Final Report of the

Security, Stability and Resiliency of the DNS Review Team

Prepared for the Internet Corporation for Assigned Names and Numbers

-- FINAL REPORT--

20 June 2012

Table of Contents

1 Summary 3
1.1 List of Recommendations 4
2 Background to Security Stability and Resiliency of the DNS Review Team 8
3 Review Methodology 10
4 Findings 12
4.1 Scope and Structure of ICANN's SSR Responsibilities 12
4.1.1 ICANN's SSR Remit and Limited Technical Mission 12
4.1.2 ICANN's SSR-Related Roles and Responsibilities 15
4.1.3 Has ICANN Deviated from its Agreed SSR Remit? 19
4.2 Effectiveness and Implementation of the SSR Framework 21
4.2.1 ICANN's SSR Framework and Strategic Plan 21
4.2.2 ICANN Operational Responsibilities 24
4.2.3 ICANN Areas of Influence as a Coordinator, Collaborator and Facilitator 29
4.2.4 ICANN Engagement with Others in the Global Internet Ecosystem 33
4.2.5 Maintaining Clear Processes for SSR Issues 35
4.2.6 ICANN's SSR-Related Budget and Staff 38
4.3 Understanding the Risk Landscape and Contingency Planning 44
4.3.1 Immediate and Near-Term Future Risk 44
4.3.2 Longer-Term Future Risk 45
4.3.3 ICANN's Risk Management Process 47
4.3.4 Risk Management Framework 49
4.3.5 Incident Response and Notification 50
5 Glossary 52

1 Summary

This report presents the work and results of the Stability, Security and Resiliency of the DNS Review Team ('SSR Review Team'). Pursuant to the Affirmation of Commitments between ICANN and the United States Department of Commerce, the review analyzes the extent to which ICANN is fulfilling its commitment to 'enhance the operational stability, reliability, resiliency, security and global interoperability of the Domain Name System ("DNS")'.

The review encompasses ICANN's existing SSR plan, which must be regularly updated to reflect emerging risks to the DNS. As directed by the Affirmation of Commitments, particular attention is paid to:

> '(a) security, stability and resiliency matters, both physical and network, relating to the secure and stable coordination of the Internet DNS;
>
> (b) ensuring appropriate contingency planning; and
>
> (c) maintaining clear processes.'

The Affirmation of Commitments further provides that the SSR review will assess the extent to which ICANN has successfully implemented the security plan, the effectiveness of the plan to deal with actual and potential challenges and threats, and the extent to which the security plan is sufficiently robust to meet future challenges and threats to the security, stability and resiliency of the Internet DNS, consistent with ICANN's limited technical mission.

The SSR Review Team was formed jointly by ICANN President and CEO and the Chair of the GAC, with participation of representatives of various stakeholder groups. It worked through physical meetings, teleconferences, email and other means of communication. The SSR Review Team analyzed material from a wide range of inputs, including documents interviews, and meeting attendance. Some crucial documents were provided by ICANN Staff upon request.

The review focuses on ICANN's management of its SSR-related functions. It is neither a formal security audit at the technical operations level, nor an audit of ICANN's large-scale management of its relations with other entities, such as governments and intergovernmental organizations. The report refers to the DNS as the system of protocols, servers, networks, organizations and companies that map domain names to IP addresses in the global Internet. When a different meaning is used (e.g. the DNS protocol alone), the report is specific in order to avoid ambiguity.

The SSR Review Team found areas in which ICANN is working well, areas in which there is room for improvement, and other areas where key elements of SSR should be defined and implemented.

We find that ICANN is performing well in a number of areas: understanding and communicating how it operates within different levels of control and influence; adhering to its SSR remit and limited technical mission; improving the formulation of the SSR Framework; engaging in good SSR-related operational practices; and providing thought leadership on DNSSEC.

The report recommends a number of areas of improvement: greater clarity around ICANN's description of its SSR remit; more clearly defined SSR-related relationships with Supporting Organizations and Advisory Committees; a more structured and prioritized SSR Framework; more specific initiatives and programs to implement the SSR Framework, with measurable goals and objectives; more details regarding the budget allocated to support SSR functions; and more closely defining SSR-related tasks with the Supporting Organizations and Advisory Committees.

The SSR Review Team also urges ICANN to expeditiously complete work to create and publish a formal and comprehensive DNS Risk Management Framework. In addition, ICANN should continue to engage in well-defined and targeted outreach efforts to positively influence the larger Internet ecosystem beyond the scope of ICANN's direct responsibilities. It also should support efforts to develop SSR-related best practices and to publish information regarding DNS threats and mitigation strategies.

The final draft version submitted for public comment stated the following:

'The SSR Review Ream will continue to examine some additional input during the public comment period and prior to publication of the final report. This input will include any output or progress of the recently chartered Board DNS Risk Management Working Group and any output from the Joint DNS Security and Stability Analysis Working Group.'

This is the final report of the SSR Review Team which supersedes the draft report posted on 15 March 2012. Since the draft report was published, a comment period of 45 days was made available to ensure Community feedback. The Team held two public webinars, plus a webinar with the GAC to elicit additional feedback.

All feedback provided has been considered by the SSR Review Team. We have incorporated our conclusions in the final report presented here. In some specific cases we discuss the way and extent in which we did so, which includes both acceptance and in some cases total or partial rejection of the comments. Most of them have been built into the report in such a way that they can be used by the Board to direct ICANN action in collaboration with the Community.

The SSR-RT is thankful for all in the Community who took part in this effort over its entire duration, and to ICANN Staff and others who provided valuable support to our work. We particularly thank Alice Jansen, Olof Nordling, Patrick Jones, Denise Michel, Jeff Moss, Steve Crocker and Rod Beckstrom.

The following section lists the key recommendations from this review:

1.1 List of Recommendations

RECOMMENDATION 1: ICANN should publish a single, clear and consistent statement of its SSR remit and limited technical mission. ICANN should elicit and gain public feedback in order to reach a consensus-based statement.

RECOMMENDATION 2: ICANN's definition and implementation of its SSR remit and limited technical mission should be reviewed in order to maintain consensus and elicit feedback from the Community. The process should be repeated on a regular basis, perhaps in conjunction with the cycle of future SSR reviews.

RECOMMENDATION 3: Once ICANN issues a consensus-based statement of its SSR remit and limited technical mission, ICANN should utilize consistent terminology and descriptions of this statement in all materials.

RECOMMENDATION 4: ICANN should document and clearly define the nature of the SSR relationships it has within the ICANN Community in order to provide a single focal point for understanding the interdependencies between organizations.

RECOMMENDATION 5: ICANN should use the definition of its SSR relationships to maintain effective working arrangements and to demonstrate how these relationships are utilized to achieve each SSR goal.

RECOMMENDATION 6: ICANN should publish a document clearly outlining the roles and responsibilities for both the SSAC and RSSAC in order to clearly delineate the activities of the two groups. ICANN should seek consensus for this across both groups, recognizing the history and circumstances of the formation of each. ICANN should consider appropriate resourcing for both groups, consistent with the demands placed upon them.

RECOMMENDATION 7: ICANN should build on its current SSR Framework by establishing a clear set of objectives and prioritizing its initiatives and activities in accordance with these objectives. This process should be informed by a pragmatic cost-benefit and risk analysis.

RECOMMENDATION 8: ICANN should continue to refine its Strategic Plan objectives, particularly the goal of maintaining and driving DNS availability. The Strategic Plan and SSR Framework should reflect consistent priorities and objectives to ensure clear alignment.

RECOMMENDATION 9: ICANN should assess certification options with commonly accepted international standards (e.g. ITIL, ISO and SAS-70) for its operational responsibilities. ICANN should publish a clear roadmap towards certification.

RECOMMENDATION 10: ICANN should continue its efforts to step up contract compliance enforcement and provide adequate resources for this function. ICANN also should develop and implement a more structured process for monitoring compliance issues and investigations.

RECOMMENDATION 11: ICANN should finalize and implement measures of success for new gTLDs and IDN fast track that expressly relate to its SSR-related program objectives, including measurements for the effectiveness of mechanisms to mitigate domain name abuse.

RECOMMENDATION 12: ICANN should work with the Community to identify SSR-related best practices and support the implementation of such practices through contracts, agreements and MOUs and other mechanisms.

RECOMMENDATION 13: ICANN should encourage all Supporting Organizations to develop and publish SSR-related best practices for their members.

RECOMMENDATION 14: ICANN should ensure that its SSR-related outreach activities continuously evolve to remain relevant, timely and appropriate. Feedback from the Community should provide a mechanism to review and increase this relevance.

RECOMMENDATION 15: ICANN should act as facilitator in the responsible disclosure and dissemination of DNS security threats and mitigation techniques.

RECOMMENDATION 16: ICANN should continue its outreach efforts to expand Community participation and input into the SSR Framework development process. ICANN also should establish a process for obtaining more systematic input from other ecosystem participants.

RECOMMENDATION 17: ICANN should establish a more structured internal process for showing how activities and initiatives relate to specific strategic goals, objectives and priorities in the SSR Framework. It also should establish metrics and milestones for implementation.

RECOMMENDATION 18: ICANN should conduct an annual operational review of its progress in implementing the SSR Framework and include this assessment as a component of the following year's SSR Framework.

RECOMMENDATION 19: ICANN should establish a process that allows the Community to track the implementation of the SSR Framework. Information should be provided with enough clarity that the Community can track ICANN's execution of its SSR responsibilities, while not harming ICANN's ability to operate effectively. The dashboard process being used to track implementation of the ATRT recommendations serves as a good model.

RECOMMENDATION 20: ICANN should increase the transparency of information about organization and budget related to implementing the SSR Framework and performing SSR-related functions. Information should be provided with enough clarity that the Community can track ICANN's execution of its SSR responsibilities, while not impeding ICANN's ability to operate effectively.

RECOMMENDATION 21: ICANN should establish a more structured internal process for showing how organization and budget decisions relate to the SSR Framework, including the underlying cost-benefit analysis.

RECOMMENDATION 22: ICANN should publish, monitor and update documentation on the organization and budget resources needed to manage SSR issues in conjunction with introduction of new gTLDs.

RECOMMENDATION 23: ICANN must provide appropriate resources for SSR-related Working Groups and Advisory Committees, consistent with the demands placed upon them. ICANN also must ensure decisions reached by Working Groups and Advisory Committees are reached in an objective manner that is free from external or internal pressure.

RECOMMENDATION 24: ICANN must clearly define the charter, roles and responsibilities of the Chief Security Office Team.

RECOMMENDATION 25: ICANN should put in place mechanisms for identifying both near and longer-term risks and strategic factors in its Risk Management Framework. This process should be informed by insights from research, business partnerships, ICANN Supporting Organizations and other sources. ICANN should publish information about risks, recognizing the sensitive nature of some of these factors.

RECOMMENDATION 26: ICANN should prioritize the timely completion of a Risk-Management Framework. This work should follow high standards of participation and transparency.

RECOMMENDATION 27: ICANN's Risk-Management Framework should be comprehensive within the scope of its SSR remit and limited missions.

RECOMMENDATION 28: ICANN should continue to actively engage in threat detection and mitigation, and participate in efforts to distribute threat and incident information.

2 Background to Security Stability and Resiliency of the DNS Review Team

The Security, Stability and Resiliency of the DNS Review Team (SSR Review Team) was formed pursuant to paragraph 9.2 of the Affirmation of Commitments between ICANN and the United States Department of Commerce ("AoC"). As required by the AoC, the SSR Review Team consists of volunteer Community members, including designated representatives of the Chair of the GAC, CEO of ICANN, relevant Advisory Committees and Supporting Organizations, and independent experts. This first SSR review commenced in October 2010 and subsequent reviews will be conducted no less frequently than every three years.

As noted in Paragraph 9.2 of the AoC, ICANN has developed a plan to enhance the operational stability, reliability, resiliency, security, and global interoperability of the DNS, which will be regularly updated by ICANN to reflect emerging threats to the DNS. The AoC directs that particular attention will be paid to:

> (a) security, stability and resiliency matters, both physical and network, relating to the secure and stable coordination of the Internet DNS;
>
> (b) ensuring appropriate contingency planning; and
>
> (c) maintaining clear processes.

It further provides that each of the SSR reviews conducted under paragraph 9.2 will assess the extent to which ICANN has successfully implemented the Security Plan, the effectiveness of the Plan to deal with actual and potential challenges and threats, and the extent to which the Security Plan is sufficiently robust to meet future challenges and threats to the Security, Stability and Resiliency of the Internet DNS, consistent with ICANN's limited technical mission.

The SSR Review Team was formed in October 2010, with a commitment to work both between and during ICANN meetings. The Team was formed from applicants selected by their respective Supporting Organizations and communities, with the final selection decision being made by both the GAC chair and the ICANN CEO and President.

The make-up of the Team is defined and outlined on the ICANN website[1] but summarized as

SO/AC Candidates

- Alejandro Pisanty (MX) – Group Chair;
- Anders Rafting (SE);
- Bill Manning (US);
- David Cake (AU);
- Hartmut Glaser (BR);
- Jeff Brueggeman (US);
- Martin Hannigan (US);
- Ondrej Filip (CZ);

[1] http://www.icann.org/en/about/aoc-review/ssr/composition

- Rodney Joffe (US);
- Simon McCalla (UK);
- Atif Nazar (PK) (resigned June 2011*);*
- Xiaodong Lee (CN) (resigned February 2012 to take ICANN post).

Independent experts:

- Andrea Rigoni (IT);
- Paul Mockapetris (US).

Designated Nominees:

- Alice Munyua (KE) – GAC Chair nominee;
- Jeff Moss (ICANN) – ICANN CEO nominee (resigned May 2011 to take ICANN post).

The Review Team commenced formal work at the Cartagena de Indias meeting and has met for six face-to-face meetings during the reporting period, outlined below:

- ICANN Meeting – Cartagena de Indias, Colombia – December 2010;
- ICANN Meeting – San Francisco, United States of America – March 2011;
- ICANN Meeting – Singapore, Singapore – June 2011;
- SSR Drafting Team Meeting – Washington DC, United States of America – July 2011;
- ICANN Meeting – Dakar, Senegal – October 2011;
- ICANN Meeting – San Jose, Costa Rica – March 2012;
- SSR Drafting Team Meeting – Washington DC, United States of America – June 2012.

3 Review Methodology

In order to fulfill its mandate under the AoC, the SSR Review Team has focused its work on three broad categories of issues:

- The scope of ICANN's SSR responsibilities, given its limited technical mission;
- The effectiveness of ICANN's SSR Plan and implementation of the Plan and its SSR responsibilities; and
- ICANN's processes for assessing the DNS risk landscape and conducting contingency planning to account for current and future challenges as well as for involving other parties required for the fulfillment of ICANN's SSR mission.

The SSR Review Team initially established three working Subteams to gather relevant documentation, conduct an initial analysis of the materials and prepare a preliminary set of issues.

The working methodology across all three Teams was to perform analysis gained from information based upon 4 key areas:

- ICANN's public library of SSR-related documentation;
- External papers and reports related to SSR and ICANN's SSR role;
- Interviews with ICANN Staff, Supporting Organizations, Community members, external experts and others;
- Insight and experience from within the assembled SSR Review Team.

The Team worked across a library of over one hundred individual documents and information sources. However, there are 5 key documents that form the backbone of the Review Team's work and the foundation of ICANN's SSR position:

- ICANN Bylaws (Including Mission and Core Values);
- DOC/ICANN Affirmation of Commitments;
- ICANN's FY 11 Security, Stability and Resiliency Framework description of scope of responsibilities;
- ICANN's FY 12 Security, Stability and Resiliency Framework description of scope of responsibilities;
- ICANN Strategic Plan 2011-2014 description of scope of responsibilities.

