FY13 ICANN Security, Stability & Resiliency Framework

17 May 2012

ICANN Security

One World

One Internet

Security, Stability & Resiliency

ICANN's role in SSR and the Internet ecosystem

What is new in this document?

- Part A is largely unchanged from the FY 12 Part A
  - Foundational section describing Bylaws, Affirmation of Commitments and Strategic Plan references to SSR; detailing ICANN's role in SSR and its place in the Internet ecosystem
  - Includes updates based on recommendations from the draft report of the Security, Stability & Resiliency Review Team (dated 15 March 2012)

- Part B Module for FY 13 showing operational priorities in SSR

- Status review of FY 12 Activities (as discussed with SSR Review Team in Dakar, that a scorecard would be a new addition for FY 13)

Terminology

- Security – the capacity to protect and prevent misuse of Internet unique identifiers.
- Stability – the capacity to ensure that the system operates as expected, and that users of the unique identifiers have confidence that the system operates as expected.
- Resiliency – the capacity of the unique identifier system to effectively withstand/tolerate/survive malicious attacks and other disruptive events without disruption or cessation of service.

Note – Definitions were from the 2009, 2010 SSR Plans & FY 12 SSR Framework. Minor wording edits for FY 13 ("identifiers in first bullet, removing "system" from unique identifiers in 2nd, revised Resiliency definition)

Terminology

To coordinate means to actively engage with stakeholders in the global Internet ecosystem to ensure

- Allocation of the Internet's unique identifiers
- Security, stability and resiliency of the Internet's unique identifiers, and
- Operational and policy development functions of the Internet's unique identifiers

Is conducted in an open, accountable and transparent manner and inclusive of the diversity of stakeholders in the ecosystem.

Ecosystem & ICANN's role

- To ensure a single, global interoperable Internet, ICANN's security, stability and resiliency role encompasses three categories of responsibility:

  1. ICANN's operational & stewardship responsibilities (internal operations including L-root & DNS Operations, DNSSEC key signing operations, IANA functions, new gTLD operations);

  2. ICANN's involvement as a coordinator, collaborator and facilitator with the global community in policy and technical matters related to the Internet's unique identifiers;

  3. ICANN's engagement with others in the global Internet ecosystem.

ICANN's Technical Mission

- Coordinating the allocation of the Internet's unique identifier systems [domain names, Internet Protocol (IP) addresses, autonomous system (AS) numbers and protocol port and parameter numbers];
- Coordinating and facilitating the stability, security and resiliency of these systems in policy development;
- Collaborating in the technical protocol development of these systems;
- Maintaining and operating the L-root server as a steward for the community;
- Managing ICANN's operations and internal systems; and
- Providing a publicly accessible information resource on these functions for the greater Internet community.

Ecosystem & ICANN's role

- ICANN does not play a role in policing the Internet or operationally combating criminal behaviour.
- 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.

Ecosystem & ICANN's role

- ICANN is not
  - A law enforcement agency
  - A court of law
  - Government agency
- ICANN cannot unilaterally
  - Suspend domain names
  - Transfer domain names
  - Immediately terminate a registrar's contract (except under limited circumstances
- ICANN is able to enforce its contracts on registries & registrars

Open Questions - Role & Remit

- What does it mean “to coordinate at the overall level the global Internet’s system of unique identifiers?”
- What are the limits of that coordination role?
- What does it mean to ensure the security and stability of the global Internet’s unique identifier systems?

Open Questions - Role & Remit

- What is ICANN's coordination role with root server operators?
- Should ICANN develop a process for transitioning a root server, should a root server operator cease that role?
- What is ICANN's scope of responsibility for addressing an attack against root servers or "against the DNS" in general?

