and resiliency.

The comment forum can be viewed at http://forum.icann.org/lists/ssr-plan-fy11/.

Detailed Analysis

Stakeholder Comments – Individuals from DNS and academic research communities

Comments in this category included input from Eric Brunner-Williams, Dev Anand Teeklucksingh and Sivasubramanian Muthusamy via the Adobe Connect chat as part of the At Large briefing on 18 October 2010. At the request of At Large Advisory Committee (ALAC) Chair Cheryl Langdon-Orr, questions provided into the Adobe Connect chat session were posted into the comment forum with staff responses on 26 October 2010. Separately, Nevil Brownlee, Computer Science Department at the University of Auckland, provided a comment into the forum on 3 November 2010.

Nevil Brownlee

Brownlee noted that as an active member of the DNS research community, he would like to see the FY 11 SSR Plan made stronger by incorporating projects related to actual measurement and monitoring. He cited ICANN's report from the February 2010 Global DNS SSR Symposium in Kyoto, Japan on Measuring Health of the Domain Name System (http://www.icann.org/en/topics/ssr/dns-ssr-symposium-report-1-3feb10-en.pdf) as an example that more should be done to define what DNS health should mean to researchers, service providers, and ordinary Internet users.

Brownlee stated there are many DNS measurement projects underway in the global Internet research community, and he would "like to see ICANN devote some real effort to supporting DNS research, and working with the Research Community to ensure that its research outcomes are deployed and used to improve DNS service at all levels."

ICANN's Security team would welcome greater involvement from the research community and will look at opportunities to involve the research community in ICANN's SSR activities.

Eric Brunner-Williams

During the At Large briefing, Brunner-Williams suggested "if there is a conficker variant off of last year's .c variant (used the dns for rendevouz points), letting last years -dns list know is an option. A lot of the -dns people dropped off, so jc [John Crain] may need to do something more than just pick up the phone."

Staff responded "A table showing Conficker variants is included in the Conficker Summary & Analysis, which was published on 7 May 2010 (http://www.icann.org/en/security/conficker-summary-review-07may10-en.pdf). There are not just Conficker variants but also other malware that uses the same domain name generation idea. John Crain is leading ICANN's participation in the Conficker Working Group, and the working group is supposed to be discussing goals for 2011. Staff agrees that picking up the phone won't be enough, and further discussions with the working group and TLD operators will continue on best mechanisms for dealing with Conficker."

On 2 November 2010, Brunner-Williams added he concurred with the Registry Stakeholder Group (RySG)'s urging that the FY 11 SSR Plan be amended to provide:

- A clear recognition that the industry's security mission is focused on core threats to the DNS itself. (Note – Brunner-Williams substituted "industry" for ICANN)
- "I also concur with the RyC's expression of preference for transparency and process, and their rejection of 'WHOIS' as an issue of comparable import."

Independently, he urged that the FY 11 SSR "Plan be amended to provide for the reduction of economic, ownership, and trust (EOT) barriers to research access to authoritative, and recursive resolver operational data." Staff notes that there is not currently policy under development on this topic, but that ICANN does participate in data sharing activities with other operators such as DNS-OARC (https://www.dns-oarc.net/). This is similar to the point raised by Nevil Brownlee, supporting improved work with the research community to better understand DNS behaviour.

Dev Anand Teelucksingh

Teelucksingh asked "Regarding ICANN Contractural Compliance, previous briefings from Contractural Compliance at ICANN meetings that Contractural Compliance appears to be understaffed to adequately perform compliance of the 20+ gTLD registries and the 900+ registrars of gTLDs. How/Can the Contractural Complance Dept. be able to implement the increased scope of compilance activities due to the SSR plan?"

Staff responded: "ICANN is currently seeking interested candidates for several positions on the Contractual Compliance team. You raise a good point about Compliance and this is a focus area for ICANN. Compliance will be working collaboratively with the law enforcement community and Internet community as a whole to identify contracted parties that may be engaged in malicious activity."