The review process involved a detailed breakdown of information gained from the library of documents. Where appropriate, questions and feedback were solicited from key Community members and ICANN Staff in order to support an analysis of key topics and supporting conclusions and recommendations. In some instances, interviews with individuals or groups led the Team to look into specific issues, requesting additional information from ICANN Staff that had not yet been published, or was an internal document.

It is worth pointing out that a decision was made early on during the review that the Team would not participate in a formal non-disclosure agreement with ICANN. The Team felt that it would be difficult to remain transparent and impartial if it were party to internal ICANN information that it could then not discuss openly within the report.

Once documented, the analysis gained from the three Subteams was circulated and discussed within the Review Team. A number of rounds of discussion and further analysis were undertaken in order to reach a consensus opinion in order to develop final recommendations. The analysis and recommendations are detailed in the following sections.

4 Findings

4.1 Scope and Structure of ICANN's SSR Responsibilities

This section of the report analyses the scope of ICANN's responsibilities in enhancing the Security, Stability and Resiliency of the DNS, consistent with ICANN's limited technical responsibilities. In order to understand ICANN's plans and actions, the Review Team must first look to how ICANN organizes its activities. The Review Team has used the following structure to analyze and understand ICANN's SSR activities:

- ICANN's operational responsibilities;
- ICANN's areas of influence as a coordinator, collaborator and facilitator; and
- ICANN's engagement with others in the global Internet ecosystem.

The report refers to these 3 'spheres of influence' throughout the following sections.

4.1.1 ICANN's SSR Remit and Limited Technical Mission

According to ICANN's Bylaws[2], its mission is as follows:

> 'The mission of The Internet Corporation for Assigned Names and Numbers ("ICANN") is to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems. In particular, ICANN:
>
> 1. Coordinates the allocation and assignment of the three sets of unique identifiers for the Internet, which are:
>
> a. Domain names (forming a system referred to as 'DNS');
>
> b. Internet protocol ('IP') addresses and autonomous system ('AS') numbers; and
>
> c. Protocol port and parameter numbers.
>
> 2. Coordinates the operation and evolution of the DNS root name server system.
>
> 3. Coordinates policy development reasonably and appropriately related to these technical functions.'

In its statement of core values, ICANN assumes responsibility not only for coordinating the allocation of resources and the operation of the DNS, but also for 'preserving and enhancing the operational stability, reliability, security, and global interoperability of the Internet.' ICANN also states that, to the extent feasible and appropriate, it will delegate coordination functions to, or recognize the policy role of other responsible entities that reflect the interests of affected parties. These potentially competing responsibilities and values are reflected in the AoC, which references ICANN's limited technical mission and its responsibility to preserve the Security, Stability and Resiliency of the DNS.

It is difficult when analyzing the appropriate ICANN documents to get a simple and concise definition of the SSR remit for ICANN. In order to understand the scope of the remit, the reader must bring together information

[2] *ICANN Bylaws* – Refer to: http://www.icann.org/en/about/governance/bylaws

from a number of documents. At times, due to minor changes in language and terminology, this can lead to a lack of clarity around tasks and responsibilities. Work on the FY12 SSR Plan[3] has shown an improvement in this regard by providing a foundation section that outlines this more clearly. This is welcomed by the Review Team as a positive step.

It would be helpful for ICANN to develop a single, clear SSR statement of responsibilities (perhaps a simple 1-page document) from which all other initiatives can be linked. The inclusion of a foundation section in the FY12 SSR plan is a step in the right direction; however this needs further clarity and focus.

Likewise, ICANN defines its technical mission in a number of ways across its key documents. It candidly discusses the challenges of having direct operational or contractual responsibilities as well as having to act as both a coordinator and participant in a much wider and significant context. ICANN recognizes the difficulty in defining ambitious goals for areas under which it has no direct control. Looking across the documentation, it would be fair to define ICANN's limited technical mission as:

- To coordinate the allocation of the Internet's unique identifier systems;
- To preserve and enhance the Stability, Security and Resiliency of these systems;
- To maintain and operate the L-Root nameserver instance as steward for the Community;
- To manage ICANN's own internal systems and to provide a publicly accessible portal to disseminate and share information.

However, it is clear that it would be helpful for ICANN to explicitly state this mission and to use consistent language when referring to the mission within other documents. It is important that ICANN consider the impact of inconsistent or perhaps confusing terminology.

It must be recognized that ICANN's SSR role also encompasses a significant effort in coordinating policy development that has a direct bearing on the technical coordination of the SSR mission. Although not explicitly discussed within the documentation, the Review Team recognizes the importance of this function.

To understand Community perceptions and positions regarding ICANN's SSR remit and limited technical mission, the Team reviewed public comments on three key documents upon which feedback has been solicited:

- Strategic Initiatives for SSR/Creation of a DNS-CERT[4];
- ICANN FY11 SSR Plan[5];
- ICANN FY12 SSR plan[6].

---

[3] *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[4] *Proposed Initiatives for Improved DNS Security, Stability and Resiliency* http://www.icann.org/en/about/staff/security/ssr/strategic-ssr-initiatives-09feb10-en.pdf

[5] *Plan for Enhancing Security, Stability & Resiliency (FY11)* http://www.icann.org/en/about/staff/security/ssr/ssr-draft-plan-fy11-13sep10-en.pdf

[6] *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

Feedback on these documents (through ICANN's documented feedback process) ranges to more than 30 public documents from a wide range of stakeholders including Registries, Registrars, national governments and large corporations.

The themes brought up in the feedback show a striking consistency. The Community clearly believes that it fully understands ICANN's limited technical remit, often with references to the wording in the AoC, and wants to ensure that ICANN does not stray into an 'operational' role. There are a number of requests for clarity and focus around specific SSR issues as well as defined goals and measures to ensure success. The lack of resources dedicated to contractual compliance is another common theme, and many believe that this could lead to degradation of SSR of the namespace.

An important point to consider is that the amount of feedback decreases for each document in the list. The 'Strategic Initiatives' document attracts by far the most comment (largely due to the DNS-CERT discussions). The FY12 plan attracts the least number of comments of the three, perhaps due to the lack of any significantly controversial topics. It is disappointing to see the low level of engagement regarding the latest SSR plan and ICANN should strongly consider how to get better engagement and feedback on such a critical area.

It is clear that ICANN needs to consider carefully how to ensure that it gets wide Community input and attention to its SSR work. Developing a stronger mechanism for feedback would be helpful.

It is important that ICANN regularly review both its existing SSR remit as well as how it is performing against this. With a clearer understanding of projects and operations, this task should become more straightforward and should allow for greater transparency. It is recommended, however, that specific attention be given to self-audit/self-review and that feedback is then solicited from the Community.

The SSR Review Team also recognizes the importance of the AoC Reviews and in particular the role of this and subsequent SSR Review Team in providing external input to ICANN's SSR performance.

RECOMMENDATION 1: ICANN should publish a single, clear and consistent statement of its SSR remit and limited technical mission. ICANN should elicit and gain public feedback in order to reach a consensus-based statement.

RECOMMENDATION 2: ICANN's definition and implementation of its SSR remit and limited technical mission should be reviewed in order to maintain consensus and elicit feedback from the Community. The process should be repeated on a regular basis, perhaps in conjunction with the cycle of future SSR reviews.

RECOMMENDATION 3: Once ICANN issues a consensus-based statement of its SSR remit and limited technical mission, ICANN should utilize consistent terminology and descriptions of this statement in all materials.

4.1.2 ICANN's SSR-Related Roles and Responsibilities

The FY12 SSR Plan is presented in two parts (Part A and B) and attempts to tie the Framework directly to the Strategic Plan. In this respect, this is a welcome development and it is clear that ICANN Staff has listened to the concerns of the SSR Review Team during the past 12 months and acted to address some of these.

In Part A of the FY12 SSR Plan, ICANN helpfully brings together SSR components from its Mission statement, core values and the Affirmation of Commitments to try and summarize its SSR responsibilities. This is a useful addition to the Plan and helps to tie in many of the supporting documents. When reviewing the FY11 Plan, this work took significant time for the Review Team, so this is a very welcome addition that should assist a first time reader of ICANN's SSR Plans.

ICANN summarizes its SSR role in Part A as encompassing three categories of responsibilities:

- ICANN's internal operations (including L-Root, DNS operations etc.);
- ICANN's role as a coordinator, collaborator and facilitator within the Community (policy coordination, technical contributor etc.);
- ICANN's role as an observer of the activities of others in the global Internet ecosystem;

Helpfully, ICANN also clarifies some areas for which it believes that it has no responsibility:

- ICANN does not play a role in policing the Internet or operationally combatting criminal behavior;
- ICANN does not have a role in the use of the Internet related to cyber-espionage and cyber-war;
- ICANN does not have a role in determining what constitutes illicit conduct on the Internet.

While ICANN states that it cannot unilaterally suspend or terminate domain names it also acknowledges that it can enforce its contracts with Registries and Registrars. Clearly this applies only to the bodies with which ICANN has contracts (e.g. not country-code Registries).

The new Part A "foundational section" of the SSR Framework is welcome, but the section still appears more as an assembly of useful material rather than a summary of ICANN's SSR role. As discussed earlier, it would be extremely useful to see a clear statement of the SSR remit related to ICANN's actual technical mission. This would help significantly when reading section B of the Plan and Framework.

The SSR Review Team agrees with ICANN's delineation of its responsibilities according to spheres of influence, but we recommend a refinement of these areas of influence as follows:

- ICANN's operational responsibilities;
- ICANN's areas of influence as a coordinator, collaborator and facilitator; and
- ICANN's **engagement** with others in the global Internet ecosystem.

The Review Team considers that this change of language would be useful to establish ICANN's role within the wider Internet ecosystem from a passive role to one in which it is much more engaged and focused on outreach.

As we look at each of these areas, we must understand that the rules around achieving success through SSR activities change depending on the level of proximity and control that ICANN has over each area. As discussed

earlier, ICANN is becoming increasingly clear in differentiating tasks that it can control, and be held accountable for, and tasks for which it must collaborate or coordinate in order to achieve success.

4.1.2.1 ICANN's Operational Responsibilities

ICANN's own SSR operations are either decided internally or built from policies developed by the Community and adopted by the Board. These will have a direct bearing on the function of the organization and how it manages its security provisions. These operations take into account the internal security of the ICANN organization itself as well as how it manages the IANA function. It is within this area that ICANN has the greatest level of control and accountability.

Given that this is the area over which ICANN has the highest degree of control, one could expect clear and consistent operational plans along with strong measurable goals and objectives for these functions as with any organization. ICANN should also be expected to play an important role as thought leader and key influencer, preferably leading by example in this area.

4.1.2.2 ICANN's Areas of Influence as a Coordinator, Collaborator and Facilitator

In the 'About' section of the ICANN website, ICANN describes its purpose in a brief summary entitled 'What does ICANN do?':[7]

> 'To reach another person on the Internet you have to type an address into your computer -- a name or a number. That address must be unique so computers know where to find each other. ICANN coordinates these unique identifiers across the world. Without that coordination, we wouldn't have one global Internet.'

In more technical terms, ICANN coordinates the Domain Name System (DNS), Internet Protocol (IP) addresses space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions.

ICANN facilitates and supports participation by a wide variety of organizations such as private-sector for-profit companies; civil society organizations; individuals; governments; academic and technical organizations such as research institutes, universities, and laboratories, as well as directly through the formal Supporting Organizations and Advisory Committees within the ICANN stakeholder model. These include RIRs, ccTLDs, and, significantly, gTLDs, registries with which it has signed contracts. In this context, the IETF, IAB, and ISOC play specific, prominent roles, as does the United States Government through the Department of Commerce's NTIA.

The relationships with these parties are very much of a two-way nature in which ICANN has to act as both recipient and contributor to discussions and policy development. It is also clear that these relationships have evolved over time with some of the entities pre-dating the formation of ICANN itself. In some cases these relationships have been formalized through contract provision and for others thru bilateral agreements or Memoranda of Understanding (MoUs).

[7] Refer to: http://www.icann.org/en/about/welcome

4.1.2.2.1 ICANN's Relationships with its SSR-Related Supporting Organizations

ICANN's organization chart[8] shows that the ICANN Board and leadership rely on the input of a number of Supporting Organizations and Advisory Committees to advise about and contribute to SSR activities. Within the stakeholder model there are seen four, formal key supporting SSR/technical issues related organizations:

- SSAC (Security & Stability Advisory Committee);
- TLG (Technical Liaison Group);
- RSSAC (Root Server Advisory Committee);
- IETF (Internet Engineering Task Force).

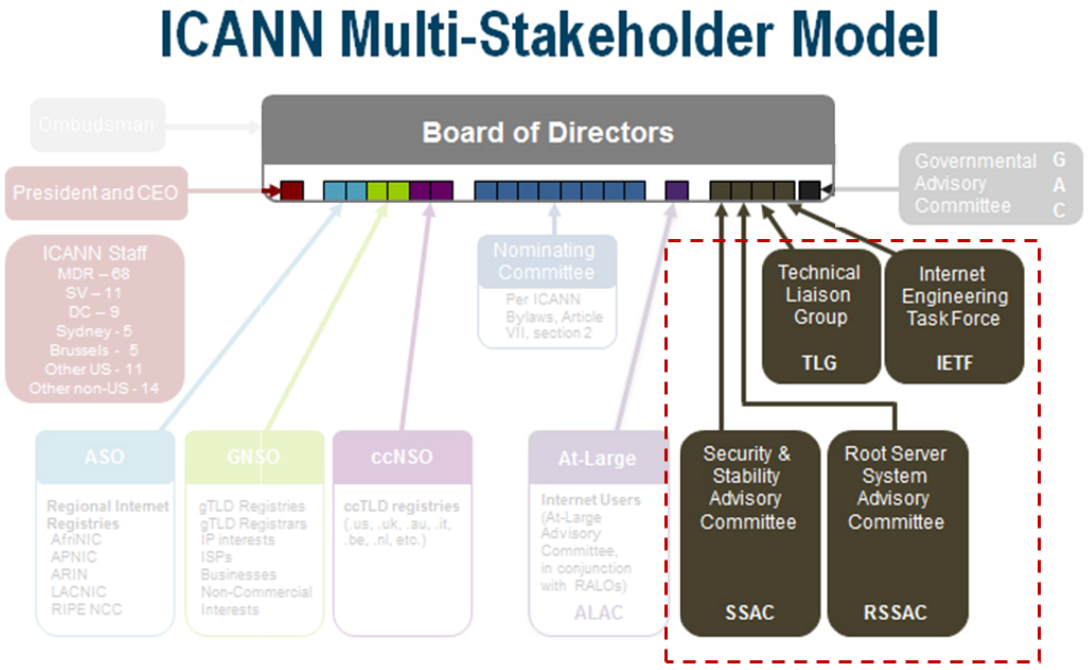

Figure 1 ICANN organization chart

All four of these groups have formed through different processes and policies to provide a broad variety of technical input to the ICANN Board:

- SSAC – ICANN mandated stakeholder group – provides Security and Stability advice directly to the Board, working with other groups (such as the IETF and TLG) to provide a coordinated opinion;
- TLG – A Liaison group to organizations such as the ITU, ETSI and W3C;
- RSSAC – ICANN mandated stakeholder group – brings together root server operators to provide advice related to root zone operations to the Board;

[8] Refer to: http://www.icann.org/en/groups/chart

- IETF – ISOC mandated organization – develops Internet technologies and protocols.

