FY12 ICANN Security, Stability & Resiliency Framework

2 May 2011

Security, Stability & Resiliency

Part B - FY 12 Module

Components of a New Framework

Part A

- Foundational Section – Mission, Core Values, Affirmation
- Ecosystem and ICANN's role

Part B – Fiscal Year 12 Module

- Categories of Action
- Strategic Projects; Community Work
- Organizational/Staff Program Areas

Three Categories of Action in SSR

- Areas of ICANN Operation
  - Internal IT, L-root, DNS Operations, IANA, Compliance, String Evaluation, Meetings logistics, Administration & Finance, among other areas
- Areas where ICANN acts as a coordinator, collaborator, facilitator with the community
  - Policy coordination, secretariat support, subject matter expert involvement, contributor on protocol development, engagement with the greater Internet community, including the technical community
- Areas where ICANN is an observer or aware of activities of others in the global Internet ecosystem

Area of Interest	Program/Initiative	Organizational Lead
Operational Responsibility	IANA functions	IANA functions staff
	DNS Operations/L-root	DNS Operations staff
	DNSSEC management	DNS Operations staff
Includes ICANN organizational support,	IT & internal network security	ICANN Security, IT staff
Finance, HR, Legal	Meetings security	ICANN Security staff
Administration	Physical/Personnel security	ICANN Security staff
	ICANN Business Continuity Plans & crisis communications	ICANN Security staff, IT
	Contractual Compliance	Compliance staff
	IDN Fast Track management	IDN team
	New gTLD implementation	New gTLD team

Area of Interest	Program/Initiative	Organizational Leads
Coordinator	Policy development process	SOs, ACs + Policy staff
	Root zone management automation	RZM partners NTIA, ICANN, Verisign
	IPv6/IPv4	NRO, RIRs, ICANN
Facilitator	Secretariat support to SOs & ACs	Policy staff
	Technical Evolution of WHOIS	Community + ICANN
Collaborator	DNS Capacity Building	ICANN + NSRC, regional TLD orgs, ISOC, community
	RPKI development	DNS Ops + NRO, RIRs
	Protocol development	IETF
	DNS measurement & metrics	RIPE NCC, DNS-OARC, others
	IDN Guidelines; Variant Mgmt	Registries + ICANN; community

Area of Interest	Program/Initiative	Organizational Leads
Coordinator	Work with Root Server Operators	RSSAC
Facilitator	Global Symposium on SSR	Security staff + community
Contributor	Resilience metrics, DNS health	ENISA + CERTs, others
Coordinator	DNSSEC adoption and deployment	DNS Ops + Registries, Registrars, Users
Facilitator	ccNSO Meetings, Tech Days	ccTLD community
Collaborator	DNS risk management strategy	Community efforts supported from Security
Facilitator	DNS Security & Stability Analysis Working Group	SO & AC participants with independent experts
Collaborator	Global Security outreach, engagement & awareness raising	ICANN Security & Global Partnerships
Collaborator	Engagement with trusted security community, business, law enforcement	ICANN Security staff

Area of Interest	Program/Initiative	Organizational Leads
Awareness of activities	IETF, IAB activities	IETF, IAB
lead by others in the community;	NRO, RIR activities	AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC
Observer role	Regional TLD organization activities	AfTLD, APTLD, CENTR, LACTLD
	International Cyber Exercises (in some cases, contributor)	Exercise coordinators (DHS, ENISA, others)
	Government developments on cyber security & critical infrastructure protection	Governments, IT-SCC, others
	Trusted Identities in Cyberspace	
	Law enforcement initiatives on malicious conduct	Interpol, Int'l law enforcement
	Risk management initiatives	
	Academic research on DNS	
	Registration practices developments	Registries, registrars, community

2011-14 Strategic Objectives

1. Maintain and drive DNS uptime
2. Increase security of the overall systems of unique identifiers
3. Increase international participation in unique identifier security
4. Coordinate DNS global risk management

Community Work

- Local DNSSEC adoption and propagation
- Whois Internationalized Registration Data
- Develop solutions for DNS (and unique identifier) security – DSSA-WG, others
- IPv6 rollout; IPv4 exhaustion risk management
- Resource Public Key Infrastructure (RPKI) deployment – with RIRs
- IDN variant case studies

