FY13 ICANN Security, Stability & Resiliency Framework

1 June 2012

Part B

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

2012-15 Strategic Objectives - SSR

1. Maintain and drive DNS availability
2. Enhance risk management & resiliency of the DNS, IP addresses & parameters
3. Promote broad DNSSEC adoption
4. Enhance international DNS cooperation
5. Improve responses to DNS security incidents

Community Work focusing on

- Continued local DNSSEC adoption and propagation
- DNS blocking & filtering impacts
- DNS Risk Management efforts
- Root resilience & collaboration in response to threats
- IPv6 deployment
- Whois
- Next phase of IDN variant projects

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

ICANN Operations & Availability

- IANA functions
- DNSSEC infrastructure
- DNS Operations & L-root
- New gTLD Operations
- ICANN Computer Incident Response Team, work with IT on monitoring ICANN networks and systems
- Meeting security
- Facilities, Personnel

Risk Management & Resilience

- Support Board Risk Committee - ICANN Risk Landscape
- Support DNS Risk Management Framework Working Group
- Participants in DNS Security & Stability Analysis Working Group
- Staff subject matter experts available to Security & Stability Advisory Committee (SSAC)
- Participants in IT Sector Risk Analysis & Risk Management Working Group (within the IT-SCC)
- Participants in Communications Security Reliability & Interoperability Council Working Group (CSRIC3 under US FCC)
- Support and participate in cyber exercises

International Cooperation

- DNS Collaboration and Capability Building
  - Work with law enforcement & operational security community
  - ccTLD Training (basic operations, attack & contingency response, secure registry operations, DNSSEC training)
  - DNSSEC adoption; root operations support (RSSAC)
- Partnerships & Agreements
- Global Engagement, Awareness, Thought Leadership
  - Example: Commonwealth Cybercrime Initiative

Engagement Criteria

- In February 2012, the Security team formalized its criteria for outreach, engagement and supporting events and activities.
- This is intended to provide clear guidance to the team and Senior Management at ICANN for the types of collaborative and community activities conducted by the Security team.

Types of Events	Example
ICANN Public Meetings	ICANN Prague, Toronto
ICANN Internal Meetings	Ops Mtg, Team Mtg, Board Wksp, Budget Mtgs, Exec
Meetings relevant to operational aspects of ICANN/IANA/L-root/DNSSEC	IETF, DNS-OARC, RIPE NCC, NOGs, SSAC, RSSAC (others)
Meetings where ICANN collaborates on global threat/mitigation	APWG, MAAWG, Team Cymru/Interpol, Cyber exercises
Trainings & Capability Building	ACRP, Secure Registry Ops, DNSSEC, Law Enforcement & Govt (SOCA, OFT, OAS, Interpol), CCI
Symposia, Invited SME conferences, Continuing Education	DNS-EASY, SATIN, SSR Symposium, Security Confab, RSA, BlackHat, FIRST, Unicode
Engagement in Ecosystem, Multi-stakeholder model	RANS, CTU, IGF, APECTEL

Engagement Criteria		✓
Does this support an ICANN Strategic Objective?	1. Maintain, Drive DNS Availability 2. Enhance Risk Mgmt & Resilience of the DNS 3. Promote broad DNSSEC adoption 4. Enhance international DNS cooperation 5. Improve responses to DNS security incidents	
Does this fit within one of the following areas:	a. Operational b. Collaboration c. Training/Capability Building d. Engagement/Awareness	
In support of a partnership, MOU or stakeholder relationship?	Does this support or add to ICANN's institutional reputation?	
How frequently does the event occur?		
Can others be met there or nearby?	Who else is attending?	
Where does this fit in the Budget?	Are we covering for another team?	