Each of these organizations finds itself with a different relationship to the ICANN Board and sometimes with overlapping or possibly conflicting responsibilities. The IETF and the root server operators came into existence long before ICANN existed.

When analysing the Supporting Organizations, Advisory Committees and their relationships as part of a review, it quickly becomes clear that there are interwoven dependencies. These are often complex to analyze and sometimes difficult to understand as to the exact nature of each agreement or relationship. Often the agreements span back over many years and are documented across multiple documents and agreement versions.

It would be helpful for ICANN to bring together all relevant agreements, whether formally contracted, or an agreed understanding, in order to clarify for the wider Community what the relationship is between ICANN and the other party. This would facilitate understanding as well as allowing a closer look at the effectiveness and applicability of each relationship to the overall SSR mission. It is understood by the Review Team that many of these relationships have formed organically and at times there may be political sensitivities to formalizing some of these. It is with the sole intent of improving the transparency of SSR arrangements that the below recommendations are made.

Several commenters on the draft report raised concerns that the existing recommendation 4 was too broad and that the meaning of 'broader emgagament' was unclear. Accordingly, we have refined the recommendation to clarify that ICANN should focus on maintaining effective working arrangements, recognizing the wide variety of these. Clearly a 'one size fits all' approach is not appropriate when dealing with the breadth of affected parties.

RECOMMENDATION 4: ICANN should document and clearly define the nature of the SSR relationships it has within the ICANN Community in order to provide a single focal point for understanding the interdependencies between organizations.

RECOMMENDATION 5: ICANN should use the definition of its SSR relationships to maintain effective working arrangements and to demonstrate how these relationships are utilized to achieve each SSR goal.

4.1.2.2.2 The specific SSR roles of SSAC and RSSAC

The SSAC and the RSSAC have some areas of responsibility which are close or even overlapping, are sourced from very much the same organizations and communities, and are equally represented through liaisons to the Board and in other Community spaces. They have separate roles and a level of firewalling between them, but also need to cooperate closely at times.

Whereas SSAC is composed of individuals selected from within the ICANN Community with relevance to ICANN's mission, RSSAC is composed of corporate entities of very different natures among themselves. Therefore, SSAC is generally on a mission charged by ICANN or identified through various channels with intense Community cooperation while RSSAC is premised on providing advice to the ICANN Board about the operational

considerations in running the Root Server System in the best possible way but with maximal independence for the operators, from each other and from any other entity including ICANN as a corporate entity.

As a result, the ICANN Board and Staff find themselves working differently with each group. With SSAC, the Board can request that work be performed by the SSAC under its charter and commitment to ICANN. ICANN must work through the RSSAC or work independently with each of the root-zone operators. Like SSAC, the RSSAC members can choose whether to heed a request or not.

A case in point regarding the difference in roles between SSAC and RSSAC is the Root-Scaling Study. General recollection and documented process both show that it was hard to define whether SSAC or RSSAC would bear responsibility for the study or whether they could cooperate. The general expectation was that this study would be performed by the RSSAC, yet ended up being performed by the SSAC. While it is not within the Review Team's mission to express any preference regarding this task, especially given that it has already been concluded, the Review Team points out that a void or lack of definition between responsibilities of the SSAC's and the RSSAC's responsibilities creates a risk for the SSR of the DNS. Better communication and coordination are required for improvement. In practice, the outcome was predicated by the fact that ICANN funds SSAC activities and not RSSAC activities.

RECOMMENDATION 6: ICANN should publish a document clearly outlining the roles and responsibilities for both the SSAC and RSSAC in order to clearly delineate the activities of the two groups. ICANN should seek consensus for this across both groups, recognizing the history and circumstances of the formation of each. ICANN should consider appropriate resourcing for both groups, consistent with the demands placed upon them.

4.1.2.3 ICANN's Engagement with Others in the Global Ecosystem

There is a significant group of technical DNS (and other protocol-layer) operators who form an important part of the DNS infrastructure and over which ICANN has little influence. Tens of thousands of global businesses operate DNS servers and infrastructure but are not involved in any way with the ICANN Community or policy-making process. In terms of ICANN's SSR outreach to these communities, it is an enormous challenge to be able to make significant SSR progress through a direct approach, particularly given the size of the ICANN corporate entity and its limited budget. It should however be possible to increase outreach to other organizations that have a more direct influence on both DNS operators and Internet users.

By far the largest group of Internet actors does not directly participate in ICANN. These are the vast majority of ordinary Internet users, whether individuals or organizations, for whom the actions of ICANN and its Community may have an effect upon their experience of the Internet. This group is often unaware of even the existence of ICANN, let alone its policies and procedures, although the outcome may have a direct impact on their use of the Internet. A case in point is the new gTLD process, where the debates and arguments surrounding the program have made international news.

4.1.3 Has ICANN deviated from its Agreed SSR remit?

ICANN has clearly taken care to ensure that it is covering a wide range of activities across the broad spectrum of SSR tasks it undertakes. Both the FY11 and FY12 SSR Plans show that ICANN is taking a considered and specific

approach to each area of the plan. This is particularly important when dealing with areas in which it has direct control and areas where it must consider itself a partner in a wider ecosystem.

There have been moments during the past 18 months where it might appear that ICANN is moving outside of its current limited technical mission. The discussions and public announcements of a proposal to run a DNS-CERT have caused confusion and consternation in the wider Community. ICANN did, however, respond appropriately to the considerable disquiet of the Community and has now rescinded that proposal.

Both the FY11 and FY12 Plans, show that ICANN is sticking to its limited technical mission and creating a program of activities that covers the majority of the SSR ground. However, it is challenging to review the differing levels of detail within these plans: some are concrete and measurable, while some tasks are vague concepts with no clear definition. The discussion of 'contingency planning exercises' amongst DNS operators is a good example of this.

ICANN also defines 'DNS Security and Stability' as one of the four 'Strategic Focus Areas' in its Strategic Plan (2011-2014). Within this Plan it mentions four strategic objectives to:

- Maintain and drive global DNS uptime;
- Increase security of the overall systems of unique identifiers;
- Increase international participation in unique identifier security activities;
- Coordinate global DNS risk management.

These themes are introduced in the FY12 SSR Plan. This is a welcome change from the FY11 documentation where it was harder to tie together the two documents.

Both the AoC and ICANN Bylaws, show that these strategic objectives for SSR are closely aligned to the Bylaw statements 'ensure the stable and secure operation of the Internet's Unique identifier systems' and 'coordinate(s) the operation and evolution of the DNS root name server system'. Where there may be some room for discussion is the difference between doing this for the 'root' name server system and for the 'global' DNS system (as per the fourth strategic objective). As discussed later in this document, that minor distinction can lead to significant disagreement around scope and remit if not handled carefully.

4.2 Effectiveness and Implementation of the SSR Framework

The SSR Review Team analyzed the extent to which ICANN's existing SSR Framework has established effective strategies to enhance the Security, Stability and Resiliency of the DNS. It also analyzed ICANN's progress in implementing the Framework and its processes for addressing SSR issues in its budget, organization, strategic plans and policy development processes. In addition to examining the structure of the SSR Frameworks, we assessed the substantive projects that ICANN has identified within each of the three types of SSR-related responsibilities. Moreover, we considered the cross-cutting issue of whether ICANN has 'clear processes' for defining, updating and implementing its SSR Framework.

4.2.1 ICANN's SSR Framework and Strategic Plan

The AoC acknowledges the fact that ICANN has developed a plan to enhance the operational stability, reliability, resiliency, security, and global interoperability of the DNS, which will be regularly updated by ICANN to reflect emerging threats to the DNS. The SSR Review Team's analysis encompasses the format of the SSR Framework, the substance of the priorities and initiatives included in the SSR Framework, and the evolution and continuity of the SSR Framework over time. We also have reviewed ICANN's Strategic Plan, which contains important details about ICANN's strategic and operational priorities, its organizational structure and its SSR-related budget.

4.2.1.1 SSR Framework

ICANN is now operating under the third iteration of its SSR Framework. Our review closely analyzed both the FY11 SSR Framework, which was finalized in November 2010, and the FY12 SSR Framework, which was finalized in May 2011 and acknowledged by the ICANN Board in a resolution dated July 28, 2011. As the Board noted, the publication of the FY12 SSR Framework was accelerated in order to align the release of the SSR Framework with the publication of ICANN's FY12 Operating Plan and Budget Cycle.[9] ICANN has initiated the development of the FY13 SSR Framework, which is scheduled to be finalized by the June 2012 ICANN meeting.

As previously discussed, the structure of the SSR Framework and the initiatives being undertaken by ICANN appear to be consistent with its SSR remit and scope of responsibilities. Part B of the FY12 SSR Framework, which focuses on the FY12 module of activities, incorporates the three spheres of responsibilities identified in Part B, which is the foundational section of the SSR Framework.[10] These categories generally are carried over into 'areas of interest' that are used to organize specific programs and initiatives.[11] The inclusion of these areas of interest is a helpful way to clarify ICANN's role externally and to maintain discipline about its activities internally.

---

[9] Board Resolution 2011.07.28.05, *Receipt of Security, Stability and Resiliency Framework for FY12*, adopted July 28, 2011. Refer to: http://www.icann.org/en/minutes/resolutions-28jul11-en.htm

[10] **Slide 4**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[11] **Slide 5-8**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

A positive development is that ICANN has added references to a number of AoC commitments in the FY12 SSR Framework.[12] This is a useful enhancement that should be even more helpful in future years, as ICANN is tracking the progress in implementing the results of the AoC Review Teams. The specific areas of emphasis identified in the FY12 SSR Framework are continuity and contingency work, maintaining clear processes and focus on emerging threats and risks.[13] These issues are analyzed and discussed further in Section 3 of our report.

However, the FY12 SSR Framework does not consistently identify specific projects and initiatives within each of the three spheres of ICANN responsibilities. For example, ICANN identifies separate lists of Community work, Security Team core areas and FY12 SSR activities.[14] These various sections of the Framework each contain a list of different activities, but they are not organized according to ICANN's roles or areas of responsibility. Moreover, the lengthy list of FY12 SSR activities includes the categories of global security outreach, collaboration, corporate security program and cross-organizational activities, but no other ICANN areas of interest.[15] This structure makes it more difficult to assess how specific projects and initiatives relate back to ICANN's general areas of responsibility.

ICANN does a thorough job of describing the types of activities that fall within its areas of responsibility in the FY12 SSR Framework,[16] but individual projects are described only in high-level bullet points with very little context or detail. ICANN also does not clearly prioritize its SSR activities. The FY11 SSR Framework, by contrast, generally provided more information about ICANN's priorities and specificity about the projects being undertaken. The SSR Review Team sees many of the changes in format as a positive step forward, particularly in helping to clarify the plan. At the same time, it also would be helpful to structure the SSR Framework so that it better conveys ICANN's priorities and specific objectives, which are important components of measuring its progress and success in fulfilling its SSR responsibilities.

The organizational structure of the FY12 SSR Framework represents a fairly substantial departure from the FY11 SSR Framework, which did not include a foundational Part A and was organized according to a set of programs and responsibilities. In Section 5 of the FY11 SSR Framework, for example, ICANN identified a number of ongoing projects that were grouped by subsections, such as core SSR responsibilities, TLD Registries and Registrars SSR issues, and activities of ICANN Supporting Organizations and Advisory Committees. Section 6 identified a number of new projects and organized them according to the same general categories. This use of a consistent organizational structure helped to convey the different types of ICANN activities and group-related projects together.

---

[12] **Slide 17-23**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[13] **Slide 17**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[14] **Slide 10-15**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[15] **Slide 12-15**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[16] **Slide 5-8**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

An additional observation is that, by changing the format of the SSR Framework from year to year, ICANN has made it more difficult to monitor its progress in implementing the plan and identify what has changed. ICANN should seek to maintain a consistent structure for its SSR Frameworks to facilitate a greater focus on how ICANN's projects and activities relate to its overall SSR remit and responsibilities.

Going forward, ICANN should consider ways to provide a clear and consistent organizational structure for the SSR Framework. Specifically, ICANN should organize all projects within its three spheres of responsibilities throughout the Framework. It should prioritize initiatives and consider utilizing subsections as it did in the FY11 SSR Framework, which helped to group projects into even more discrete categories according to the type of activities.

ICANN should consider in all of its SSR activities a pragmatic cost and benefit analysis at the same time ensuring that activities for developing regions are fully encompassed and are not ruled out on a cost or risk basis. Working together with the broader Community, ICANN may seek to identify technological contributions that are affordable to parties with scarce resources and help develop them.

RECOMMENDATION 7: ICANN should build on its current SSR Framework by establishing a clear set of objectives and prioritizing its initiatives and activities in accordance with these objectives. This process should be informed by a pragmatic cost-benefit and risk analysis.

4.2.1.2 Strategic Plan

In addition to the SSR Framework itself, ICANN has an ongoing process of developing strategic plans for rolling three-year time periods. The Strategic Plan relates to a number of programs identified in the SSR Framework and provide more detailed information about some of ICANN's activities related to its SSR remit. As with the SSR Framework, the Strategic Plan distinguishes between activities that are within ICANN's control and areas where it wields some influence.[17] The SSR Review Team has analyzed both the 2011-14 Strategic Plan and the 2012-15 Strategic Plan, which was released during the course of our review. Our analysis of specific substantive issues and objectives is included in relevant sections of this report.

The FY12 SSR Framework references the four primary goals of the 2011-14 Strategic Plan, so there is a clear linkage between the two documents.[18] ICANN subsequently finalized the 2012-15 Strategic Plan, which is substantively consistent with the SSR Framework. The 2012-15 Strategic Plan identifies five strategic objectives that relate to ICANN's SSR responsibilities: (1) maintain and drive DNS availability; (2) enhance risk management and resiliency of the DNS, IP addresses and parameters; (3) promote DNSSEC adoption; (4) enhance international DNS cooperation; and (5) improve responses to DNS incidents. In addition, the Strategic Plan provides additional details about a number of SSR-related priorities, particularly the focus areas of DNS stability

[17] Page 6, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[18] **Slide 9, Part B**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

and security, and core operations including IANA.[19] It also establishes strategic metrics for measuring ICANN's performance and progress, which is something that is not included in the SSR Framework itself. Thus, the Strategic Plans add an important component of additional details and metrics that complement the high-level programs and objectives set forth in the SSR Frameworks.

Overall, ICANN should maintain a consistent process that provides details about individual SSR-related goals and activities, including a description of the goal that is being pursued and the work that the project entails. This detailed documentation does not necessarily need to be reflected in the SSR Framework, but it should be cross-referenced in the SSR Framework and reflected in the Strategic Plan or other public documents that are readily available to the ICANN Community.

It would also be helpful if ICANN were to establish more detailed connections to demonstrate how the SSR Framework is being implemented through priorities and projects in the Strategic Plan, and ICANN's budget and staffing decisions. The SSR Review Team finds that there is already a great deal of consistency between the SSR Framework and the Strategic Plan.

By tightening the linkage between projects in the SSR Frameworks and those in the Strategic Plans, and utilizing a consistent organizational structure and program descriptions, ICANN will ensure a consistent focus on priority projects and increase transparency about the progress in meeting operational goals. It will also make it easier for the ICANN Community to identify ICANN's priorities and track its progress in meeting strategic and operational goals. The net result should be a plan that demonstrates how ICANN is fulfilling its areas of responsibility and that it integrates projects and activities into a comprehensive strategic and operational plan.

