FY12 ICANN Security, Stability & Resiliency Framework

14 April 2011

ICANN

One World

One Internet

ICANN is a global organization that coordinates the Internet's unique identifier systems for worldwide public benefit, enabling a single, global interoperable Internet.

ICANN's inclusive multi-stakeholder model and community-developed policies facilitate billions of computers, phones, devices and people into one Internet.

Executive Summary

The Internet has thrived as an ecosystem engaging many stakeholders organizing through collaboration to foster communication, creativity and commerce in a global commons.

The interoperability of the global commons depends on the operation and coordination of the Internet's unique identifier systems.

ICANN and the operators of these systems acknowledge that maintaining and enhancing the security, stability and resiliency of these systems is a core element of their collaborative relationship.

Security, Stability & Resiliency FY 12 Framework

- The SSR Framework outlines to a wide range of stakeholders how ICANN will contribute to global efforts in addressing security, stability and resiliency as challenges for the Internet, focused on its mission related to the Internet's unique identifiers.
- The framework describes the foundation for ICANN's role and boundaries to how it engages in this area; overviews the ecosystem, ICANN community and staff structure, strategic objectives and planned activities through the next operational year.
- The framework provides a roadmap as to how ICANN meets its responsibilities.

Components of a New Framework

- Foundational Section – Mission, Core Values, Affirmation
- Ecosystem and ICANN's role
- Annual Update – Fiscal Year Module
  - Community Work
  - Strategic Projects
  - Organizational/Staff Program Areas

Foundational – ICANN's Mission

The mission of ICANN is to coordinate, at the overall level,

the global Internet's

systems of unique identifiers,

and in particular, to ensure the stable and secure operation

of the Internet's unique identifier systems.

Source: ICANN Bylaws as amended 25 January 2011

Core Value #1

Preserving and enhancing the operational stability, reliability, security, and global interoperability of the Internet

Source: http://www.icann.org/en/general/bylaws.htm#I

Acknowledged in the Affirmation of Commitments: "global technical coordination of the Internet's underlying infrastructure – the DNS – is required to ensure interoperability"

Security, Stability, Resiliency

- Security – the capacity to protect and prevent misuse of Internet name and numbering systems.
- Stability – the capacity to ensure that the system operates as expected, and that users of the unique identifier systems have confidence that the system operates as expected.
- Resiliency – the capacity of the unique identifier systems to effectively respond to, react to and recover from malicious attacks and other disruptive activity.

Note – Definitions were from the 2009, 2010 SSR Plans.

Challenge

- Misuse of and attacks against the DNS and other Internet infrastructures challenge overall unique identifier security. Cyber security attacks target individuals, corporations, civil society and governments.
- As the frequency and sophistication of disruptive attacks and other malicious behaviour increases, ICANN and its community must continue to collaborate toward improving the resilience of the unique identifier systems and strengthen its capabilities.

Challenge

- Increasingly, the activity on the Internet reflects the full range of human motivations and conduct. In part, such activity reflects the open nature of the Internet that has made it successful, enabled innovation at its edge, and allowed for communication, creativity and commerce in a global commons.
- But openness has also come with vulnerabilities. For example, activity that takes advantage of opportunities to spoof or poison DNS resolution to misdirect computer connections of unwitting users is growing.
- Routing hijacks, address registration and ASN hijacks continue to grow. Denial of Service attacks disrupt users of all types.

Affirmation of Commitments

- 3(b) Preserve the security, stability and resiliency of the DNS
  - ICANN has adopted an SSR Plan, which will be regularly updated to reflect emerging threats to the DNS [including unique identifiers, not just DNS]
  - This will be reviewed no less than every three years

Affirmation of Commitments by the US Department of Commerce and ICANN, signed 30 September 2009