Based on this comment, and comments received from the Coalition for Online Accountability and Microsoft Legal & Corporate Affairs, the FY 11 SSR Plan will be updated to clarify that "The Contractual Compliance Department will continue to aggressively enforce ICANN's registrar and registry contracts in the interest of protecting registrants and encouraging public confidence in the DNS."

Sivasubramanian Muthusamy

Muthusamy asked "What are the targets for the DNSSEC program? Root Servers + Registry Servers ? Also National Internet Exchanges? What else?" He also asked "Has the Security and Stability program looked at all targets and is there a plan to make this an all inclusive exercise?"

The responses to his questions were provided as follows:
DNSSEC for the root zone is a joint effort between ICANN and VeriSign, with support from the U.S. Department of Commerce. Final deployment of DNSSEC has been completed in the root zone, meaning, all root server operators are serving the production signed root zone). ICANN is supporting efforts by all registry operators to sign TLD zones, and efforts to extend the chain of trust through to registrars. Information on DNSSEC for the root zone is available at http://www.root-dnssec.org/. In addition,

DNSSEC is a requirement for delegation in the draft Applicant Guidebook for the new gTLD process.

Implementation of DNSSEC in the root zone was a major step, involving substantial work from the technical community, VeriSign & the U.S. Department of Commerce. There is more work to be done, and ICANN staff (particularly ICANN's DNS Operations team, http://dns.icann.org/ksk/) will be working to educate, provide support and facilitate the adoption of DNSSEC across the spectrum by registries, registrars, and end users. While particular targets for DNSSEC adoption have not been set in the FY 11 SSR Plan, that is a suggestion that can be made in ICANN's upcoming 2011-2014 Strategic Plan and the FY 12 Operating Plan cycle. You correctly note that some of these targets may be beyond ICANN's relationships with registries and registrars, but ICANN intends to conduct outreach to promote DNSSEC adoption by the broader community.

Registry Operators, TLD Associations and Internet Organizations

Inputs in this category were received from the Internet Society, Nominet, and the Registries Stakeholder Group (RySG).

The Internet Society

ISOC noted its support for the Plan's statement of scope on ICANN's role. While it shares with ICANN the recognition of the importance of the stability, security and resiliency of the Internet's routing system, ISOC raised some concern with the language in the Plan addressing Resource Public Key Infrastructure (RPKI), as the section "could be seen as describing an inappropriate interpretation, which leads to an unfounded assertion of ICANN and IANA's role in operating a trust anchor repository for the RPKI standard being developed at the IETF."

ISOC does not see the basis for asserting ICANN's acquisition of such a strategy or responsibility.

ISOC suggested that the text in the SSR Plan be "adjusted to reflect ICANN's role as collaborator in RPKI implementation (through the IANA functions) and ultimately, maintainer of the root trust anchor (as ICANN, through the IANA functions, is the maintainer of the DNSSEC root trust anchor), not as having provided a basis for ICANN to acquire strategic responsibilities for the stability, security and resiliency of the entirety of the Internet's routing system."

ISOC's feedback on the RPKI section is welcomed. ICANN's technical experts within the DNS Operations and IANA functions teams are actively participating on the development of RPKI. Staff will clarify the section on RPKI that ICANN is not claiming to own the strategic responsibility for the security, stability and resiliency of the routing system.

Nominet

Nominet welcomed the opportunity to comment on the FY 11 SSR Plan but indicated disappointment that the FY 11 SSR did not incorporate the feedback received during the comment period on the Security Strategic Initiatives paper which closed in May 2010 (http://www.icann.org/en/public-comment/summary-analysis-strategic-ssr-initiatives-and-dns-cert-business-case-24may10-en.pdf).

Nominet asserts "there appears to be a real need to do a more complete risk assessment and gap analysis and to assess how best to embed DNS expertise in the existing computer and network security response capability, ensuring the best use of existing networks."

This point is consistent with the proposal for a more system-wide risk analysis from ICANN's Security Strategic Initiatives paper dated February 2010, and consistent with feedback received on that document. A Joint Security and Stability Analysis Working Group is also being formed with representatives from ALAC, ccNSO, GNSO, NRO and independent experts. Staff notes that the comment period on the Strategic Initiatives paper closed after the development of ICANN's FY 11 Operating Plan and Budget, but risk assessment initiative could be included into the FY 12 Strategic and Operating Plan process. The working group could also suggest alternative models of funding or structures to conduct a system-wide risk assessment in collaboration with the DNS community.