RECOMMENDATION 8: ICANN should continue to refine its Strategic Plan objectives, particularly the goal of maintaining and driving DNS availability. The Strategic Plan and SSR Framework should reflect consistent priorities and objectives to ensure clear alignment.

4.2.2 ICANN Operational Responsibilities

The SSR Review Team agrees with how ICANN describes its operational responsibilities in the FY12 SSR Framework. ICANN has DNS operational responsibility for IANA functions, management of the L-root and DNSSEC. It has internal corporate security responsibilities, which encompasses IT and network security, and administrative responsibilities for the new gTLD program, contractual compliance and IDN fast track management. The SSR Review Team recognizes that Risk Management and Business Continuity Planning are important components of ICANN's operational responsibilities, and these issues are covered in Section 4.3 of this report. We have not analyzed ICANN's meeting or personnel security, which is beyond the scope of the AoC review process.

19 **Page 1**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

4.2.2.1 DNS Operations.

In the FY12 SSR Framework, ICANN highlights IANA functions, DNS operations for the L-root and DNSSEC as programs and initiatives within its operational responsibilities.[20] ICANN's list of Corporate Security Programs includes implementation of improvements from the L-root contingency exercises and L-root single nodes.[21]

The operational activities that ICANN has included in the FY12 SSR Framework build on initiatives from the FY11 SSR Framework, which included the following: rollout of DNSSEC across all root servers; improved root zone management through automation and authentication of root-zone requests; and business continuity exercises. Specific initiatives undertaken in connection with ICANN's operational responsibilities included signing of the root as part of DNSSEC implementation, an L-Root scaling study and additional L-root servers being added in the Czech Republic, Turkey and Latin America.

One of the four strategic areas of focus in ICANN's 2012-15 Strategic Plan is "Core Operations, Including IANA". Consistent with the SSR Framework, ICANN includes flawless IANA operations and resilient L-root operations as key strategic objectives within this area of focus.[22] These objectives are then reflected in the following specific strategic metrics: (i) meet or exceed IANA contract service level agreement performance; (ii) demonstrating process improvements over time through the European Foundation for Quality Management ('EFQM') model; (iii) RPKI deployment within the period of the plan; and (iv) 100% L-root uptime.[23]

ICANN maintains an operational team for the IANA and has established processes for managing SSR-related issues. The SSR Team interviewed ICANN Staff and obtained information about ICANN's procedures. We were informed that ICANN uses formalized standards as a guide e.g. ISO, but has not sought accreditation under the same. ICANN has some operational procedures for L-Root management, including some personnel reliability criteria and a change management process with a change and approval process modeled after the ITIL change control methodology. The IANA also maintains an Information Security Plan that provides guidelines for initiating, implementing, maintaining and improving information security activities. It is noted that the RZ KSK process has received a SysTrust certification.

A major operational initiative for ICANN has been the implementation of root zone automation. In 2011, ICANN achieved a major milestone. After running parallel manual and automated processes for more than six months, on July 21, 2011, ICANN began accepting root zone changes from the automated system as the primary process. The automated system will generate process notifications to end users, providing requests to confirm, technical details and status updates. A number of safeguards were built into the process to ensure a smooth transition.

---

[20] **Slide 5**, **Part B**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[21] **Slide 13**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[22] **Pages 11-12**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[23] **Pages 12-13**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

In discussions with ICANN Staff, we understand that documentation is retained as part of the change process for the L-root which has been used to facilitate a post mortem for operational events, with the goal of improving infrastructure and associated processes to avoid repeating the same mistakes. The change process is intended to provide peer review among operational team members and to ensure that changes do not cause surprises. Moreover, data is automatically collected from certain infrastructure elements (e.g., servers maintained using change control software, router/switch elements) so that any changes made outside the change control process can be identified. This provides some degree of an ad hoc audit capability within the Operations Team, but no formal audit of this process has been conducted by ICANN or any third parties.

ICANN's operational responsibilities include its important role as the DNSSEC Root Zone Key Signing Key (RZ KSK) manager. In 2010, ICANN obtained SysTrust Certification, which involved an audit to ensure that ICANN has appropriate controls in place for availability, processing integrity and security objectives related to management of the RZ KSK system. The most recent renewal certification was issued on January 23, 2012.

ICANN has appropriately identified a number of strategic objectives that relate to its core operational responsibilities, and it has made progress in developing strategic metrics for measuring progress in achieving these objectives. It has made progress clarifying and refining its operational objectives beyond "100% DNS uptime", which was used in earlier versions of the Strategic Plan, to objectives that are appropriately within its control. The SSR Review Team agrees with ICANN that it should maintain the focus on IANA contract performance, implementation of process improvements, and DNSSEC and RPKI deployment.

One of our findings is that ICANN has utilized ISO and ITIL security standards as a guide, but generally has not obtained certifications under these standards or conducted the type of formal audits that would be required pursuant to such certifications. As noted, an exception is the SysTrust Certification and audit process for its change control process. We recognize that extensive use of security certification processes may not be well aligned with ICANN's operations and evolution, and could distract Staff's attention from required tasks. However, to the extent ICANN is relying on established security standards, it should publish those standards and the results of any audits that are conducted. Of course, any public reporting should be done in a way that does not compromise ICANN's SSR position.

As commenters on the draft report have emphasized, some of ICANN's SSR activities are unique and it would be wasteful to create certification processes for them. On the other hand, software development, technical operations, outsourcing, and IT security already enjoy the benefit of standardization. To the extent that doing so does not distort ICANN's operations, dilute its focus, or otherwise detract from sound planning and operational excellence, those certifications that are reasonable should be achieved and used as standards.

RECOMMENDATION 9: **ICANN should assess certification options with commonly accepted international standards (e.g. ITIL, ISO and SAS-70) for its operational responsibilities. ICANN should publish a clear roadmap towards certification.**

4.2.2.2 Internal Corporate Security

ICANN identifies a number of projects related to its internal corporate security efforts in the FY12 SSR Framework. This includes implementing process improvements from vulnerability assessments and testing,

training for IT and Security Staff, and retention of a full-time employee for Business Continuity Planning and contingency exercise support.[24]

ICANN does not include any organizational security measures as part of the 2012-15 Strategic Plan, but it does commit to a strategic objective of continuous improvement in operational excellence, which includes increased capacity for and scalability of operational workload.[25]

ICANN's IT and Security Staff have implemented a variety of procedures to safeguard its internal corporate security. The Staff provided the SSR Review Team with information about various security procedures. This includes a multi-layer information security plan that covers computing and communications systems that ICANN uses to deliver services. The plan is guided by the Framework of security controls set forth in ISO 17799/27002. It is reviewed on an annual basis and revised as necessary to respond to changes in ICANN's assessment of risks to its information security.

Further, ICANN maintains procedures and guidelines covering a number of other security issues. This includes a backup policy for information resources, a user account management policy, a change management policy for information resources, and a problem management plan to track and manage technology problems. There are also procedures for employee and meeting security, which the SSR Review Team did not review because those issues are beyond the scope of this report.

The SSR Review Team agrees with ICANN's efforts to conduct process improvements and Staff training as part of fulfilling its SSR responsibilities. It would be helpful for ICANN to include more specifics about these activities and the goals that ICANN is seeking to achieve. These details do not necessarily need to be reflected in the SSR Framework, but could be incorporated into the Strategic Plan or publicly available reports about ICANN's administrative activities that could be cross-referenced in the SSR Framework. In addition, we note that our recommendations that ICANN should publish any security standards that it relies on as guidance and consider developing a roadmap toward more formal certification of its SSR-related processes also is applicable to ICANN's internal security.

4.2.2.3 Administration

ICANN includes contractual compliance, IDN fast track management and new gTLD implementation as SSR-related initiatives within its administrative responsibilities[26]. However, specific projects in these areas are identified as cross-organizational activities in the FY12 SSR Framework.[27] This raises some questions about the level of responsibility being assumed by ICANN Staff. At the same time, ICANN identifies specific activities that are being undertaken by ICANN, such as vulnerability testing for new gTLDs, adding Staff and improving registry

[24] **Slides 13-14**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[25] **Page 12**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[26] **Slide 5**, **Part B**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[27] **Slides 14-15**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

and registrar contractual compliance, and supporting a String Evaluation Panel and DNS Stability Panel for the IDN program.[28]

In the 2012-15 Strategic Plan, ICANN states that DNS security, improved compliance mechanisms and consumer trust are increasingly important issues as the market for new gTLDs matures.[29] ICANN broadly defines consumer trust as the concept that unique identifiers work all the time and deliver consistent results when used.[30] The SSR Review Team agrees with ICANN's focus on consumer trust and its broad conception of how consumer trust should be defined.

ICANN also appropriately acknowledges the challenging environment it faces with respect to SSR issues. It notes that cybersecurity attacks continue to grow in size and sophistication, and that Law Enforcement continues to engage more.[31] Additionally, ICANN recognizes that the significant expansion of new gTLDs provides SSR challenges and that IDNs and their variants could increase vulnerabilities by increasing phishing, thus posing stability issues.[32]

Accordingly, as part of its strategic objectives, ICANN commits to benchmarking the effect of new gTLDs on competition, consumer choice, malicious conduct, rights protection and other considerations.[33] ICANN establishes a goal to reduce the incidence and impact of registration abuse and malicious conduct by supporting projects that have the potential to affect the behavior of Internet participants.[34] Related projects are to improve the contractual compliance regime for gTLD Registries and Registrars, and to secure predictable environments for users by encouraging the development of best practices for Registries and Registrars to address the abusive registration of domain names and by incorporating of Registrar Accreditation Agreement amendments.

The associated strategic metrics include the following: (i) implement measures of success for new gTLDs and IDN fast track that align with ICANN core values and program objectives; (ii) measure effectiveness of Rights Protection Mechanisms in the new gTLD program; (iii) build, publish and execute a contractual compliance

[28] **Slides 14-15**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf
[29] **Page 8**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[30] **Page 8**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[31] **Page 5**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[32] **Page 5**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[33] **Page 9**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[34] **Page 9**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

regime for addressing the new expanded TLD space; and (iv) address domain names that are not compliant with the IDNA2008 protocol.[35]

ICANN's administration of the new gTLD program, contract compliance and IDN program management are significant SSR-related issues that should be prioritized in the SSR Framework and implemented with a more detailed set of activities and objectives. ICANN should proceed to develop and implement measures of effectiveness for these administrative issues, seeking Community input, as outlined in the 2012-15 Strategic Plan. It also should incorporate additional substantive information about these important activities into the SSR Framework itself. ICANN should add the SSR Framework (in evolution), metrics, goals, and impact assessment in its management of the new-gTLD program.

The SSR Review Team has also analyzed how ICANN has addressed contract compliance and the new gTLD program in its organization and budgeting process. We recognize that ICANN has initiated a number of programs and assigned dedicated Staff to administer contract compliance and the new gTLD program. Nevertheless, the SSR Review Team believes that development and implementation of more specific metrics for contract compliance and other administrative responsibilities will help to strengthen ICANN's focus and effectiveness on these issues, and improve the ability of Community stakeholders to gauge its progress. Our analysis and recommendations related to ICANN's budget process and assessment of incremental resource needs related to the launch of the new gTLD program are addressed later in the report.

RECOMMENDATION 10: ICANN should continue its efforts to step up contract compliance enforcement and provide adequate resources for this function. ICANN also should develop and implement a more structured process for monitoring compliance issues and investigations.

RECOMMENDATION 11: **ICANN should finalize and implement measures of success for new gTLDs and IDN fast track that expressly relate to its SSR-related program objectives, including measurements for the effectiveness of mechanisms to mitigate domain name abuse.**

4.2.3 ICANN Areas of Influence as a Coordinator, Collaborator and Facilitator

ICANN has a wide range of coordination, collaboration and facilitation responsibilities. Through these activities, ICANN can bear on developments through influence though not through command or control. In this sphere of influence, ICANN coordinates with the U.S. Department of Commerce, RIRs, root server operators, ccTLD operators and other operators of DNS infrastructure. ICANN also interacts with and supports various constituent organizations on policy development, including: private-sector, for-profit companies; civil society organizations; users and individuals; the GAC; academic and technical organizations such as research institutes, universities, and laboratories; and those Registries and Registrars with which it has signed contracts.

ICANN's coordination, collaboration and facilitation responsibilities encompass an extensive list of diverse activities. In this area, ICANN maintains a range of two-way relationships in which it can contribute to informed decision-making and capture the combination of situation analysis and Community sentiment through a

[35] **Pages 9-10**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

combination of ICANN Staff support and productive relationships. Given this complexity, it is not surprising that programs and initiatives in which ICANN lacks direct control, but exerts some influence, constitute a significant portion of the SSR Framework. Goals and activities related to ICANN's areas of influence also are addressed in the Strategic Plan.

4.2.3.1 Technical and Operational Issues

In the FY12 SSR Framework, ICANN identifies a number of Community work projects focused on DNS technical and operational issues, namely: DNSSEC adoption; WHOIS internationalized registration data; DNS security solutions; IPv6 rollout and IPv4 exhaustion risk management; RPKI deployment in collaboration with RIRs; and IDN variant case studies.[36]

ICANN is implementing these general priorities through a number of operational-related projects, which are included in the "Collaboration" section of the FY12 SSR Framework. These collaborative projects include the following: support for DNS measurement and metrics tools, implementation of root zone automated systems with NTIA and VeriSign; development of Resource Public Key Infrastructure ("RPKI") resource certification with RIRs; and completion of system trust audit and KSK ceremonies for DNSSEC key rollover.[37]

The SSR Review Team agrees with the general programs that ICANN has identified in the FY12 SSR Framework. We also recognize the importance of ICANN's collaboration with other parties in managing and implementing its SSR-related operational responsibilities. But the SSR Framework should clearly identify specific activities that ICANN will undertake and more specific objectives that it intends to achieve. In some cases, ICANN may need to collaborate with other parties to jointly develop these specific activities and objectives.

In addition, the 2012-15 Strategic Plan includes a number of SSR-related technical and operational issues that are subject to ICANN's influence, but not its control. In the DNS Stability and Security section, ICANN commits to maintain and drive DNS availability, not only by exercising control over L-root operations, but also by leveraging contractual and other relationships with TLDs and Registrars.[38] Strategic projects include facilitating IPv6 adoption and leveraging contractual and other relationships with TLDs and Registrars to support DNS uptime, including Business Continuity Planning for Registries and Registrars.[39]

Moreover, ICANN will continue to promote broad DNSSEC as a strategic objective.[40] In order to meet this objective, ICANN will work with the Community to monitor and improve DNS resiliency and to coordinate the

---

[36] **Slides 10**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[37] **Slides 12-13**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[38] **Page 5**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[39] **Page 5**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[40] **Pages 5-6**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

development of an Internet resource certification.[41] ICANN plans to seek continued engagement with the Internet Community and Law Enforcement Agencies to deter malicious conduct, and to promote work in the Community to develop Business Continuity Planning and testing to address risks and threats.[42]

ICANN has established a number of metrics to measure its progress in meeting these strategic objectives. It will initiate Community development of key performance indicators for measuring 100% DNS uptime and monitor contract enforcement of TLD uptime service level agreement.[43] It will measure progress toward certification for a global business continuity standard.[44] And it will track the number of DNSSEC TLD signings and IPv6 awareness raising engagements during the plan period.[45] ICANN also will initiate an Internet number resource certification security effort and collaborate with the Community on implementation within the plan period.[46]

In the "Core Operations Including IANA" section, ICANN notes that it is responsible for coordinating the IP address space and operation of the authoritative DNS root server system, as well as the allocation of three sets of unique identifiers (DNS, IP and Ports & Parameters).[47]

The SSR Review Team supports ICANN's programs and objectives to collaborate and coordinate with TLD operators and others to enhance DNS security, stability and resiliency. We agree that the general goal of 100% DNS availability should be refined and implemented through more specific metrics. Moreover, by engaging with Registries and Registrars, ICANN can play an important role in promoting the development and implementation of SSR-related best practices. These efforts also can serve as a model for other DNS operators.