Previous SSR Plans

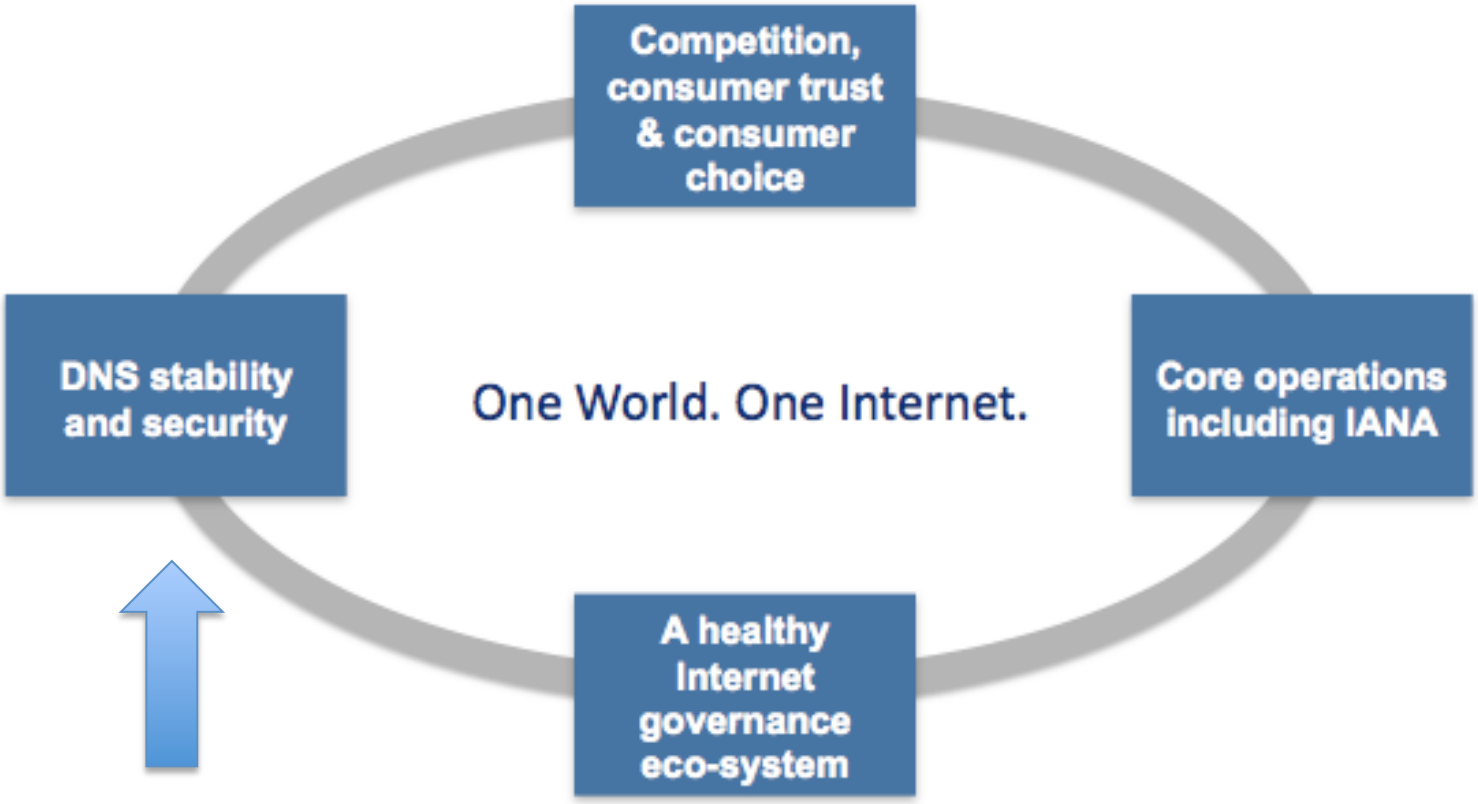
- May 2009 (covered FY 10) – accepted by the ICANN Board in Sydney, June 2009
  - https://www.icann.org/en/topics/ssr/ssr-draft-plan-16may09-en.pdf
  - http://www.icann.org/en/minutes/resolutions-26jun09.htm#1.7
- Sept 2010 (covered FY 11) – accepted by the ICANN Board in Cartagena, Dec 2010
  - https://www.icann.org/en/topics/ssr/ssr-plan-fy11-clean-23nov10-en.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

Timing for FY 12 Framework

- Initial review 1-8 Apr 2011 (SSAC and small expert group)
- Translation prep 11-27 Apr 2011
- Publication 27 Apr 2011 with translations
- Comment period to 27 May 2011
- Present to Board at ICANN 41 in Singapore, June 2011

2011-14 Strategic Plan Areas

See http://www.icann.org/en/strategic-plan/strategic-plan-2011-2014-28mar11-en.pdf



Components of a New Framework

- Foundational Section – Mission, Core Values, Affirmation
- Ecosystem and ICANN's role
- Annual Update – Fiscal Year Module
  - Community Work
  - Strategic Projects
  - Organizational/Staff Program Areas

Ecosystem & ICANN's role

- ICANN is charged to operate for the benefit of the Internet community as a whole. The public is a diverse and disparate collection of communities knitted together by the Internet and operating as a complex ecosystem.
- As the Internet continues to be a greater enabler of gross domestic product, government daily operations and global security activities, the profile of Internet governance has also elevated.

Ecosystem & ICANN's role

- ICANN acts in accordance with its bylaws in conducting multi-stakeholder, consensus-based processes, policies and programs, including those related to security, stability and resiliency.
- ICANN's role must focus on its core missions related to the unique identifier systems.
- ICANN's role includes participating in activities with the broader Internet community to combat abuse of the unique identifier systems. These activities will involve collaboration with governments combating malicious activity.