Nominet expressed its support for ICANN's capacity-building initiatives by working with other organisations. "We recognize the importance of a culture of emergency preparedness in the DNS community and of embedding best practice across the industry." Nominet raised some concern that many of its initiatives do not involve the DNS industry, such as its engagement with the Forum for Incident Response and Security Teams (FIRST).

Nominet asked for more detail on the ccNSO's involvement on the Attack & Contingency Response Planning or Registry Operations Course. Staff notes that ICANN, in partnership with the Network Startup Resource Center & ISOC, recently conducted a registry operations training course at the APTLD meeting in Amman, Jordan (2-6 November 2010). A similar course was conducted in Mali for AfTLD in September 2010. Details on the ccTLD Capacity Building Initiative are available at https://nsrc.org/trac/cctld/. Staff will update the SSR Plan with more information on this initiative.

Nominet also identified an omission on page 53 for deliverables of e-IANA implementation. This will be corrected in the updated document. Nominet notes that there is no discussion of IPv4 exhaustion and any security, stability or resilience implications, but section 5.1.1 of the Plan describes ICANN work with the RIRs on IPv4 exhaustion.

Finally, Nominet notes that it would be useful for the Plan to mark clearly those activities from the 2009 Plan that have been completed. This is a good point, and is preparing a chart to include with the updated plan showing completed activities from the 2009 Plan.

Registries Stakeholder Group (RySG)

The RySG submitted a consensus comment from the gTLD registries stakeholder group, appreciating ICANN's commitment to the security, stability and resiliency of the DNS. The RySG was generally pleased with the description of ICANN's role one pages 2-3, noting it "is important for ICANN to acknowledge and communicate its role, and to avoid 'mission creep' into areas outside of ICANN's mission." The RySG noted ICANN's withdrawal from operating a DNS-CERT was an appropriate choice as this was outside ICANN's role.

The RySG stated that ICANN should provide very specific examples of anticipated participation in activities with the broader Internet community to combat abuse of the unique identifier systems, as this statement is likely to be perceived as ICANN preparing to move beyond its scope and mission.

The RySG expressed its support for core DNS risk assessment and threat analysis, and requested that the FY 11 Plan be amended to provide:

- Assurance that there will be transparency and use of community processes in efforts to establish metrics, assessments and programs regarding health of the DNS and threats to its security and stability, including an assurance that SSAC will be a central participant in such efforts.

- A clear recognition that ICANN's security mission is focused on core threats to the DNS itself.

On WHOIS, the RySG noted that staff omitted the Inventory of WHOIS Service Requirements paper published in July 2010, http://gnso.icann.org/issues/whois/whois-service-requirements-final-report-29jul10-en.pdf. This omission will be corrected and a reference to the report will be included in the updated document.

Business Community

Comments were received from the Coalition for Online Accountability and Microsoft Legal and Corporate Affairs.

Coalition for Online Accountability

The Coalition for Online Accountability (COA) comment focused on two areas: 1) improvements to the Registrar Accreditation Agreement (RAA), and 2) contractual compliance. On the RAA, the comment identifies an omission on page 37 of the document – the Plan does not reference the recent work of a drafting team composed of GNSO & ALAC representatives on possible amendments to the RAA. COA is correct, and the SSR Plan will be updated to include this information. The final report on possible improvements to the RAA was published on 18 October 2010, during the comment period on the FY 11 SSR Plan. A link to the report is available at http://gnso.icann.org/issues/raa/raa-improvements-proposal-final-report-18oct01-en.pdf.

With regard to contractual compliance, COA states "it is disappointing to see how little attention it receives in the draft Plan." COA notes the contractual compliance section on page 43 is not clearly written and should be clarified. Staff appreciates this comment, and will be correcting the error in the Compliance section to read: "The Contractual Compliance Department will continue to aggressively enforce ICANN's registrar and registry contracts in the interest of protecting registrants and encouraging public confidence in the domain name system. In an effort encourage contract compliance and **enhance** public confidence, the Contractual Compliance Department is developing a system to publically identify **non-**compliant parties."