However, the Community has raised concerns about ICANN assuming an operational role on SSR issues and the SSR Review Team does not believe ICANN should go so far as to establish an emergency response team (DNS CERT) that extends beyond ICANN's own areas of operational responsibility.[48]

4.2.3.2 Organizational Support

The FY12 SSR Framework identifies the following Community work projects which involve collaboration within ICANN itself: GNSO activities related to the Registrar Accreditation Agreement; SSAC and RSSAC activities;

---

[41] **Page 6**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[42] **Page 6**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[43] **Page 6**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf.
[44] **Page 6**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[45] **Page 7**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[46] **Page 7**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[47] **Page 11**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[48] **Page 6**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

collaborative responses to malicious abuse of the unique identifier system (e.g. Conficker Working Group); and policy development, including the Registration Abuse Working Group and internationalized WHOIS.[49]

In some cases, ICANN Staff is relying on other parties to take the lead on specific SSR-related activities. For example, the FY12 SSR Framework references the DSSA Working Group in connection with DNS security solutions and indicates it will contribute to the work of others on the technical evolution of WHOIS.[50] It also cites GNSO and ccNSO policy development activities in connection with registration abuse and the Registrar Accreditation Agreement (RAA).[51]

Likewise, ICANN references a number of Community support efforts in the 2012-15 Strategic Plan. ICANN indicates that it will follow the lead of Community Working Groups to develop an approach to solutions, such as coordination of an emergency response team or other solutions to address Internet security.[52] ICANN also will work with the Community to explore cost effective approaches to SSR solutions.[53]

An ongoing concern has been the slow progress of some Community efforts to address registration abuse and other SSR-related issues within the standard policy process. For example, governments and Law Enforcement representatives identified a number of recommendations for provisions that should be included in the RAA. As a result of escalating pressure, ICANN moved forward with active negotiations with accredited Registrars to incorporate a series of RAA amendments of impact for Law Enforcement, including provisions related to WHOIS verification, requiring Registrars to maintain points of contact for reporting abuse, reseller obligations, heightened obligations relating to privacy/proxy service and increased compliance mechanisms, among others.

ICANN has recognized the importance of implementing effective mechanisms to prevent, identify and respond to malicious abuse of the unique identifier system. It also has initiated a range of activities to address these issues. The SSR Review Team is concerned, however, that SSR-related issues have not always been addressed in a timely manner. It also can be difficult to achieve consensus on practices that may create costs and operational burdens on contracted parties. Accordingly, we recommend that ICANN build on its recent activities and prioritize the development and implementation of a set of SSR-related best practices that can be incorporated into the RAA and other agreements with contracted parties.[54]

---

[49] **Slide 16**, **Part B**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[50] **Slides 10 & 13**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[51] **Slide 13**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[52] **Page 6**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[53] **Page 6**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

[54] ICANN's contractual compliance activities are discussed in our analysis of ICANN's administration activities (Section 4.2.2.2) and its budget and staffing process (Section 4.2.6).

RECOMMENDATION 12: ICANN should work with the Community to identify SSR-related best practices and support the implementation of such practices through contracts, agreements, MOUs and other mechanisms.

RECOMMENDATION 13: ICANN should encourage all Supporting Organizations to develop and publish SSR-related best practices for their members.

Comments on the draft report received for recommendation 13 have suggested measuring the impact of implementing best-practices on the organization: making it more nimble, increasing quality, increasing effectiveness and reducing costs. Clearly, it is important that best practices are applicable and relevant to each organization in question and these may need to be tailored across different Supporting Organizations and communities.

4.2.4 ICANN Engagement with Others in the Global Internet Ecosystem

In addition to areas where ICANN can exert influence, ICANN engages with others in the global Internet ecosystem. This includes governments, Law Enforcement, inter-governmental organizations, and the larger Community of Internet users. ICANN can help to support the security, stability and resiliency of the Internet by engaging in outreach and education, which often involves partnering with other organizations. The SSR Review Team recognizes that this broader "rest of the world" sphere is where some of the most significant risks to DNS security, stability and resiliency originate. In addition to engaging in education and outreach efforts, these broader risks are an important part of ICANN's risk management and Business Continuity Planning efforts, which are discussed in Section 4.3 below.

ICANN identifies a number of projects that involve broader engagement with Internet stakeholders and capacity building on SSR-related issues. For example, ICANN lists facilitation of a global symposium[55] on SSR issues, ccNSO meetings and tech days among its priority programs. It also lists DNS capacity building efforts in collaboration with regional TLD organizations, ISOC and others in the Community.[56]

In its list of specific FY12 activities, ICANN includes global security outreach and engagement with the broader Community, including businesses, the academic Community, the technical Community and Law Enforcement.[57] ICANN also identifies contributions to technical implications government requirements may have on unique identifiers and support for partners and stakeholders.[58] In addition, ICANN identifies an extensive list of activities as part of its DNS capacity building program, including training conducted in partnership with the

[55] **Slide 12**, **Part B**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[56] **Slide 6**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[57] **Slide 12**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

[58] **Slide 15**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf

Network Startup Resource Center and various training events rotating through Africa, Latin America and Asia regions.[59]

In the 2012-15 Strategic Plan, ICANN indicates that Staff and community work will focus on global security outreach and collaboration with RIR operators to improve overall security and support regional and local organizations.[60] ICANN also seeks continued engagement with the Internet community and Law Enforcement Agencies to deter malicious conduct, and to work cooperatively to build SSR capabilities in developing countries.[61] As the IDN and new gTLD programs result in more Registries and Registrars across all regions, ICANN will conduct education and training programs in partnership with ISOC, local TLD operators and the local Internet communities.[62]

In terms of specific objectives, ICANN commits to describing the priorities of the regional education program and report progress, and to document and publish IDN guidelines in 2012.[63] The SSR Review Team agrees with ICANN's focus on broader engagement and capacity building, and we also support the development of priorities and reports on progress. As ICANN has recognized, these efforts will be even more important with the expansion of IDNs and new gTLDs.

The SSR Review Team recognizes that ICANN does not have any direct authority, or even direct means of communications, with the larger global Internet Community. Recognizing the large number of private DNS operators that may have limited or no interaction with ICANN, an area of focus for ICANN should be expanding its efforts to facilitate technical coordination with these operators on key SSR issues, such as DNSSEC deployment. Many DNS operators will be members of professional bodies, peering organizations or industry fora, and their technical Staff are likely to subscribe to relevant industry and technical journals and publications. It would be beneficial for ICANN to consider how it might use other channels such as this to discuss significant SSR issues (such as DNSSEC) where a targeted communications approach may yield significant interest amongst parties who might otherwise be disengaged. While many of the outreach activities that take place within the ICANN Community are very successful (take-up of DNSSEC amongst registry operators for example) due to a consistent and determined approach, take-up of the same SSR/DNSSEC issues amongst others in the DNS value-chain (ISPs for example) has been extremely low.

An excellent example of an organization that has adapted its approach to outreach might be seen in looking at the activities performed by ISOC in its World IPv6 awareness campaign. Here it is clear that ISOC have chosen to

[59] **Slide 19**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf
[60] **Page 6**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[61] **Page 6**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[62] **Page 9**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[63] **Page 10**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

reach beyond their normal audience, working directly with large and small businesses to build momentum behind the outreach day[64].

RECOMMENDATION 14: ICANN should ensure that its SSR-related outreach activities continuously evolve to remain relevant, timely and appropriate. Feedback from the Community should provide a mechanism to review and increase this relevance.

Moreover, ICANN should continue to find ways for itself and for members of the ICANN Community to positively influence the environment in favor of SSR interests. This is an area where ICANN can play a helpful convening role as a forum for identifying issues and connecting members of the Community. We recommend that ICANN's Security Staff remain focused on efforts to strengthen technical coordination on key SSR issues, such as DNSSEC deployment, and to support work on SSR-related issues within ICANN.

In addition to continuing its expansive list of engagement and outreach activities, ICANN should go a step further and publish information about DNS threats and mitigation strategies, including Business Continuity Planning guidelines, as a guide for governments, Law Enforcement Agencies and others in the broader Internet Community. This may include finding ways to more broadly publish materials prepared by SSAC, the DSSA WG, the emerging Board DNS Security Framework Working Group, and other groups within the ICANN Community. A good example of where this could have been achieved was the recent suggested attacks on the root server and other DNS infrastructure. This would have been an ideal opportunity for the ICANN Security Team to take a leading role in ensuring the Community was well prepared for such an attack, should it have arisen.

The multi-stakeholder environment of the Internet, of which ICANN is a pioneer, is questioned regularly, either directly or as a result of other actions. At present the upcoming WCIT and WTSA events of the ITU see some countries proposing changes to the ITRs that could disrupt and challenge the evolution of the multi-stakeholder model. ICANN must act in concert with other parties favorable to the evolution of the multi-stakeholder, bottom-up decision making, in order to inform and perform active outreach, and be open to dialog on these issues while taking a principled position against reckless endangerment of the SSR of the DNS.

RECOMMENDATION 15: ICANN should act as facilitator in the responsible disclosure and dissemination of DNS security threats and mitigation techniques.

4.2.5 Maintaining Clear Processes for SSR Issues

The AoC directs the SSR Review Team to pay particular attention to whether ICANN is maintaining clear processes for SSR issues. The SSR Review Team has analyzed ICANN's process for developing its SSR Framework and obtaining Community input. We also have examined ICANN's process for tracking implementation of the SSR Framework and refining its plans on an ongoing basis.

4.2.5.1 Community Input

ICANN has an established process for socializing the SSR Framework with the Community and obtaining public comment on the draft Framework before it is finalized. A draft of the FY2011 SSR Plan was issued on September

[64] http://www.worldipv6launch.org/

13, 2010 and the public comment forum was open until November 3, 2010. According to ICANN's summary of public comments, only seven parties filed written comments on the draft FY11 SSR Framework. Additional input was received during six Community briefings that were conducted by ICANN Staff. A final version of the FY11 SSR Framework, which incorporated input received during the public comment forum, was issued on November 23, 2010. The modifications included a number of updates and some edits to the description of ICANN's ongoing SSR activities and its relationship with the Internet Community on contract compliance.

On May 2, 2011, ICANN released a draft FY12 SSR Framework and initiated a public comment forum. This plan was issued in a new presentation format, as opposed to the report format of earlier SSR plans. At the request of the ccNSO, the public comment period for the draft FY12 SSR Framework was extended to June 7, 2011. Only five parties filed written comments on the draft FY12 SSR Framework and the Registry Stakeholder Group submitted questions to ICANN Staff during the comment period. In addition, ICANN Staff conducted briefings on the SSR Framework and ICANN activities in SSR prior to and during the comment period on the following dates, including:

- SSAC preview of SSR Framework (April 7, 2011);
- ALAC open call preview (April 26, 2011);
- ccNSO work Team briefing call (May 9, 2011);
- IT Sector Coordinating Council International Committee meeting in Washington, DC (May 10, 2011);
- National Cyber-Forensics and Training Alliance, SpyEye/Zeus Conference in Pittsburgh, PA (May 19, 2011).

ICANN initiated the development of the 2012-2015 Strategic Plan in June 2011. ICANN issued a draft Strategic Plan on October 3, which reflected input from consultations with the GNSO, ALAC, ccNSO, ICANN Staff focus area working sessions and strategic metric updates. The public comment period closed on November 17, 2011.

Five parties submitted comments on the 2012-15 Strategic Plan – the IPC, BC, ccNSO, AFNIC and ALAC. The comments recommended that ICANN enhance the plan to clarify what it is trying to achieve, but also maintain the distinction between influence and control. In addition, there were recommendations to decrease the number of strategic goals and refine metrics used to measure progress. There was also support expressed for outreach and capacity building efforts to promote a healthy Internet ecosystem. A number of changes were made to the 2012-15 Strategic Plan to incorporate the public comments and other input that was submitted.

ICANN has an established and effective process that is structured to provide a transparent decision-making process and to elicit input and public comments. The issuance of draft versions of the SSR Framework and Strategic Plan, redline updates and summaries of public comments helps to establish a transparent process. Moreover, the new Framework used for the FY12 SSR Plan and the accompanying explanations help to improve the accessibility of the draft plan for commenters. This in turn contributes to the clear process which is a subject of this review. ICANN has improved the clarity of its processes that lead to SSR, internally, with parties in direct bilateral collaboration, and elsewhere.

In addition to ICANN's public comment and outreach process for the SSR Framework, ICANN is engaging in a wide variety of outreach and engagement efforts that help to inform and shape the SSR Framework. ICANN's

interaction with SOs and ACs provides additional opportunities for obtaining input into the development and evolution of the SSR Framework.

ICANN should consider ways to raise awareness and expand the amount of public input on the draft SSR plans. And given the focus of commenters on ICANN's appropriate roles and responsibilities, the SSR Review Team is specifically suggesting that ICANN conduct a proceeding that focuses directly on the issue of ICANN's role in ensuring the security, stability and resiliency of the DNS, given its limited technical mission. The SSR Review Team also believes that the DSSA WG may provide a good platform for expanding Community engagement and input into SSR issues, including but not limited to the SSR Framework itself.

RECOMMENDATION 16: ICANN should continue its outreach efforts to expand Community participation and input into the SSR Framework development process. ICANN also should establish a process for obtaining more systematic input from other ecosystem participants.

As commenters of the draft version of this report have suggested, engaging in the IETF debates on SSR-related issues is desirable. While such engagement is already ongoing, and ICANN has many formal and informal links to the IETF and IAB, note is taken of the suggestion for emphasis.

4.2.5.2 Implementation Tracking

ICANN does not have a formal process for publicly tracking the implementation of the SSR Framework or reviewing the status of the SSR Framework at the conclusion of the fiscal year. The SSR Review Team interviewed ICANN Staff regarding ICANN's process for tracking implementation of the SSR Framework and assessing the progress of implementation to inform the ongoing development and evolution of the SSR Framework. ICANN maintains internal information about the status of individual SSR-related activities and uses this information to develop its Strategic Plan and Budget, but there is not a comprehensive process in place for tracking implementation of the SSR Framework.

ICANN should maintain a consistent internal process for tracking and assessing the implementation of SSR Framework, and making any necessary adjustments over time. In discussions with the SSR Review Team, ICANN Staff agreed with our recommendation that it would be helpful to conduct an annual operational assessment of implementation progress as part of the process for developing the following year's SSR Framework.

Now that ICANN has had the opportunity to develop three versions of the SSR Framework, there should be more stability and continuity in the process by incorporating a regular review and assessment component into the SSR Framework development process. ICANN also has developed a public dashboard for tracking implementation of the Accountability and Transparency Review Team (ATRT) recommendations. In discussions with ICANN Staff, they suggested that the ATRT dashboard could provide a model for tracking implementation of the SSR Framework and the SSR Review Team recommendations. We agree and have included that in our recommendations for enhancing ICANN's clear process related to SSR issues.