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

DNS Capability Building Program

- Training conducted in partnership with the Network Startup Resource Center, ISOC, and regional TLD organizations AfTLD, APTLD, LACTLD
- Over 300 participants from developing region ccTLDs have attended over the life of the program
- In 2011/12, trainings conducted in Australia, Gambia, Senegal, Trinidad & Tobago, Chile
- 6-8 training events planned for FY 13, rotating among Africa, LAC, Asia regions
- Adding training with LE & Op Sec community

Maintaining Clear Processes

- Registry Services Technical Evaluation Panel – RSTEP
- DNS Stability Panel in the IDN ccTLD Fast Track
- Evaluation for confusability and non-contentious strings in the IDN ccTLD Fast Track
- New gTLD program
- Technical Evolution of Whois
- Enterprise Risk Management

Emerging Threats and Issues

- Threats leveraging the DNS & unique identifier system
  - Botnets
  - Denial of Service attacks
  - Social engineering, fraud, malicious conduct
  - Route hijacking
- Threats on the underlying infrastructure
  - TLD & registrar failure
  - Disasters
  - Authority or authentication compromise

Emerging Issues

- IDN implementation and application acceptance, variant issues, IDN tables; Internationalized Registration Data work
- Government interventions
- DNSSEC implementation & adoption
- IPv6/IPv4 address space issues – working with RIRs
- Interactions between the DNS and applications (such as mobile apps, social media apps) – for awareness
- Increasing engagement with law enforcement and user communities on SSR

Work on Emerging Threats

- DNS Security & Stability Analysis Working Group
  - Charter approved at Cartagena meeting in Dec 2010
  - WG composed of ALAC, ccNSO, GNSO, NRO, GAC, SSAC reps and other experts
  - Undertaken & led by community representatives
    1. WG will examine actual level, frequency and severity of threats to DNS
    2. The current efforts and activities to mitigate these threats
    3. The gaps (if any) in the current security response to DNS issues

Ongoing work on collaborative response

- Collaborative Response on botnets & malicious conduct – ICANN will continue to contribute to the Conficker Working Group and will work with trusted security community, registration infrastructure providers and law enforcement in this area – benefits the greater Internet community

- Supportive of AntiPhishing Working Group and MAAWG efforts; engaging with IT-ISAC (Information Technology Information Sharing and Analysis Center)

FY 13 Resourcing

- ICANN’s FY 13 Operating Plan & Budget projects expenses of approximately $74 mil USD
- Security team initiatives estimated to be approximately $3.6 million USD in FY 13
- Additional percentage of budget from Compliance, nTLD Operations, DNS Ops, IT, among others, has SSR elements

FY 13 Resourcing – Security team

- $1.83m for Personnel
- Professional Services $1.38m
- $255k for travel & meetings
- $68k for administrative (subscriptions, training & skill-building for staff, etc)

Note – these figures may be adjusted if priorities change or based on direction from senior management.

FY 13 Resourcing – Security team

Professional services includes:

- DNS Security & Law Enforcement Training Capability Program ($200k)
- DNSSEC Adoption & Awareness ($160k)
- IT process auditing, monitoring tools ($200k)
- Physical security on office moves in Playa Vista & Brussels ($72k)
- Meeting, Travel Security ($210k)
- Risk Landscape Assessments ($125k, $40k)
- Mobile device, email security ($144k)

FY 13 Contractual Compliance

- Continue to grow Compliance resources in numbers & expertise to:
  - Improve operations with increased monitoring & proactive enforcement of contracts and policies
  - Proactively engage and collaborate with registrars to improve compliance and reduce complaints
  - Promote a culture of Compliance & increase awareness through global outreach
  - Support resource increases w/Registry, Registrar, Legal, IT, Finance, Security, Policy teams

FY 13 Contractual Compliance

- Continue to grow Compliance resources in numbers & expertise to:
  - Standardize operations, systems, tools for efficiency & effectiveness (automation in complaint tracking, replace current complaint intake systems, etc)
  - Communicate, develop, implement robust Compliance risk and audit strategy
  - Develop performance metrics for core operations & improve and deliver fact-based communications and reporting to the community

Conclusion

ICANN’s SSR Plan “will evolve over time as part of the ICANN strategic and operational planning process, allowing ICANN efforts to remain relevant and to ensure its resources are focused on its most important responsibilities and contributions.”

