



17 June 2008

SAC 034: SSAC Comment on the FY09 Operating Plan and Budget¹

Summary

The Security and Stability Advisory Committee believes that ICANN should assign highest priority to projects that uniquely and directly support ICANN's primary mission. SSAC recommends that funding for secondary outreach activities be directed instead to projects which improve ICANN's core function of managing the root zone and top level of the addressing system.

Analysis

SSAC strongly believes that ICANN should assign highest priority to projects that fall uniquely within its purview of and directly support ICANN's primary mission. These include support for:

- root zone management,
- the Internet addressing systems for IPv4 and IPv6,
- protocol parameter registries, and
- security and stability of the TLD registries and registrars.

ICANN must also give reasonable priority to the security and scalability of the systems it operates in support of its missions. These include operation of the L Root and operation of its enterprise systems, both externally visible and internally used.

ICANN's outreach activities, while laudable, are not a substitute for essential security projects. Other organizations such as the regional TLD organizations and ISOC currently perform many of these activities without requiring funds from ICANN.

Several security projects appear to be absent from the budget. These should be supported and given "line item" attention. These include:

1. Support for signing the root zone,
2. Implementation of the ICANN's role as defined in the root server management transition agreement, and
3. Management of certificates for the addressing system (RPKI).

¹<http://www.icann.org/financials/fiscal-30jun09.htm>

Improving Transparency

SSAC recommends that future ICANN strategic plans, operating plans and budgets should classify its activities and projects in the manner below so that the community can better understand how resources are allocated and at what cost. Each project should be classified as either an ongoing activity or a development project. For each project, appropriate key performance indicators and major milestones for determining completion and success should be defined. Further, status reports should be provided on a regular basis.

Many projects and activities fall within ICANN's mission and scope. The Operating Plan and Budget does not describe ICANN project selection process in a way that permits clear understanding or appreciation of the priorities ICANN has set and how its projects meet these priorities.

SSAC invites ICANN to consider organizing ICANN's security- and stability-related activities into the following categories.

- I. Root Zone Management
- II. ICANN Managed Subordinate Zones
- III. Address System Management
- IV. IETF Protocol Parameter Registries
- V. gTLD Registry and Registrar support
- VI. ccTLD Registry support
- VII. L Root operation
- VIII. Externally visible enterprise systems, e.g. email, web site, etc.
- IX. Internal enterprise systems
- X. Other

In the tables below, we have attempted to match the various security-related or stability-related projects to these categories. We include the projects proposed in the Budget as well as projects which SSAC has discussed in other forums but which are not represented in the referenced Budget.

Each project is annotated with

- + if it directly supports ICANN's core mission,
- o if it supports a different business operation,
- # if it's a service that adds value to the community but is not essential to ICANN's core mission, or
- if it's a project that should exist to support ICANN's core mission but is not funded.

Security and Stability-Related Projects (Part 1)

	Area	Projects
I	Root Zone Management	<ul style="list-style-type: none"> + Reliable Update of Root Zone (EPP) + Automated interface for TLD Operators (eIANA) + Trust Anchor Repository for the TLD DNSSEC keys -- DNSSEC for Root Zone -- Root Server Distribution transition to ICANN -- Root server route announcement monitoring -- IRIS/CRISP prototype deployment
II	ICANN Managed subordinate zones (.ARPA, .INT, etc.)	<ul style="list-style-type: none"> + DNSSEC for .ARPA
III	Address System Management	<ul style="list-style-type: none"> -- Address Block Certificates (RPKI)
IV	IETF Protocol Parameter Registries	(No specific initiatives identified)
V	gTLD Registries	<ul style="list-style-type: none"> + Maintain registrar data to preserve choice and protect registrants + Implement Registry Failover Plan including live testing with a registry or registries + RSTEP Evaluations <p># Cooperate with registries and registrars to mitigating malicious activity, especially in eradicating BOTNETs and mitigating DDOS related to fast flux.</p>

Security and Stability-Related Projects (Part 2)

	Area	Projects
VI	ccTLD Registries	<p># Asia/Pacific region ccTLD community training for disaster planning and mitigation</p> <p># Provide continued training on disaster planning and mitigation in other regions of the globe</p> <p># Provide focused assistance/training for capacity building with DNS operator community, especially with ccTLDs.</p>
VII	L Root Operations	<p>o Increase in capacity and multiple locations (anycast)</p>
VIII	Enterprise Security – External	<p>o Protection of the external web sites, email spam filtering, etc.</p>
IX	Enterprise Security – Internal	<p>o Hardening internal servers, VPNs, etc.</p>
X	Other	<p># SSAC Operations</p> <p># Engage ICANN and global cyber security communities representing ICANN and its security perspective and objectives</p> <p># Leverage ICANN’s conduct of operational functions (L-root; .ARPA, etc.) as a platform for enhancing operational practices for DNS operations</p> <p># Work with DNS operational community to establish best practices, enhance information sharing, training and exercise approaches and cooperative programs to enhance security, stability and resiliency mitigation planning to include replicating threats in a technical training/exercise</p> <p># Provide expertise regarding a program to train advanced threat characteristics, mitigation planning to include replicating threats in a technical training/exercise environment establish and begin implementing a staged program across ICANN/DNS community to enhance security capacity</p> <p># Establish best practices sharing and lessons learned repository by end of 2008 assuming heavy partnering with others to develop and disseminate as part of execution approach</p>

We recommend that this organization and these priorities be considered in subsequent operating plan and budget discussions.

Recommendations

1. Fund all projects marked with "--" in the tables above. These critical activities will strengthen ICANN internal operations that support the root zone and the Internet's addressing systems.
2. Consider measures that will improve ICANN's project selection and prioritization choices. Collaborate with relevant constituencies, including the Security and Stability Advisory Committee to provide a basis and rationale for selecting projects. For each project, identify benchmarks for the Fiscal Year as well as metrics that may be used to assess the quality of work performed. (This comment applies to all projects undertaken by ICANN.)
3. Review and re-prioritize the list of outreach related activities, eliminating those activities that are better provided by other organizations. Provide clear deliverables and milestones for each.