- We are interested in community feedback on the role & remit statement

Evolving Environment

Over the last year, there have been a variety of events that have raised the profile of impacts on the DNS:

- Continued adoption of DNSSEC by TLD operators, ISPs
- Expiration of the free pool of IPv4 address space and growth in IPv6 use
- Growth in IDN ccTLDs; Launch of the New gTLD process
- DNS filtering and blocking legislation
- Government interventions
- Increasing sophistication of denial of service attacks by groups

Developments Over Last Year

- US International Strategy for Cyberspace (16 May 2011) - http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf
- G8-G20 Deauville Declaration (26-27 May 2011) - http://www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html
- EU Commissioner Neelie Kroes' Compact for the Internet (28 June 2011) - http://blogs.ec.europa.eu/neelie-kroes/i-propose-a-compact-for-the-internet/
- OECD Principles for Internet Policy-Making (28-29 June 2011) - http://www.oecd.org/dataoecd/33/12/48387430.pdf
- Council of Europe Principles for Internet Governance (21 Sept 2011) - https://wcd.coe.int/ViewDoc.jsp?id=1835773
- London Conference on Cyberspace (1-2 Nov 2011) - http://www.fco.gov.uk/en/global-issues/london-conference-cyberspace/
- World Economic Forum Principles for Cyber Resilience (27 Jan 2012) - http://www.weforum.org/issues/partnering-cyber-resilience-pcr

Previous Plans, Framework

- May 2009 (covered FY 10) – accepted by the ICANN Board in Sydney, June 2009
  - https://www.icann.org/en/topics/ssr/ssr-draft-plan-16may09-en.pdf
  - http://www.icann.org/en/minutes/resolutions-26jun09.htm#1.7
- Sept 2010 (covered FY 11) – accepted by the ICANN Board in Cartagena, Dec 2010
  - https://www.icann.org/en/topics/ssr/ssr-plan-fy11-clean-23nov10-en.pdf
  - http://www.icann.org/en/minutes/resolutions-10dec10-en.htm#1.8
- May 2011 (covered FY 12) – acknowledged by Board on 28 July 2011
  - http://www.icann.org/en/minutes/resolutions-28jul11-en.htm#2

Timing for FY 13 Framework

- Advance draft copy to SSR RT, Feb 2012
- Initial review by SSAC and small expert group; consultations – Apr 2012
- Publication May 2012 in 5 UN languages
- Comments through June 2012 & after ICANN Prague
- Community briefings before & during ICANN 44 in Prague

Security, Stability & Resiliency

Part B - FY 13 Module

Components of FY13 Framework

PART A – Foundational Section (Ecosystem & ICANN's Role)

Part B – FY 13 Module (Activities & Initiatives)

Status Review of FY 11 & FY 12 Activities

How does Security fit into ICANN's functional areas?

ICANN Functions - Three Areas

- Operational & Stewardship
  - L-root, DNS Operations, KSK Operations, IANA functions, Services Evaluation, Request/Application Evaluation & Management
- Organizational
  - Facilities, Administration, HR, Financial, Legal, Board support, Meetings (Travel & Logistics), Communications, Internal IT & Information Security, Corporate Security & Risk Management
- Multi-stakeholder & Policy
  - Stakeholder Relations (includes Government Affairs, Global Partnerships and Engagement), Policy Support, SSR, Compliance, Protocol Development

Security, Stability & Resiliency at ICANN

Multiple ways to view:

- As a Core Value for ICANN
- As one of the four Strategic Focus areas of the ICANN Strategic Plan
- As an overall thematic area cutting across the organization
- As a stand-alone department
- As a essential element in programs and projects

Security Team Core Areas

- SSR Coordination
- Global Security Engagement, Awareness, Thought Leadership
- Security Collaboration & Capability Training
- Information & Corporate Security Programs (includes ICANN Information Security, Meetings, Physical & Personnel Security)
- Risk Management & Resilience (includes business continuity & exercises, DNS risk management efforts)