RECOMMENDATION 17: ICANN should establish a more structured internal process for showing how activities and initiatives relate to specific strategic goals, objectives and priorities in the SSR Framework. It also should establish metrics and milestones for implementation.

RECOMMENDATION 18: ICANN should conduct an annual operational review of its progress in implementing the SSR Framework and include this assessment as a component of the following year's SSR Framework.

RECOMMENDATION 19: ICANN should establish a process that allows the Community to track the implementation of the SSR Framework. Information should be provided with enough clarity that the Community can track ICANN's execution of its SSR responsibilities, while not harming ICANN's ability to operate effectively. The dashboard process being used to track implementation of the ATRT recommendations serves as a good model.

4.2.6 ICANN's SSR-Related Budget and Staff

ICANN has some dedicated budget and Staff related to SSR functions. In the FY12 SSR Framework, ICANN estimates that SSR initiatives comprise 17% of ICANN's total Operating Plan and Budget (i.e., approximately USD 12 million of USD 69.8 million of expenses).[65] ICANN also indicates that it is adding 3+ Staff for contract compliance.[66] Staff and budget issues are not otherwise addressed in the SSR Framework.

In the 2012-15 Strategic Plan, ICANN commits to improving the transparency and structure of the budget process by defining metrics to ensure that the appropriate percentage of the ICANN budget is dedicated to DNS stability, security and resiliency.[67] It generally discusses the need to dedicate resources and personnel to address contract compliance and SSR challenges associated with the expansion of IDNs and new gTLDs.[68] ICANN also commits to implementing a new financial system which it states will improve the inter-relationship between the Strategic Plan and the Operating Plan, and also assist in identifying the operating budgets allocated to the four strategic areas of focus and in providing the rationale for expenditure levels.[69]

4.2.6.1 SSR

ICANN also makes significant mention of its SSR plans in both the FY11 and FY12 Operating Plan and Budget documents, with SSR matters defining one of its four "Strategic Focus Areas" (under the heading DNS Stability and Security). Looking at the allocation of budget to SSR work we see:

- FY11 – USD 7.087M (12% of total budget – up 23.2% on F10 budget)

[65] **Slide 25**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf
[66] **Slide 14**, *FY12 ICANN Security, Stability & Resiliency Framework*, 2 May 2011. Refer to: https://www.icann.org/en/topics/ssr/ssr-plan-fy12-partb-02may11-en.pdf
[67] **Page 7**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[68] **Pages 8-9**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf
[69] **Page 12**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

- FY12 – USD 7.836M (11.7% of total budget – up 10.6% on FY11 budget)[70]

Clearly this is a significant amount of budget and outlines ICANNs intent to pursue SSR as a key strategic goal. However, the SSR Review Team notes that the amount of SSR-related budget identified in the FY12 SSR Framework (i.e., approximately USD 12M) is significantly more than the budget directly allocated SSR-related work in the budget itself (i.e., USD 7.836M). This disparity makes it more difficult to track ICANN's expenditures on SSR-related activities.

Both the FY11 and FY12 operating plans show some specific areas where this budget allocation will be used. These expenditures reflect programs and activities identified in the SSR Framework and the Strategic Plan. Examples include the following:

- Conduct risk assessment exercises prior to 2013;
- Support DSSA-WG through facilitating its efforts so that it delivers a gap analysis of the DNS risks and threats by the end of 2012;
- Collaborate with DNS operators on DNSSEC, including periodic key rollover and audit;
- Implement improvements from FY11 L-root contingency planning exercises;
- Implement objectives contained in the FY12 SSR Framework;
- Develop a long-term plan and obtain resources to support TLD capability training in developing countries; and
- Close gaps identified with ISO 27002 standard for ICANN's internal information security and develop comprehensive BCP plan.[71]

If we attempt to track how the overall amount is broken down across these activities, however, there is little detail to support further analysis within the plans. Following requests to ICANN Staff we obtained a further breakdown that showed that for FY12 the budget under control of the CSO is:

- Personnel costs – USD 1.2M
- Admin costs – USD 35.5K
- Travel – USD 244.325K
- Professional Services – USD 1.15M
- **Total: USD 2.55M**

In analyzing ICANN's spending on initiatives such as SSR, we must take into account that the budget allocated will spread across multiple departments and people. A good example of this might be training and outreach activities that may include a security component but would not be managed by the Security Team.

It is important, however, to realize that of the USD 7.836M allocated to SSR activities in FY12, USD 4.683M (60% of SSR budget) does not appear to fall under the control or remit of the CSO. As we look to understand how the

[70] **Page 13**, *FY12 Operating Plan and Budget*, Fiscal Year ending 30 June 2012, adopted 24 June 2011. Refer to: http://www.icann.org/en/financials/adopted-opplan-budget-fy12-09aug11-en.pdf

[71] **Pages 13-14**, *FY12 Operating Plan and Budget*, Fiscal Year ending 30 June 2012, adopted 24 June 2011. Refer to: http://www.icann.org/en/financials/adopted-opplan-budget-fy12-09aug11-en.pdf

SSR budget is being spent and how well the allocated activities further ICANN's SSR mission, the lack of budgetary information makes it difficult to assess how the budget is being used on specific projects and expenditures. In addition, there is no clear breakdown as to the owners (both operationally and financially) of the tasks outlined in the Plan. This again makes tracking of efficacy of spend and project performance considerably harder when looking in from the outside. Whilst we recognize that much of the SSR spend will be allocated across multiple departments and initiatives, it would be helpful to understand the high level 'buckets' of funding in order to understand the efficacy of the overall budget.

The Security Team is comprised of a Staff of seven people reporting to the Chief Security Officer (CSO). This group is responsible for managing ICANN's internal security operations and supporting SSR-related policy development and Supporting Organization activities, including the Board Risk Committee, SSAC, the DSSA Working Group and the newly formed Board DNS Risk Working Group. In addition, there is a separate organization with dedicated Staff for IANA functions (Staff of ten people reporting to the Vice President (VP) IANA and Technical Operations) and DNS operations (Staff of five people reporting to the VP IANA and Technical Operations).

Based on our review of available budget information, the SSR Review Team concludes that ICANN should closely consider improving the way in which it both plans and details its annual budget and Staff requirements, as well as making clear how these large sums of money are being spent and tracked and who within the organization owns the overall performance of the SSR program. ICANN has committed to defining metrics to ensure the appropriate percentage of the ICANN budget is dedicated to SSR-related issues. The development of more detailed budget information will increase the transparency of the budget process and also will support the metrics that ICANN itself has proposed to implement.

4.2.6.2 Compliance

The FY12 budget allocates USD 4.25 million for contractual compliance activities, which represents a 25% increase from 2010.[72] This includes hiring Compliance Staff and increasing compliance efforts with support from the Registry Liaison, Registrar Liaison, Legal, Policy, Security and IT departments. Compliance activities include:

- Solidify process needed to proactively monitor and enforce the contractual provisions of registrar and registry agreements;
- Improve communications with, and reporting to, the Community;
- Enforce existing policy related to WHOIS, including refining Port 43 monitoring tool and methodology;
- Conduct FY12 WHOIS Data Reminder Policy audit and publish findings;
- Enforce existing policy related to Data Escrow procedures;
- Implement further improvements to the WHOIS data problem reporting system and analyze complaint data;
- Compile and communicate compliance statistics and data;
- Implement an upgrade or replacement of the consumer complaint intake system (CTicket); and

[72] **Page 14**, *FY12 Operating Plan and Budget*, Fiscal Year ending 30 June 2012, adopted 24 June 2011. Refer to: http://www.icann.org/en/financials/adopted-opplan-budget-fy12-09aug11-en.pdf

- Develop stronger relationships through dedicated outreach to Registries and Registrars in Europe, Middle East, South America and Asia Pacific regions by June 30, 2012.

The Compliance organization currently consists of a Senior Director Contractual Compliance and a Staff of eleven people, all of whom report up to the ICANN General Counsel. The FY12 budget includes an allocation for three additional compliance Staff members.

Contractual compliance has become a key component in the relationship between ICANN, the GAC, some individual governments, and Law Enforcement authorities. The opposition between the demands of Law Enforcement for prompt, clear identification of domain-name Registrants and the inability of some Registries and Registrars to provide trustworthy, updated information came to a head in 2011. Strengthening the compliance function through leadership and human resources allows a favorable forecast for the evolution of this controversy.

Data escrow for Registries and Registrars is a critical aspect of compliance, and is a key element for resiliency and stability of top-level domains. The SSR Review Team encourages close monitoring and enforcement of all aspects of data escrow compliance.

It is significant in terms of SSR of the DNS in that better contractual compliance is expected to lead to raising the barrier for domain-name abuse and for some attacks and abuses on the DNS, as well as to a diminution of the controversy involving ICANN, Registries and Registrars, Law Enforcement Authorities, and the GAC. Showing competence and progress in compliance immediately will provide some assurance to those concerned that ICANN will be able to step up to the challenges once new gTLDs are set up and put into operation.

4.2.6.3 New gTLD Program

As ICANN acknowledges in the FY12 Strategic Plan, the new gTLD program will create SSR challenges and IDNs and their variants could increase vulnerabilities by increasing phishing, thus posing stability issues.[73] Accordingly, it will be important for ICANN to be prepared to allocate appropriate headcount and other resources to maintain the security, stability and resiliency of the DNS as the new gTLD program is implemented.

The SSR Review Team has interviewed ICANN Staff regarding the budget and staffing planning process for the new gTLD program. This analysis covers ICANN's preparedness to process applications and delegate approved strings, but also provides a high-level overview of post-delegation operational preparedness within ICANN. ICANN's planning efforts consider a range of staffing needs based on the assumption of an anticipated 500 newly delegated gTLDs, and the possibility of significantly lower (e.g., 100 new gTLDs) and higher (e.g., 1000 new gTLD volumes).

Based on information provided by ICANN Staff, the SSR Review Team has conducted an analysis of key SSR-related functions that may be impacted by the new gTLD program.

gTLD Program Office (GPO). The GPO is the new department responsible for all aspects of gTLD application processing. This includes selecting, contracting and "onboarding" third parties for a number of new gTLD

[73] **Page 5**, *ICANN Strategic Plan – July 2012-June 2015 (Draft Plan)*, 3 October 2011. Refer to: http://www.icann.org/en/strategic-plan/draft-strategic-plan-2012-2015-clean-03oct11-en.pdf

processes, such as the Uniform Rapid Suspension (URS) and Trademark Clearinghouse processes. The GPO has assessed both pre-launch and operations risks associated with the application processing program. One area of focus is on data security, and ICANN has contracted with third-party independent security consultants to review and test security of the application process.

Legal. ICANN's Office of the General Counsel will provide legal support and advice to the new gTLD program, including application review and processing, and handling of objection and contention resolution processes. It also will have a central role in the execution of registry agreements with successful new gTLD applicants. The development of a standard registry agreement is expected to make review and execution of these agreements more efficient.

Finance. ICANN's Finance department will support the new gTLD program for all application deposit and fee transactions. This will involve an initial setup process and ongoing processing of payments. In addition to these application processing activities, a significant amount of new registry and registrar billing and collections work is anticipated. A new financial system was implemented in Fall 2011 that is designed to accommodate the new environment.

IANA. The IANA department is responsible for scaling issues introduced by new gTLDs. For the 331 existing TLDs, root zone management functions include initial delegation, transfer of a TLD and routine maintenance of existing TLDs. There are certain steps that require interaction with NTIA and VeriSign. In preparation for the new gTLD program, IANA has conducted a business excellence review to analyze existing processes and identify risks, gaps and areas of improvement. The functional analysis notes that some elements of the IANA process have been streamlined and automated, but manual review steps are still necessary to ensure changes to the root zone are properly authorized and have no negative impact on security and stability.

Registry Liaison. The Registry Liaison function includes responsibility for managing registry agreement contracts, processing new registry service requests, interpreting and implementing policy, and facilitating constituency support. Efforts are underway to standardize and document existing processes to ease staffing and on-boarding efforts. ICANN identified a number of key risks, including resources and staffing, the likelihood that new Registries will be less knowledgeable and the potential of increased registry failures. In addition to its standardization efforts, ICANN plans to implement a Customer Relationship Management (CRM) system, which is designed to provide self-service processes for Registries.

Registrar Liaison. The Registrar Liaison department currently works with approximately 970 ICANN-accredited registrars that operate pursuant to the Registrar Accreditation Agreement (RAA). This function includes reviewing Registrar Accreditation Applications, interpreting and implementing policy and RAA provisions, ensuring a smooth transfer of domain names and coordinating with other Teams to promote registrar compliance. Key risks being considered include staffing and resources to meet demands of an increased registrar population, a population of less experienced registrars and the need for coordination with Contractual Compliance. While some of these tasks cannot be automated, ICANN plans to implement increased automation of some processes in order to mitigate risks and increase the efficiency of registrar support processes.

Contractual Compliance. As previously discussed, the Contractual Compliance department is focused on contractual enforcement and monitoring activities for the 18 gTLD Registries and the approximately 970

registrars. Key risks being considered include an expected increase in contractual compliance demands and a geographic expansion of the registrar market. Contractual Compliance will partner with the Registry Liaison to develop an effective on-boarding process, which is expected to benefit from a standardized contract. ICANN's long-term plan is to focus on additional formalization and automation of key tasks, as well as establish a dedicated help desk and an upgraded, centralized customer complaint ticketing system.

Based on our analysis of information provided by ICANN Staff, it appears ICANN has identified key issues and risks for a number of functions that are directly related to SSR issues. It also began the planning process for managing these risks with a combination of additional resources and streamlined processes. As a next step, ICANN should develop a public assessment that documents its planning efforts and allows the Community to review the prospective budget and staffing resource requirements related to the new gTLD program.

After the publication of the draft report ICANN launched the application process for the new gTLD program and received almost 2000 applications. Recent events surrounding the stability of the application process (post publication of the draft report) underscore the importance of ICANN's effective management of the new gTLD program and, in particular, its SSR responsibilities in this expansion of the DNS.

RECOMMENDATION 20: ICANN should increase the transparency of information about organization and budget related to implementing the SSR Framework and performing SSR-related functions. Information should be provided with enough clarity that the Community can track ICANN's execution of its SSR responsibilities, while not impeding ICANN's ability to operate effectively.

RECOMMENDATION 21: ICANN should establish a more structured internal process for showing how organization and budget decisions relate to the SSR Framework, including the underlying cost-benefit analysis.

RECOMMENDATION 22: ICANN should publish, monitor and update documentation on the organization and budget resources needed to manage SSR issues in conjunction with introduction of new gTLDs.

4.3 Understanding the Risk Landscape and Contingency Planning

4.3.1 Immediate and Near-Term Future Risk

The Security and Stability Advisory Committee ('SSAC') is currently set up to advise the Board on risk-related matters that have immediate or near-term consequences on the stable operation of the DNS. SSAC works with the ICANN CSO team to provide a cohesive response to security threats and risks. The SSAC has provided valuable advice to ICANN, IANA, and the Community. Over the years it has produced 53 reports and advisories (at the time of this writing) covering a wide range of issues.[74]

The SSAC provides advice on issues such as operational matters (e.g. correct and reliable operation of the root name system), administrative matters and registration matters (e.g., registry and registrar services, such as WHOIS). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming, and address allocation services to assess where principal threats to stability and security. SSAC has focused more on DNS issues than on Internet number assignment and address issues.