This Framework is intended to demonstrate a commitment to further improvements in ICANN’s strategic and operational planning for SSR, as well as a recognition of ICANN’s capacity limitations and willingness to collaborate for the benefit of the greater community.

Status Review of FY 12

FY 12 - Area	Program/Initiative	Status
Global Security Outreach	Conduct 3rd Global DNS SSR Symposium	Held in October 2011 with GC-SEC in Rome
	Other global engagement	SATIN 2012, March in UK; APWG; MAAWG; OAS
		APNIC/APRICOT; Caribbean Telecom Union; RSA; APT
Collaboration	DNS Capability Training (DNSSEC & ACRP)	Training sessions conducted in FY 12 in Trinidad, Chile, Gambia, Senegal, Australia
		Engagement with Commonwealth Cybercrime Initiative & CCI Steering Group; Interpol
	Measurement – RIPE ATLAS	Sponsorship contribution to RIPE ATLAS program, distribution of nodes through ICANN Security networks
	Measurement – L-root	Support for L-root resilience and distribution

FY 12 - Area	Program/Initiative	Status
Collaboration	Technical Evolution of Whois	Supporting work in SSAC, community, IETF
	DNSSEC – participate in key ceremonies; SSAC work party on key rollover	Conducted key ceremonies in Culpeper & El Segundo; participating in SSAC work party
	DNSSEC – support efforts related to SysTrust audit & certification	SysTrust audit successfully completed
		Key signing infrastructure with PCH in Singapore; supported DPS with NIC.CR
	Root resilience	Collaborative exercises with partners & root operators in March 2012
	LE & Op Sec	Workshops in Dakar, Costa Rica; APWG
		UK SOCA, OFT

FY 12 - Area	Program/Initiative	Status
Corporate & Information Security Programs	Improved network security monitoring and resourcing	Added Information Security Engineer (internal transfer from ICANN IT, Sean Powell)
	TAS Resilience – nTLD Operations	Supported testing and monitoring on TAS pre-launch and during nTLD Application Process
		Incident response on TAS outage in April 2012
		Social engineering testing of ICANN staff and processes
	Meeting Security	Covered ICANN Dakar, Costa Rica; preparations for Prague & upcoming meetings in FY 13
	Physical Security	Office moves in Los Angeles & Brussels

FY 12 - Area	Program/Initiative	Status
Corporate & Information Security Programs	Mobile Device Policy development	Developing mobile device policy with IT
	S/MIME Certificates for Email	Improved internal email and developed plans for FY 13 email infrastructure changes
	Best practices toward ISO 27001 series	Documented against gaps
	SANS training for IT staff	Training conducted; supported social engineering training for staff
	Business Continuity Planning	Retained business continuity expert to review plans and assist with documentation in March 2012
Cross-Organizational	Compliance	Assisted Compliance with registrar incident in Australia; guidance with LE

FY 12 - Area	Program/Initiative	Status
Cross-Organizational	IDN Programs	Supported IDN ccTLD Fast Track with DNS Stability Panel; Unicode liaison; IDN Variant Project case study
	IANA	Support with documentation for Security
	Traveler Security	International SOS service for ICANN travelers
	Global Partnerships/Government Affairs	Support for meetings and engagement on ICANN SSR activities
Thought Leadership	Increase papers and publications	Guidance on Domain Seizures and Takedowns published; comments to Interpol, Unicode; Article on RESTful Whois (USENIX)
		DNSSEC overview and materials for ICANN meetings & presentations

FY 12 - Area	Program/Initiative	Status
Risk Management	IT-SCC DNS Risk Update	Participating as subject matter experts; report to be released by IT-SCC/US DHS
	Board-level DNS Risk Management Framework WG	Developing staff assessment for DRMFWG; will seek consultant to assist with Risk Management Framework
	Community-led DNS Security & Stability Analysis WG	Supporting DSSA WG, WG making progress on threat analysis for Prague
	Internal Risk Management	Supporting program-level risk reviews and reports to Board Risk Committee

One World

One Internet

More Information:
icann.org/en/security