ICANN Security Team

- Jeff Moss – VP & Chief Security Officer (Team lead & member of Executive team)
- Geoff Bickers – Dir. of Security Operations (Information Security, Corporate Security Programs & Meetings Security)
- John Crain – Sr. Dir., Security, Stability & Resiliency (Security Collaboration & Capability Building, Global Engagement, Monitoring and work with technical community)
- Whitfield Diffie – VP Information Security & Cryptography (adviser on Info Security)
- Patrick Jones – Sr. Dir., Security (Team coordination, risk management, IDN security and cross-organizational activity)
- Richard Lamb – Sr. Program Manager, DNSSEC (DNSSEC adoption & awareness raising; Global Engagement)
- Dave Piscitello – Sr. Security Technologist (Global Engagement, collaboration with law enforcement & operational security, thought leadership)
- Sean Powell – Information Security Engineer (Network and info security, collaboration with IT and support to Dir. Security Operations)

Cross-Organizational Function

- ICANN's Security team supports activities across ICANN's functions and strategic areas, protecting ICANN's internal Operations & Availability, facilitating international cooperation and participation in DNS coordination; engaging on DNS risk management and resilience

International Cooperation

Risk Management & Resilience

ICANN Operations & Availability

FY 13 SSR Activities

Global Security Engagement	Actions/Events in FY 13
Engagement with broader community, businesses, academic community, technical and law enforcement	4th Global DNS SSR Symposium – partnering with APWG, Fajardo, PR in October 2012
	Participate in events with regional partners
	BlackHat/Defcon in July 2012
	Budapest Conference on Cybersecurity
	Internet Governance Forum
	Caribbean Telecommunications Union events
	Commonwealth Cybercrime Initiative Steering Group meetings

FY 13 SSR Activities

Collaboration	
Further support of DNS measurement and metrics tools, such as RIPE NCC's ATLAS program	Contribute & encourage placement of nodes at edges of network for measurement, conduct data analysis
Root zone automation	Implement automated system with NTIA, Verisign
DNSSEC deployment and adoption	Support training & encourage adoption by developing TLDs, registrars, end users
Training with Operational Security community, law enforcement, Interpol	

FY 13 SSR Activities

Collaboration	Actions/Events in FY 13
Support DNS Security and Stability Analysis Working Group examine risks, threats to DNS & gaps	Working Group will follow its timelines, support publication of findings in FY 13
Technical Evolution of Whois	Contribute to efforts led by others in FY 13
Policy development – Registration Abuse; Registrar Accreditation Agreement	Support GNSO, ccNSO policy development activities
DNSSEC –key rollover work party & audit	Successful KSK ceremonies; SysTrust audit

Corporate Security Programs	
Enhance ICANN's internal network security, access controls, processes following ISO 27002 best practices	Implement process improvements from vulnerability assessments and testing; improve staff training & resources
L-root resilience	Continue to support L-root deployment and root resilience exercises

FY 13 SSR Activities

Corporate Security Programs	Actions/Events in FY 13
Enhance staff training supporting ICANN Computer Incident Response Team on best practices	SANS training or equivalent for IT & Security staff; social engineering training
Internet business continuity plan and crisis communications exercises	Implement lessons learned from root resilience exercises with partners
Meeting security – risk assessments & location, traveler security	Risk assessments on ICANN meeting locations in FY13, FY14; on-ground security & traveler & emergency services (ISOS)

Cross-Organizational	
New gTLD Operations	Support resilient operations for TAS & nTLD processes
Contractual Compliance	Adding X staff; improving registry & registrar compliance

FY 13 SSR Activities

Cross-Organizational	Actions/Events in FY 13
Support to IDN Program	Support string evaluation processes, DNS Stability Panel; produce informational materials on IDNs & security best practices; variant program next phase; Internationalized Registration Data
Enterprise Risk Management	Support internal risk management processes, including Board Risk Committee; DNS risk management framework & study by outside consultant; major program risk tracking
Support to Global Partnerships & Government Affairs	Contribute to educational efforts on technical implications government requirements may have on the Internet's unique identifiers; support engagement with partners & stakeholders; Regional Vice Presidents with engagement

More Information:
icann.org/en/security