The ICANN CSO team is responsible for capturing and implementing responses from the SSAC (in addition to their own self-generated risk assessment work). This may take the form of internal operations for which ICANN has complete control, or alternately they may need to work collaboratively with the Community in order to implement recommendations. An example of a directly implementable action would be the phased implementation of new gTLDs into the root, following advice from SSAC and RSSAC on root scaling. A good example of Community action would be the phased deployment of DNSSEC that involves a broad range of parties, and a complex timeline and implementation plan. In both cases, the ICANN CSO Team generally has been effective in implementing these types of action.

In discussions with the SSAC, it became apparent that at times they felt pressure to deliver an answer to specific problem within a very limited timeframe. This led to a shorter time period to evaluate the issue and more targeted recommendations as a result. Clearly, there will be times, when looking at immediate risks, that a timeframe is enforced upon research work. This is unavoidable. It would be prudent, however, to ensure that with proper planning, the SSAC and RSSAC are given as much time as possible to provide high-quality research work and findings.

The broader finding of the SSR Review Team is that Working Groups (e.g., Board DNS Risk Management Working Group and DSSA-WG) and Advisory Committees (e.g., SSAC and RSSAC) should be put in a position that enables them to produce good decisions. While the SSR Review Team's focus is on SSR-related Working Groups and Advisory Committees, there is not a bright line in activities that fall within that category. A pre-condition for producing good results is staffing and other resources that are appropriate for the demands placed upon working groups and advisory committees. It also is important that Working Groups and Advisory Committees operate in an environment that allows them to reach objective decisions, free from internal or external pressure.

[74] http://www.icann.org/en/groups/ssac/documents-by-category

RECOMMENDATION 23: ICANN must provide appropriate resources for SSR-related Working Groups and Advisory Committees, consistent with the demands placed upon them. ICANN also must ensure decisions reached by Working Groups and Advisory Committees are reached in an objective manner that is free from external or internal pressure.

4.3.2 Longer-Term Future Risk

ICANN's SSR activities are not are done in isolation. Further, the DNS is not static and ICANN's SSR processes have evolved and must continue to evolve. In some respects, the annual update of the SSR Framework is a publication of the tactical activities of the ICANN CSO Team. This section will look at the DNS ecosystem and ICANN's ability to identify longer-term risks and engage in strategic forecasting.

As stated elsewhere in this report, the SSR Review Team is not going to look into the details of ICANN's internal corporate structure. We simply note that a sound and sustainable parent organization, which is well-respected in the Community, is crucial for the success of the CSO Team and its plan execution.

ICANN has a number of channels for collecting information on longer-term risks, such as the SSAC, RSSAC, DSSA Working Group, the Board Risk Committee and the newly formed Board DNS Risk Management Working Group. However, in this layer of influence, ICANN identifies longer-term risk to the DNS mostly through the collaborative effort of the DSSA WG and RSSAC. Looking into the future, those mechanisms or improved replacements will have to include long-term and systemic risk, in coordination with other community parties, notably the SSAC and the Board DNS Risk Management Working Group.

Beyond the commonplace problem that 'the hardest thing to predict is the future', good risk management for the DNS requires a prospective, systemic view that allows stakeholders to prepare for potential longer-term threats. The SSAC, the Board Risk Committee and ICANN Stakeholders, including root-server operators, TLD Registries and Registrars, have a direct interest in the ability to predict risks and have acted to follow this purpose, albeit with loose or no coordination.

Other sources of information for prospective management of the risk landscape have been in use by ICANN since its inception. The following are examples of practices that contribute to the identification of longer-term system risk: a close connection to the IETF/IAB, including by liaison to the Board; membership in the SSAC, RSSAC, and DSSA WG of people who work in organizations that include DNS risk in their risk management; participation in symposia and other international meetings; interaction with research and development organizations; and standard information security practice executed by qualified ICANN Staff.

Longer-term risks come from a wide variety of sources, such as fundamental changes in the nature of the DNS, new implementations of DNS software, and legal and regulatory changes. They also may come from significant, strategic or political factors in the environment within which ICANN operates. In this layer, where entities and individuals operate without ICANN having access to a large degree of control over events, the situation is more complex, and some longer-term risks emerge in ways that are particularly difficult to predict.

Historically, fundamental changes in the DNS have taken some time to evolve and become adopted. However, these changes are accelerating. Notable in this regard are the adoption and rollout of IPv6 and the ability to

encode IPv6 in the DNS, the use and adoption of IDN encoding, and DNSSEC. These are examples of how ICANN has been successful in planning for certain types of longer-term risks.

Other, more difficult to plan for strategic risks may be characterized by low probability, rapid change and high cost of failure. These types of strategic risk are difficult to accommodate in the existing SSR planning Framework. There are also risks that are unexpected, but high impact. An example of this kind of risk would be the discovery of the Kaminsky vulnerability on the DNS. This was an unexpected event that had significant ramifications and needed immediate action in order to protect the DNS.

Proposals or attempts to modify the evolution of Internet governance away from the multi-stakeholder model represent a particular threat for the DNS. Fundamental changes in the legal and regulatory framework could impact many of ICANN's activities, but do not clearly fall within the existing SSR Framework planning process.

ICANN's prevention strategy for this type of systemic risk has included a commitment over many years to participate through staff attendance, collaboration with other organizations, and some funding for events such as the Internet Governance Forum. The results are hard to measure, with the best achieved when the organization has been listening to the evolution of events on several levels and had principals in place for networking. In those cases, preventive action, negotiation, and fine-tuning of ICANN's speech have resulted in risk reduction and good handling of issues.

Other areas of risk, rapid change, and high cost of failure are fundamental changes to the DNS protocol and its operational characteristics.

The SSR Review Team recommends that ICANN carefully consider the resourcing and structure of the CSO Team based upon a thorough analysis of the challenges presented by the risk landscape which it has to tackle. It would also be helpful to define the CSO team's role in relation to the other security related functions within both ICANN and its Supporting Organizations e.g. SSAC and the Board Risk Committee.

The ability of the Advisory Committees and Working Groups to provide high quality, timely information to the CSO Team is dependent on appropriate support of those activities.

In developing a strategic sense of risk, care needs to be taken to not ignore the potential for disruptive events, even if they are low probability.

RECOMMENDATION 24: ICANN must clearly define the charter, roles and responsibilities of the Chief Security Office Team.

RECOMMENDATION 25: ICANN should put in place mechanisms for identifying both near and longer-term risks and strategic factors in its Risk Management Framework. This process should be informed by insights from research, business partnerships, ICANN Supporting Organizations and other sources. ICANN should publish information about risks, recognising the sensitive nature of some of these factors.

4.3.3 ICANN's Risk Management Process

ICANN has repeatedly identified the importance of establishing a Risk Management Framework. The following is a brief history of these developments:

- November 2001 – ICANN established the President's Standing Committee on Security & Stability.[75] The Committee charter, which was approved in March 2002, stated that one of its purposes was:

> 'To develop a security framework for Internet naming and address allocation services that defines the key focus areas, and identifies where the responsibilities for each area lie. The committee will focus on the operational considerations of critical naming infrastructure.'[76]

- May 2002 – the Standing Committee was changed to an Advisory Committee (SSAC), but the group retained the same charter.[77]

- May 2009 – the need for a Risk Management Framework was reiterated in an independent review of SSAC, which included the following recommendation:

> 'As a part of SSAC's first annual plan, SSAC revisit task area one in conjunction with ICANN Staff. Task area one reads as follows: "Develop a security framework for Internet naming and address allocation services that defines the key focus areas, and identifies where the responsibilities for each area lie.' [78]

- October 2009 - SSAC responded to the independent review by indicating that it was not the appropriate body for this task:

> 'The first bullet in the [SSAC] charter, "To develop a security framework for Internet naming and address allocation services..." is more appropriate for research and development than for an advisory committee composed of volunteers... It should be removed.'[79]

---

[75] **Standing Committee on Security and Stability**, *Third Annual Meeting of ICANN Board in Marina del Rey Preliminary Report* http://www.icann.org/en/minutes/prelim-report-15nov01.htm#StandingCommitteeonSecurityandStability

[76] *Security Committee Charter*, 14 March 2012, http://www.icann.org/en/committees/security/charter-14mar02.htm

[77] **Security Committee**, *Special Meeting of the Board Preliminary Report*, http://www.icann.org/en/minutes/prelim-report-13may02.htm#SecurityCommittee

[78] **Final Report**, *Review of the Security & Stability Advisory Committee* – 14 May 2009 – **JAS Communications LLC** http://www.icann.org/en/reviews/ssac/ssac-review-final-15may09.pdf

[79] *ICANN Security & Stability Advisory Committee* – 15 October 2009 - http://www.icann.org/en/committees/security/sac039.pdf

- March 2010 – A Board Working Group tasked with implementing the independent SSAC review proposed to remove the Security Framework responsibility from the SSAC Charter.

- March 2011 – The ICANN Board approved the Bylaws change recommended by the Board Working Group and tasked the Board Governance Committee with creating a Working Group to address the issue.[80]

In summary, as a result of the SSAC review, the Board decided to relieve the SSAC from the responsibility of creating a comprehensive Risk Management Framework for the DNS and to start creating a new set of structures, embodied mainly in a Board Working Group.[81] During the course of our review, the Board DNS Risk Management Working Group was organized and populated. Its Charter has been made public and approved by the Board. The purpose of the Board DNS Risk Management Framework Working Group is to develop goals and milestones towards the implementation of a DNS security risk management Framework for Internet naming and address allocation services, accompanied by defined timelines and budgetary implications. Further, the Working Group will oversee the creation of an initial assessment which will serve as a baseline for the task.

The scope of the Board DNS Risk Management Framework Working Group is limited to providing oversight towards the definition of goals, milestones and reports for a newly created DNS security Framework. In addition, the Working Group will oversee the creation of a baseline assessment and the integration of this function into

[80] **Approval of Revision of Bylaws re: Implementation of SSAC Review Working Group Report**, *Adopted Board Resolutions – Adopted Board Resolutions Silicon Valley/San Francisco*
http://www.icann.org/en/minutes/resolutions-18mar11-en.htm#1.4

[81] **Final Report**, *Review of the Security & Stability Advisory Committee* - 29 January 2010 - **SSAC Review WG**
http://www.icann.org/en/reviews/ssac/ssac-review-wg-final-report-29jan10-en.pdf
<*http://www.icann.org/en/general/bylaws.htm* Note: The review recommended that this task should be removed because it is out of scope of the activities of the SSAC.

Whereas, on 18 March 2011, the Board approved the amendment to the Bylaws reflecting the removal of task area one from the SSAC Charter, which read "To develop a security Framework for Internet naming and address allocation services that defines the key focus areas, and identifies where the responsibilities for each area lie. The committee shall focus on the operational considerations of critical naming infrastructure."

Whereas, the ICANN Board desires that the work foreseen within task area should be performed by ICANN.

Resolved (2011.03.18.07), the Board directs the Board Governance Committee to recommend to the Board a working group to oversee the development of a risk management Framework and system for the DNS as it pertains to ICANN's role as defined in the ICANN Bylaws. The Board recommends that the BGC consider in its recommendation the inclusion of a member of the working group to come from the SSAC. The Board requests that the BGC submit its recommendation consideration at the Board meeting in Singapore in June 2011."
http://www.icann.org/en/minutes/resolutions-28oct11-en.htm#1.8

regular ICANN Staff activity. In considering its task, the Working Group is directed to take into account: (i) the overarching requirement to preserve the security and stability of the DNS; (ii) ICANN's limited role with regard to security and stability; (iii) input and advice from the technical Community in respect to the implementation of the Framework; and (iv) the relevant documents that have been produced by the SSAC.

The mandate given to the Board DNS Risk Framework Working Group is of an oversight nature, i.e. the Working Group will see to it that others actually create the Framework, not create the Framework by its own, self-contained effort. We strongly recommend that as the Working Group is chartered and begins its work, it take the necessary steps to prioritize the timely completion of a Risk Management Framework. It is important that this group has a clear definition of responsibilities and accountability, to ensure that it will have a demonstrable positive effect on the SSR activities of ICANN.

In parallel to this Board-level activity, following the discussions outlined earlier in this report about the desire for ICANN to facilitate or run a DNS-CERT, the ALAC, ccNSO, GNSO and NRO established the DSSA-WG with the goal of obtaining a better understanding of the security and stability of the global DNS. The DSSA-WG will report to the participating SOs and Acs on:

- the actual level, frequency and severity of threats to the DNS;
- current efforts and activities to mitigate these threats; and
- any gaps in the current security response to DNS issues, to the extent considered appropriate and feasible by the DSSA-WG.

It is foreseeable that the Board structure and others will take up the results from the DSSA and use it as one input for building the Risk Management Framework.

RECOMMENDATION 26: ICANN should prioritize the timely completion of a Risk-Management Framework. This work should follow high standards of participation and transparency.

4.3.4 Risk Management Framework

An organization of ICANN's standing is expected to have a formal mechanism for identifying, understanding and mitigating risk. This activity takes the form of a formal and defined Risk Management Framework. Within this Framework, issues such as severity, likelihood and nature of the risk are captured. This provides a mechanism for prioritizing risk in a consistent manner across the organization. The real benefit of a formalized Risk Management Framework is that it allows important and high impact risks to become highly visible, and it takes both emotion and politics out of risk management.

In discussions with the CSO Team and Supporting Organizations, it has become clear to the SSR Review Team that it can be difficult to prioritize risk and threat assessment due to competing pressures and limited volunteer resources. In a situation such as this, a formalized Risk Management Framework would help provide prioritized

tasking. As previously discussed, until recently, ICANN had not clearly assigned responsibility for creating and maintaining a comprehensive risk management and contingency planning process. This responsibility was originally assigned to the SSAC, but has now transferred to a new Board Committee and other structures which are outlined above.

In the absence of a comprehensive and formalized Risk Management Framework for the DNS, ICANN's CSO Team operates within an informal Framework that allows for organized, successful conduct of operations. IANA however, has a formalized and published Risk Management Framework through which it operates.

A formal Risk Management Framework for ICANN will allow for completeness and better prioritization of risk management at all levels. The most important impact will be seen in the middle sphere of influence since, the Framework should be built in a way that makes it easy for parties to know and be convinced of their roles. It also should stimulate collaboration.

The Risk Management Framework should be participative, incorporate the huge mass of knowledge in the Community, be forward looking, proactive, structured, and able to incorporate dynamic change and scalability.

RECOMMENDATION 27: ICANN's risk-management framework should be comprehensive within the scope of its SSR remit and limited missions.

4.3.5 Incident Response and Notification

ICANN has two roles with regard to incident response which are relevant to this report. First, in the area of direct operations of the DNS infrastructure for L-root, ICANN has an obligation to be aware of and respond to published incidents in a timely manner. This involves collaboration with other DNS software vendors, infrastructure suppliers and DNS operators. The second area of influence is where ICANN can act as a clearinghouse for incident reporting and collaboration. In each of these cases, ICANN is acting in a reactive mode and responding to realized threats.

The SSR Review Team notes that ICANN as an organization has started to take a more proactive stance in the evaluation of threats, which will inform proactive incident response. The hiring of the current CSO (who has a history in the threat identification business) is a positive step in this direction. The Team also notes that ICANN is actively reaching out to Law Enforcement bodies in order to identify threat and coordinate incident response.

In order to maintain a trustworthy Internet, it is imperative to ensure robust incident management, resiliency, and recovery capabilities for the DNS. In an interconnected global environment, weak security in one system compounds the risk to others. No one entity can have full insight into the DNS and its transport networks and all parties have an obligation to share insights about networks and collaborate with others when events might threaten us all. As ICANN continues to build and enhance its own response capabilities, it necessarily will work with others to expand the international networks that support greater global situational awareness and incident response, including all affected parties.