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

The Ecosystem at Work in SSR

- Nov 2001- International public meeting focused on Security and Stability of the Internet Naming and Address Allocation System
- 2002 - Security and Stability Advisory Committee formed, continues to this day (http://icann.org/en/committees/security/)
- Supporting tech days with the ccTLD community at ICANN meetings since 2006
- Annual contingency exercises since 2008
- Conficker Working Group, 2008-present
- Global DNS SSR Symposia in 2009 (Georgia Tech), 2010 (Kyoto)
- Collaborated on signing of the root zone with DNSSEC in 2010 (http://root-dnssec.org)

Responsibilities

- ICANN is responsible for Internet Assigned Numbers Authority (IANA) functions operations. Ensuring secure, stable and resilient operation of the DNS root zone function has been, and will remain, the highest priority.
- ICANN is an enabler for the DNS and addressing community efforts to strengthen SSR foundations of the system. Such efforts will include supporting the development of protocols and supporting technologies to authenticate Internet names and numbers.
- ICANN is an enabler and facilitator of the SSR activities conducted by DNS registries, registrars and other members of the community.

Responsibilities

- ICANN is responsible for the secure, stable and resilient operation of its own assets and services.
  - ICANN maintains an internal Computer Incident Response Team, https://www.icann.org/en/cirt/, and has joined FIRST
  - Supports annual updating of ICANN security plans and effective security controls and procedures
  - Ensures internal staff have strong skills, appropriate tools and are current with security threats and best practices
  - This work includes stable, continuous L-root operations; DNSSEC key management