The Plan will also be clarified to reiterate the Contractual Compliance team will work with the broader community, not only contracted parties, to serve the public interest.

Microsoft Legal & Corporate Affairs

Russell Pangborn from Microsoft Legal and Corporate Affairs applauded ICANN's recognition of the mission of public trust in coordinating the Internet's unique identifier systems, but noted "the SSR Plan does not more clearly reflect this public trust responsibility." Pangborn called attention to the sections on contractual compliance and WHOIS and encouraged ICANN to continue its efforts to improve these areas. On new gTLDs, Pangborn indicated that the plan understates the SSR implications of the planned introduction [of new gTLDs] while simultaneously overstating the scope and anticipated efficacy of ICANN's efforts to mitigate these implications.

According to Pangborn, "ICANN has not sufficiently included key stakeholders such as enterprises or users in its security, stability, and resiliency initiatives, and the SSR Plan indicates that ICANN will continue to focus on the contracted parties in such initiatives." The SSR Plan was developed out of the Strategic and Operational Planning process, which the entire ICANN community had an opportunity to provide input. Briefings were conducted on ICANN SSR activities with a broad spectrum of the community, to users and enterprises, and many of the initiatives to be conducted in FY 11 involve a wide spectrum of the community, not only contracted parties. Staff has also reached out to Microsoft's security experts, as well as others in the security community for greater engagement in ICANN's SSR activities in FY 11.

The SSR Plan does not differentiate gTLD registries and registrars as core stakeholders separate from other users and enterprises. Pangborn states that "the referenced Kyoto and Georgia Tech symposia did not include numerous users and enterprises…many of the attendees at the symposia were employees of gTLD and ccTLD registries." While there were attendees at both symposia from the TLD community, attendees were also present from Internet Service Providers, such as Comcast and NTT, enterprises such as PayPal, Arbor Networks, NLNet Labs, ISC, Juniper Networks, representatives from security companies, representatives from the academic community and government (US Department of Defense, NIST, and NTIA). Future symposia could be improved by increased participation from experts in the broader spectrum of the DNS community and ICANN welcomes the opportunity for greater engagement from Microsoft's security & operations experts.

Next Steps

The FY 11 SSR Plan will be revised based on comments received, and a final version of the document will be provided to the ICANN Board for the upcoming ICANN meeting in Cartagena de Indias, Colombia 5-10 December 2010. ICANN staff will be briefing stakeholder groups, interested participants in the community, and ICANN Supporting Organizations & Advisory Committees during the Cartagena meeting.

Separately, ICANN will soon be posting a draft 2011-2014 Strategic Plan for public comment, and comments on ICANN's SSR activities and strategic focus areas are welcomed, as this will help inform the development of the FY 12 ICANN Operating Plan and the next iteration of the SSR Plan.

Comments Received

Nevil Brownlee - http://forum.icann.org/lists/ssr-plan-fy11/msg00007.html

Eric Brunner-Williams - http://forum.icann.org/lists/ssr-plan-fy11/msg00000.html and http://forum.icann.org/lists/ssr-plan-fy11/msg00002.html

The Internet Society - http://forum.icann.org/lists/ssr-plan-fy11/msg00005.html

Steven Metalitz on behalf of the Coalition for Online Accountability (COA) - http://forum.icann.org/lists/ssr-plan-fy11/msg00004.html

Microsoft Legal & Corporate Affairs - http://forum.icann.org/lists/ssr-plan-fy11/msg00006.html

Sivasubramanian Muthusamy - http://forum.icann.org/lists/ssr-plan-fy11/msg00000.html

Nominet - http://forum.icann.org/lists/ssr-plan-fy11/msg00003.html

Registries Stakeholder Group - http://forum.icann.org/lists/ssr-plan-fy11/msg00001.html

Dev Anand Teelucksingh - http://forum.icann.org/lists/ssr-plan-fy11/msg00000.html