Security Team Core Areas

- Global Security Outreach (Engagement, Awareness with the Global Community and greater ICANN Community)
- Security Collaboration
- DNS Capacity Building
- Corporate Security Programs (includes ICANN Information Security, Meetings, Physical & Personnel Security), Business Continuity, Risk Management
- Cross-Organizational Support (includes new gTLDs, IDNs, DNSSEC, Policy Development, Compliance, Global Partnerships/Government Affairs)

FY 12 SSR Activities

Global Security Outreach	Actions/Events in FY 12
Engagement with broader community, businesses, academic community, technical and law enforcement	DNS SSR Symposium – potentially Europe Q3 2011 or Q1 2012
	Participate in events with regional partners

Collaboration	
Support adoption 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
RPKI/Resource Certification development	Work with RIRs

FY 12 SSR Activities

Collaboration	Actions/Events in FY 12
Support DNS Security and Stability Analysis Working Group examine risks, threats to DNS & gaps	Working Group will follow its timelines, may publish findings in FY 12
Technical Evolution of Whois	Contribute to efforts led by others in FY 12
Policy development – Registration Abuse; Registrar Accreditation Agreement	Support GNSO, ccNSO policy development activities
DNSSEC – periodic key rollover & audit	Complete SysTrust Audit and successful KSK ceremonies on key rollover

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	Implement improvements from FY 11 L-root contingency exercise; L-single nodes

FY 12 SSR Activities

Corporate Security Programs	Actions/Events in FY 12
Enhance staff training supporting ICANN Computer Incident Response Team on best practices	SANS training or equivalent for IT & Security staff
Internet business continuity plan and crisis communications exercise	Retain FTE for business continuity & exercise support
Meeting security – risk assessments & location, traveler security	Risk assessments on ICANN meeting locations in FY12; on-ground security & traveler & emergency services (ISOS)

Cross-Organizational	
New gTLD implementation	Launch new gTLD process (pending approval of program); vulnerability testing on TAS; [see separate slide on new gTLDs]
Contractual Compliance	Adding 3+ staff; improving registry & registrar compliance

FY 12 SSR Activities

Cross-Organizational	Actions/Events in FY 12
Support to IDN Program	Support string evaluation processes, DNS Stability Panel; produce informational materials on IDNs & security best practices; variant management case studies
Enterprise Risk Management	Support internal risk management processes, including Board Risk Committee; conduct risk reassessment prior to FY 13 Operational Plan & Budget development
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

Community SSR Work

- Enhancements to the Registrar Accreditation Agreement – GNSO
- SSAC and RSSAC activities
- Collaborative response to malicious abuse of the unique identifier system – Conficker & trusted security community
- Policy development – such as Registration Abuse Working Group; Internationalized Whois

Tracking the Affirmation of Commitments areas of emphasis

- Continuity and contingency work
- Maintaining clear processes
- Focus on emerging threats and risks

Continuity & Contingency Work

- DNS Capacity Building Program, including Attack & Contingency Response, Secure Registry Operations Courses for regional TLD organizations and operators, DNSSEC training and support
- ICANN contingency plans and exercises
- Participation in international exercises with operators
- Data escrow processes & registrar data escrow program

DNS Capacity Building Program

- Training conducted in partnership with the Network Startup Resource Center, ISOC, and regional TLD organizations AfTLD, APTLD, LACTLD
- Over 250 participants from developing region ccTLDs have attended over the life of the program
- In 2010/11, trainings conducted in Mali, Jordan, Guatemala, Hong Kong (supporting Nicaragua & Kenya events before ICANN Singapore meeting)
- At least 8 training events planned for FY 12, rotating among Africa, LAC, Asia regions

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
- 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 12 Resourcing

- ICANN's FY 12 Operating Plan & Budget projects expenses of $69.8 mil USD
- SSR initiatives as a whole estimated to be 17% of ICANN's total budget (approximately $12 mil USD in FY 12)

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 an evolution 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.

One World

One Internet

More Information:
icann.org/en/security