ICANN Plan to Enhance Internet Security, Stability & Resiliency

24 June 2009

Greg Rattray

Chief Internet Security Advisor

Principles Guiding Drafting

- Plan intended as an initial foundation focused on ICANN role definition and framework for delineating programs, activities and resources
  - Not tabling new initiatives; programs and activities already part of ICANN strategic & operational plans
  - Why? – Need community buy-in on starting point

Plan Purpose (Section 1)

- Delineate ICANN role
- Overview existing programs & activities
- Detail planned activities & resource commitments in FY 10
  - Integrated into ICANN strategic and operational planning

Challenges and Opportunity (Section 2)

- Growing misuse of the Internet
  - Often leverages the unique identifier systems
- ICANN has long-standing commitment to “ensure stable and secure operation of the Internet's unique identifier systems”
- Plan provides the community a roadmap for ICANN efforts

ICANN's Role (Section 3)

- ICANN focuses on its core missions related to the Internet's unique identifier system
- ICANN does not play a role as a policeman in operationally combating criminal behavior
- ICANN does not have a role regarding use of the Internet for cyber-espionage and cyber war
- ICANN does not have a role in what constitutes illicit content on the Internet
- ICANN will continue to participate in activities with the broader Internet community to combat abuse of the unique identifier systems that enable malicious activity

ICANN Contributors (Section 4)

- Activities engage most elements ICANN Staff
  - Security staff serves as orchestrator
- Supporting Organizations and Advisory Committees
  - SSAC and RSSAC identified explicitly

ICANN Programs (Section 5)

- ICANN is directly responsible for IANA operations as the highest priority
- ICANN is an enabler for the DNS and addressing community efforts to strengthen the security, stability and resiliency including supporting protocols to authenticate Internet names and numbers
- ICANN is an enabler and facilitator of the security, stability and resilience activities conducted by DNS registry and registrars
- ICANN is directly responsible for the secure, stable and resilient operation of its own assets and services
- ICANN is a key participant in broader forums and activities related to the security, stability and resiliency of the Internet's unique identifier systems

Major Program Elements

- 5.1 Core DNS/Addressing Security, Stability and Resiliency
  - 5.1.1 IANA Operations
  - 5.1.2 Root Server Operations
- 5.2 TLD Registries and Registrars
  - 5.2.1 gTLD Registries
  - 5.2.2 new gTLDs and IDNs
  - 5.2.3 gTLD Registrars
  - 5.2.4 Contractual Compliance
  - 5.2.5 Protecting gTLD Registrants
  - 5.2.7 ccTLDs
  - 5.2.8 IANA Technical Requirements
  - 5.2.9 Collaborative Response to Malicious Abuse of DNS
  - 5.2.10 Enabling Overall DNS Security and Resiliency

Major Program Elements (cont.)

- 5.3 Engaging with Number Resource Organization (NRO) & Regional Internet Registries (RIRs)
- 5.4 ICANN Corporate Security and Continuity Operations
  - 5.4.1 Security Programs
  - 5.4.2 Business Continuity Program
- 5.5 Activities of ICANN Support Organizations and Advisory Committees
- 5.6 Global Engagement to Enhance Security, Stability and Resiliency
  - 5.6.1 Global Partners and Activities
  - 5.6.2 Regional Partners and Activities
  - 5.6.3 Working with Governments

ICANN FY10 Plans: Key Initiatives (Section 6)

- **6.1.1 IANA Operations**: Key initiatives include improving root zone management through automation; improved authentication of communications with TLD managers; and supporting DNS Security Extensions (DNSSec) implementation
- **6.1.2 DNS Root Server Operations:** Continuing to seek mutual recognition of roles and responsibilities and initiate a voluntary effort to conduct contingency planning and exercises
- **6.2.1 gTLD Registries**: Establish processes for applicant evaluation and operation of new gTLD and IDN applicants to ensure technically secure operations & ensure protection of registrants. ICANN will mature the gTLD registry continuity plan and test the data escrow system
- **6.2.4 ccTLD Registries:** ICANN will focus its collaboration on maturing the joint Attack and Contingency Response Planning program established in conjunction with the ccNSO and the regional TLD associations and working more closely with ISOC on technical capacity building

ICANN FY10 Plans: Key Initiatives (cont.) (Section 6)

- **6.2.6 Contractual Compliance:** ICANN will increase the scope of contractual enforcement activities to include initiating audits part of implementing the March 09 RAA amendments and identify potential involvement of contracted parties in malicious activity for compliance action.
- **6.2.7 Response to Malicious Abuse of Domain Name System:** ICANN will build on its collaborative efforts to enable understanding of activity involving malicious conduct enabled by the use of the DNS and facilitating information sharing to respond
- **6.4 Internal ICANN Security and Continuity Operations**: ICANN will ensure its security programs are conducted within overall corporate risk management, crisis management, and business continuity programs. A major focus will be the establishment of a sound foundation of documented plans and supporting procedures
- **6.5 Ensure Global Engagement and Cooperation**: ICANN will further extend strong partnerships and engage in global dialogues to foster understanding of the security, stability, and resiliency challenges and improve response capabilities

Example Slide:

Corporate Security Program (Security, IT, others across staff)

Objectives

- Improve and implement IT/Facilities/ Personnel Security Programs
  - Establish Formal Plans
    - Institute Security Training
- Implement Traveler and Meetings Security & Contingency Plans

Deliverables (milestones)

- Conduct Security Training Programs (part of ICANN on-boarding by Sep 09)
- Improved IT & Physical Access Control Systems implemented (IT authentication on key systems – Fall 09)
- Exercise Traveler and Meetings Security (one drill per trimester)
- Security Program outside audit (April 10)

Key Stakeholders

- ICANN Security & Resiliency Team
- ICANN IT/IANA/DNS Ops
- ICANN Human Resources
- ICANN Global Meetings Team
- Other ICANN Staff

Resources

Human – 2 FTEs (includes IT support for security)

Financial – $1.1 M including FTEs, physical & IT access controls, professional services for conducting training and audits