The SSR Review Team finds that ICANN maintains a significant level of readiness for incident response and continuously builds upon its capabilities. The CSO Team is trained and can count on systems and support. It is well networked in the Community for additional ability to predict and prevent incidents and to provide a

resilient response. However, this incident response ability may be too concentrated in the core Team. The size of the organization and the rate of rotation require frequent training for new personnel as well as retraining for those already in. This finding applies as well to the project management system on which the entire IT system relies.

We found less clear evidence of contingency preparedness for ICANN Staff beyond the core CSO Team. Precautions for incident avoidance are in place, but we did not find evidence of follow-up or audits.

ICANN does not constantly share deliberate incident response preparation in the second layer of influence with similar consistency or intensity. Responses from the Supporting Organizations and Advisory Committees will be more ad hoc or based on established procedures for too few people, and will rely on their ability to convene other responders. This can be improved through Best Practice documents developed with ICANN leadership and consensus.

For the third, outermost layer ICANN's incident response and preparedness strategy, or its evolution, must be twofold:

Prevention: outreach and education to the broader user and stakeholder Community is of primary interest. Internet users and domain name Registrants can make good use of educational materials. In many cases, these can be provided on the spot 'just in time, just in place, just enough' and thus requiring cooperation from Registries, Registrars, ISPs, OSPs, and others who are the primary contacts for the users. The SSAC paper on 'Securing Domain Names', which was directed to Registrants, is an example of this trend. Other outreach and educational efforts must be directed to Registries, Registrants, ISPs, OSPs and other entities in closer contact with the domain-name registration system.

Incident response and planning: as discussed elsewhere, the world outside ICANN's SSR remit is not subject to management by ICANN. However, the broader environment is source of risk for incident planning purposes. Hackers, accidents, and errors are part of this broad landscape and must be included in ICANN's preparatory process.

RECOMMENDATION 28: ICANN should continue to actively engage in threat detection and mitigation, and participate in efforts to distribute threat and incident information.

5 Glossary

A

Accountability & Transparency Review (ATRT)

The first completed review under the Amok containing 27 recommendations to enhance activities throughout ICANN, including the governance and performance of the Board, the role and effectiveness of the Governmental Advisory Committee, public Input and public policy processes, and review mechanisms for Board decisions.[82]

Advisory Committee

An Advisory Committee is a formal advisory body made up of representatives from the Internet community to advise ICANN on a particular issue or policy area. Several are mandated by the ICANN Bylaws and others may be created as needed. Advisory committees have no legal authority to act for ICANN, but report their findings and make recommendations to the ICANN Board.[83]

Affirmation of Commitments (AoC)

Signed on September 30th 2009 between ICANN and the US Department of Commerce (Affirmation) contains specific provisions for periodic review of four key ICANN objectives. These reviews provide a mechanism to assess and report on ICANN's progress toward fundamental organizational objectives; they are:

Ensuring accountability, transparency and the interests of global Internet users;

Preserving security, stability and resiliency of the DNS;

Promoting competition, consumer trust and consumer choice;

WHOIS policy.[84]

At-Large Advisory Committee (ALAC)

ICANN's At-Large Advisory Committee (ALAC) is responsible for considering and providing advice on the activities of the ICANN, as they relate to the interests of individual Internet users (the "At-Large" community).

[82] Refer to: http://www.icann.org/en/about/aoc-review
[83] Refer to: http://www.icann.org/fr/about/learning/glossary
[84] Refer to: http://www.icann.org/en/about/aoc-review

Address Supporting Organization (ASO)

The ASO advises the ICANN Board of Directors on policy issues relating to the allocation and management of Internet Protocol (IP) addresses. The ASO selects two Directors for the ICANN Board[85].

c

The Country-Code Names Supporting Organization (ccNSO)

The ccNSO is are the body responsible for developing consensus based global policies relating to country code Top Level Domains and making recommendations on these to the ICANN Board. The ccNSO do much more than policy development and we actively exchange information and best practices for country code top level domain (ccTLD) managers.[86]

Country Code Top Level Domain (ccTLD)

Two letter domains, such as .uk (United Kingdom), .de (Germany) and .jp (Japan) (for example), are called country code top level domains (ccTLDs) and correspond to a country, territory, or other geographic location. The rules and policies for registering domain names in the ccTLDs vary significantly and ccTLD registries limit use of the ccTLD to citizens of the corresponding country.[87]

Computer Emergency Response Team (CERT)

Computer Emergency Response Team is a name given to expert groups that handle computer security incidents. Most groups append the abbreviation CERT or CSIRT to their designation where the latter stands for Computer Security Incident Response Team. For some teams the spelling of CERT refers to Computer Emergency Readiness Team while handling the same tasks.[88]

The CERT Cyber Security Engineering (CSE) team focuses on research and education to help software and systems acquirers, managers, developers, and operators address security and survivability throughout the development and acquisition life cycles—especially in the early stages.[89]

D

[85] Refer to: http://www.icann.org/fr/about/learning/glossary
[86] Refer to: http://www.icann.org/fr/about/learning/glossary
[87] Refer to: http://www.icann.org/fr/about/learning/glossary
[88] Refer to: http://en.wikipedia.org/wiki/Computer_emergency_response_team
[89] Refer to: http://www.cert.org/

DNS Domain Name System (DNS)

The Domain Name System (DNS) helps users to find their way around the Internet. Every computer on the Internet has a unique address - just like a telephone number - which is a rather complicated string of numbers. It is called its "IP address" (IP stands for "Internet Protocol"). IP Addresses are hard to remember. The DNS makes using the Internet easier by allowing a familiar string of letters (the "domain name") to be used instead of the arcane IP address. So instead of typing 207.151.159.3, you can type www.internic.net. It is a "mnemonic" device that makes addresses easier to remember.[90]

DNSSEC

DNSSEC works by digitally signing each DNS record so that any tampering of that record can be detected. The digital signatures, and keys used to create them, are distributed just like any other records in the DNS making DNSSEC backward compatible. Keys in each layer in the DNS hierarchy are signed by keys from the preceding layer which effectively vouches for them just like domain names are delegated from one layer to the next. This "chain of trust" is used to validate the digital signatures accompanying DNSSEC protected records to detect changes.[91]

G

Governmental Advisory Committee (GAC)

ICANN receives input from governments through the Governmental Advisory Committee (GAC). The GAC's key role is to provide advice to ICANN on issues of public policy, and especially where there may be an interaction between ICANN's activities or policies and national laws or international agreements. The GAC usually meets three times a year in conjunction with ICANN meetings, where it discusses issues with the ICANN Board and other ICANN Supporting Organizations, Advisory Committees and other groups. The GAC may also discuss issues between times with the Board either through face-to-face meetings or by teleconference. The Chairman of the GAC is Heather Dryden of Canada.[92]

Generic Names Supporting Organization (GNSO)

The Generic Names Supporting Organization (GNSO) of ICANN is the successor to the responsibilities of the Domain Name Supporting Organization that relate to the generic top-level domains. ICANN's by-laws outline three supporting organizations, of which the GNSO belongs. The SOs help to promote the development of

[90] Refer to: http://www.icann.org/fr/about/learning/glossary
[91] Refer to: http://www.icann.org/en/news/in-focus/dnssec
[92] Refer to: http://www.icann.org/fr/about/learning/glossary

Internet policy and encourage diverse and international participation in the technical management of the Internet. Each SO names two Directors to the ICANN Board.[93]

Generic Top Level Domain (gTLD)

Most TLDs with three or more characters are referred to as "generic" TLDs, or "gTLDs". They can be subdivided into two types, "sponsored" TLDs (sTLDs) and "unsponsored TLDs (uTLDs).[94]

I

Internet Assigned Numbers Authority (IANA)

The IANA is the authority originally responsible for the oversight of IP address allocation, the coordination of the assignment of protocol parameters provided for in Internet technical standards, and the management of the DNS, including the delegation of top-level domains and oversight of the root name server system. Under ICANN, the IANA continues to distribute addresses to the Regional Internet Registries, coordinate with the IETF and others to assign protocol parameters, and oversee the operation of the DNS.[95]

Internet Corporation for Assigned Names and Numbers (ICANN)

The Internet Corporation for Assigned Names and Numbers (ICANN) is an internationally organized, non-profit corporation that has responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions. Originally, the Internet Assigned Numbers Authority (IANA) and other entities performed these services under U.S. Government contract. ICANN now performs the IANA function. As a private-public partnership, ICANN is dedicated to preserving the operational stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy appropriate to its mission through bottom-up, consensus-based processes. The DNS translates the domain name you type into the corresponding IP address, and connects you to your desired website. The DNS also enables email to function properly, so the email you send will reach the intended recipient.[96]

IDNs Internationalized Domain Names

IDNs are domain names that include characters used in the local representation of languages that are not written with the twenty-six letters of the basic Latin alphabet "a-z". An IDN can contain Latin letters with diacritical marks, as required by many European languages, or may consist of characters from non-Latin scripts such as Arabic or Chinese. [97]

Internet Engineering Task Force (IETF)

[93] Refer to: http://www.icann.org/fr/about/learning/glossary
[94] Refer to: http://www.icann.org/fr/about/learning/glossary
[95] Refer to: http://www.icann.org/fr/about/learning/glossary
[96] Refer to: http://www.icann.org/fr/about/learning/glossary
[97] Refer to: http://www.icann.org/fr/about/learning/glossary

The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.[98]

Internet Protocol (IP)

The communications protocol underlying the Internet, IP allows large, geographically diverse networks of computers to communicate with each other quickly and economically over a variety of physical links. An Internet Protocol Address is the numerical address by which a location in the Internet is identified. Computers on the Internet use IP addresses to route traffic and establish connections among themselves; people generally use the human-friendly names made possible by the Domain Name System.[99]

International Organization for Standardization (ISO)

ISO (International Organization for Standardization) is the world's largest developer and publisher of International Standards.[100]

Internet Society (ISOC)

The Internet Society is the international organization for global cooperation and coordination for the Internet and its Internet working technologies and applications. ISOC membership is open to any interested person.[101]

IPV4

IPv4 is the most widely used version of the Internet Protocol. It defines IP addresses in a 32-bit format, which looks like 123.123.123.123. Each three-digit section can include a number from 0 to 255, which means the total number of IPv4 addresses available is 4,294,967,296 (256 x 256 x 256 x 256 or 2^32).[102]

IPV6

IPv6, also called IPng (or IP Next Generation), is the next planned version of the IP address system. (IPv5 was an experimental version used primarily for streaming data.) While IPv4 uses 32-bit addresses, IPv6 uses 128-bit addresses, which increases the number of possible addresses by an exponential amount.[103]

Internet Service Provider (ISP)

[98] Refer to: http://www.icann.org/fr/about/learning/glossary
[99] Refer to: http://www.icann.org/fr/about/learning/glossary
[100] Refer to: http://www.iso.org/iso/about.htm
[101] Refer to: http://www.icann.org/fr/about/learning/glossary
[102] Refer to http://tools.ietf.org/html/rfc791
[103] Refer to: http://tools.ietf.org/html/rfc2460

An ISP is a company, which provides access to the Internet to organizations and/or individuals. Access services provided by ISPs may include web hosting, email, VoIP (voice over IP), and support for many other applications[104].

J

Joint DNS Security & Stability Analysis Working Group (DSSA-WG)[105]

The objective of the DSSA Working Group is to draw upon the collective expertise of the participating SOs and ACs, solicit expert input and advice and report to the respective participating SOs and ACs on:

The actual level, frequency and severity of threats to the DNS;

The current efforts and activities to mitigate these threats to the DNS; and

The gaps (if any) in the current security response to DNS issues.[106]

P

Phishing

Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social engineering schemes use spoofed emails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers.[107]

R

Registrar

Domain names ending with .aero, .biz, .com, .coop, .info, .museum, .name, .net, .org, and .pro can be registered through many different companies (known as "registrars") that compete with one another. A listing of these companies appears in the Accredited Registrar Directory.[108]

Registry

The "Registry" is the authoritative, master database of all domain names registered in each Top Level Domain. The registry operator keeps the master database and also generates the "zone file" which allows computers to route Internet traffic to and from top-level domains anywhere in the world. Internet users don't interact directly

[104] Refer to: http://www.icann.org/fr/about/learning/glossary
[105] Refer to: http://ccnso.icann.org/workinggroups/dssa-wg.htm
[106] Refer to: http://ccnso.icann.org/workinggroups/dssa-wg.htm
[107] Refer to: http://www.icann.org/fr/about/learning/glossary
[108] Refer to: http://www.icann.org/fr/about/learning/glossary

with the registry operator; users can register names in TLDs including .biz, .com, .info, .net, .name, .org by using an ICANN-Accredited Registrar.[109]

RIR Regional Internet Registry

There are currently five RIRs: AfriNIC, APNIC, ARIN, LACNIC and RIPE NCC. These non-profit organizations are responsible for distributing IP addresses on a regional level to Internet service providers and local registries.[110]

Root Servers

The root servers contain the IP addresses of all the TLD registries - both the global registries such as .com, .org, etc. and the 244 country-specific registries such as .fr (France), .cn (China), etc. This is critical information. If the information is not 100% correct or if it is ambiguous, it might not be possible to locate a key registry on the Internet. In DNS parlance, the information must be unique and authentic.[111]

Resource Public Key Infrastructure (RPKI)

The Resource Public Key Infrastructure (RPKI) enables users of public networks, such as the Internet, to verify the authenticity of data that has been digitally signed by the originator of the data.[112]

S

Security and Stability Advisory Committee (SSAC)

The Security and Stability Advisory Committee advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., matters pertaining to the correct and reliable operation of the root name system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services such as WHOIS). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly.[113]

SO Supporting Organizations

The SOs are the three specialized advisory bodies that will advise the ICANN Board of Directors on issues relating to domain names (GNSO and CCNSO) and, IP addresses (ASO).[114]

T

[109] Refer to: http://www.icann.org/fr/about/learning/glossary
[110] Refer to: http://www.icann.org/fr/about/learning/glossary
[111] Refer to: http://www.icann.org/fr/about/learning/glossary
[112] Refer to: http://www.apnic.net/services/services-apnic-provides/resource-certification/RPKI
[113] Refer to: http://www.icann.org/fr/about/learning/glossary
[114] Refer to: http://www.icann.org/fr/about/learning/glossary

Top-level Domain (TLD)

TLDs are the names at the top of the DNS naming hierarchy. They appear in domain names as the string of letters following the last (rightmost) ".", such as "net" in "www.example.net". The administrator for a TLD controls what second-level names are recognized in that TLD. The administrators of the "root domain" or "root zone" control what TLDs are recognized by the DNS. Commonly used TLDs include .com, .net, .edu, .jp, .de, etc.[115]

W

World Wide Web Consortium (WW3)

The W3C is an international industry consortium founded in October 1994 to develop common protocols that promote the evolution of the World Wide Web and ensure its interoperability. Services provided by the Consortium include: a repository of information about the World Wide Web for developers and users; reference code implementations to embody and promote standards; and various prototype and sample applications to demonstrate use of new technology.[116]

WHOIS

WHOIS (pronounced "who is"; not an acronym) An Internet protocol that is used to query databases to obtain information about the registration of a domain name (or IP address).[117]

[115] Refer to: http://www.icann.org/fr/about/learning/glossary
[116] Refer to: http://www.icann.org/fr/about/learning/glossary
[117] Refer to: http://www.icann.org/fr/about/learning/glossary