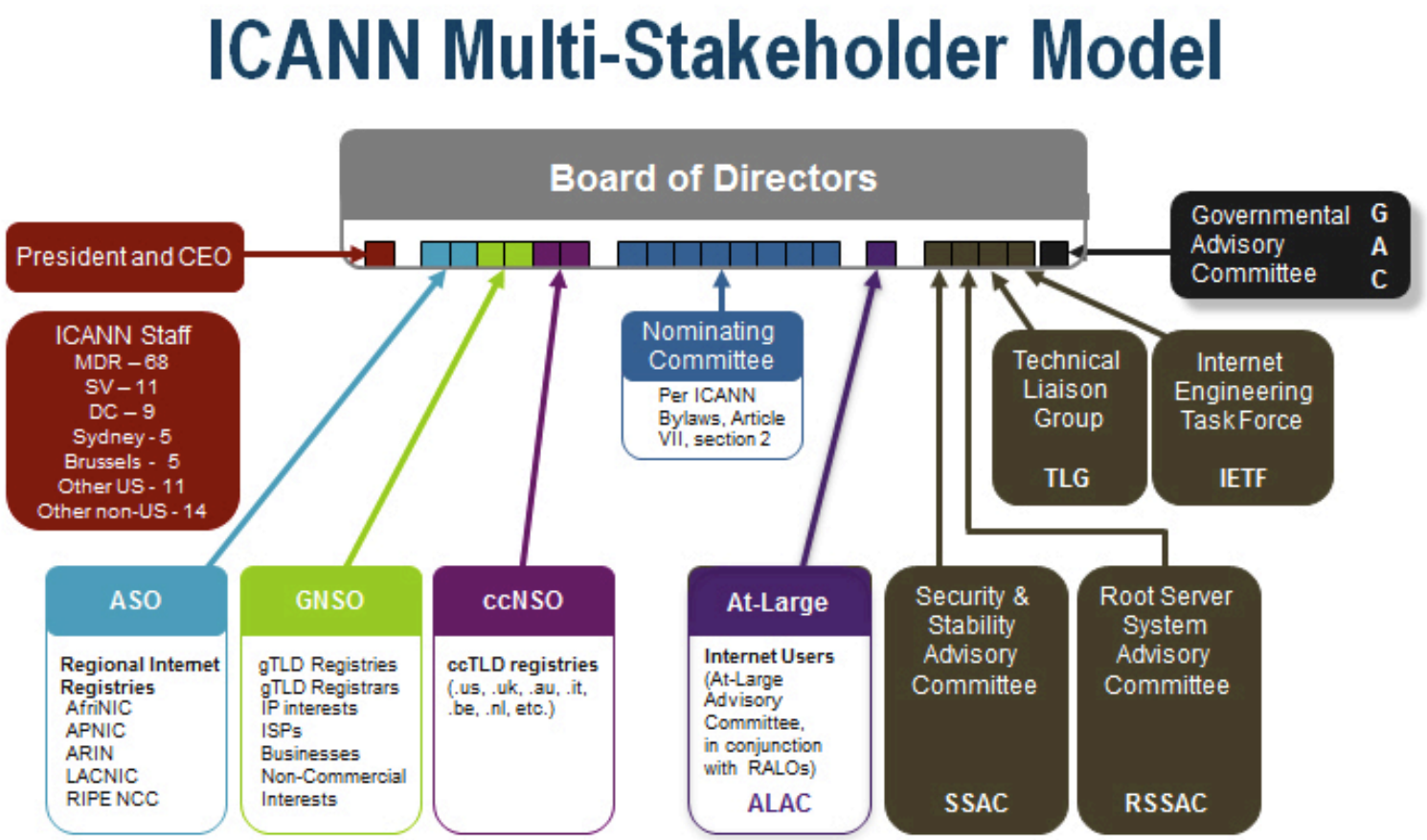
Ecosystem Layers

- Global Community – those who rely on the secure & stable functions of the Internet's unique identifier systems, but may not be aware of or participate in ICANN
- ICANN Community – greater community of actors involved in ICANN programs, processes and activities who drive the multi-stakeholder, private-sector led policy development model for the benefit of global Internet users
- ICANN Organizational Operations/Staff – the operational structures, processes and supporting staff of ICANN as an organization

Ecosystem Participants

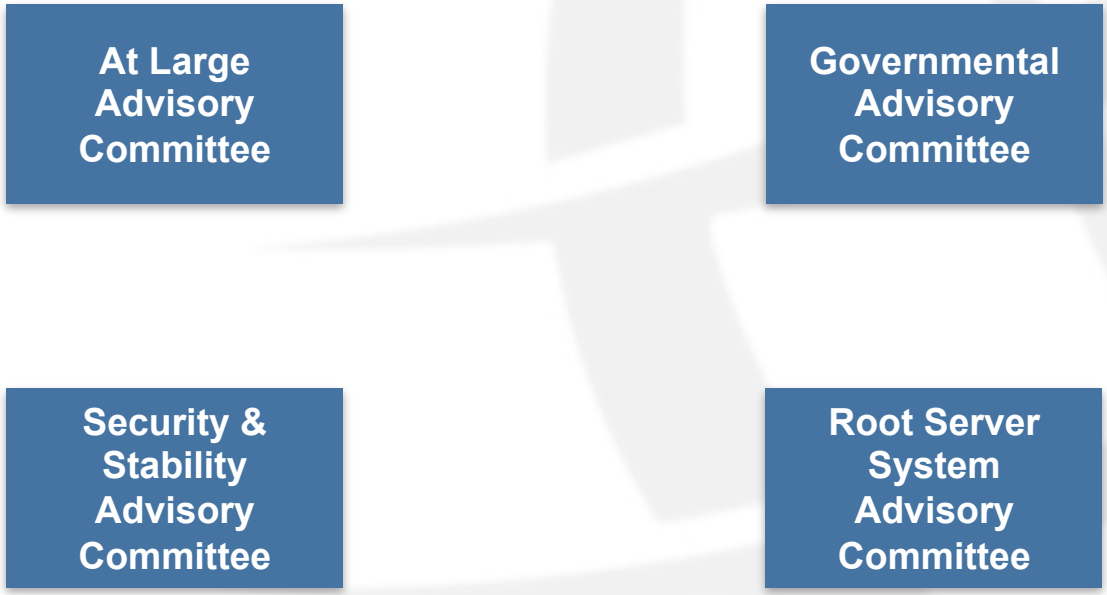
- Technical Community
- Governments & NGOs
- Business
- Noncommercial & Academic
- Users/At-Large
- Law Enforcement & Operational Security

ICANN Organization



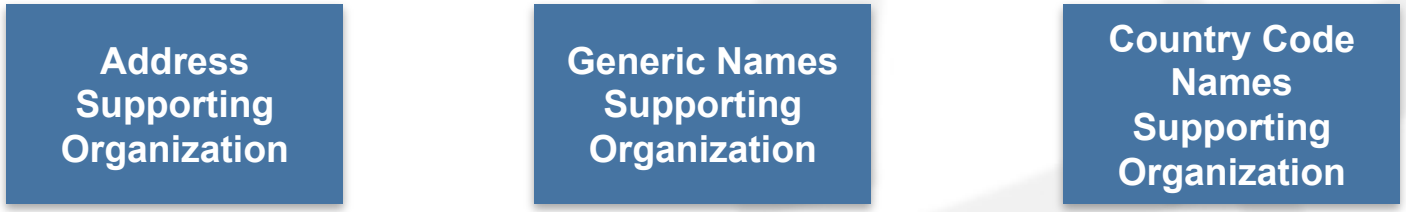
ICANN Community Structures

- Advisory Committees advise the ICANN Board, provide input into policy development processes and support community engagement on issues under consideration.



ICANN Community Structures

- Supporting Organizations



- Stakeholder Groups
- Constituencies

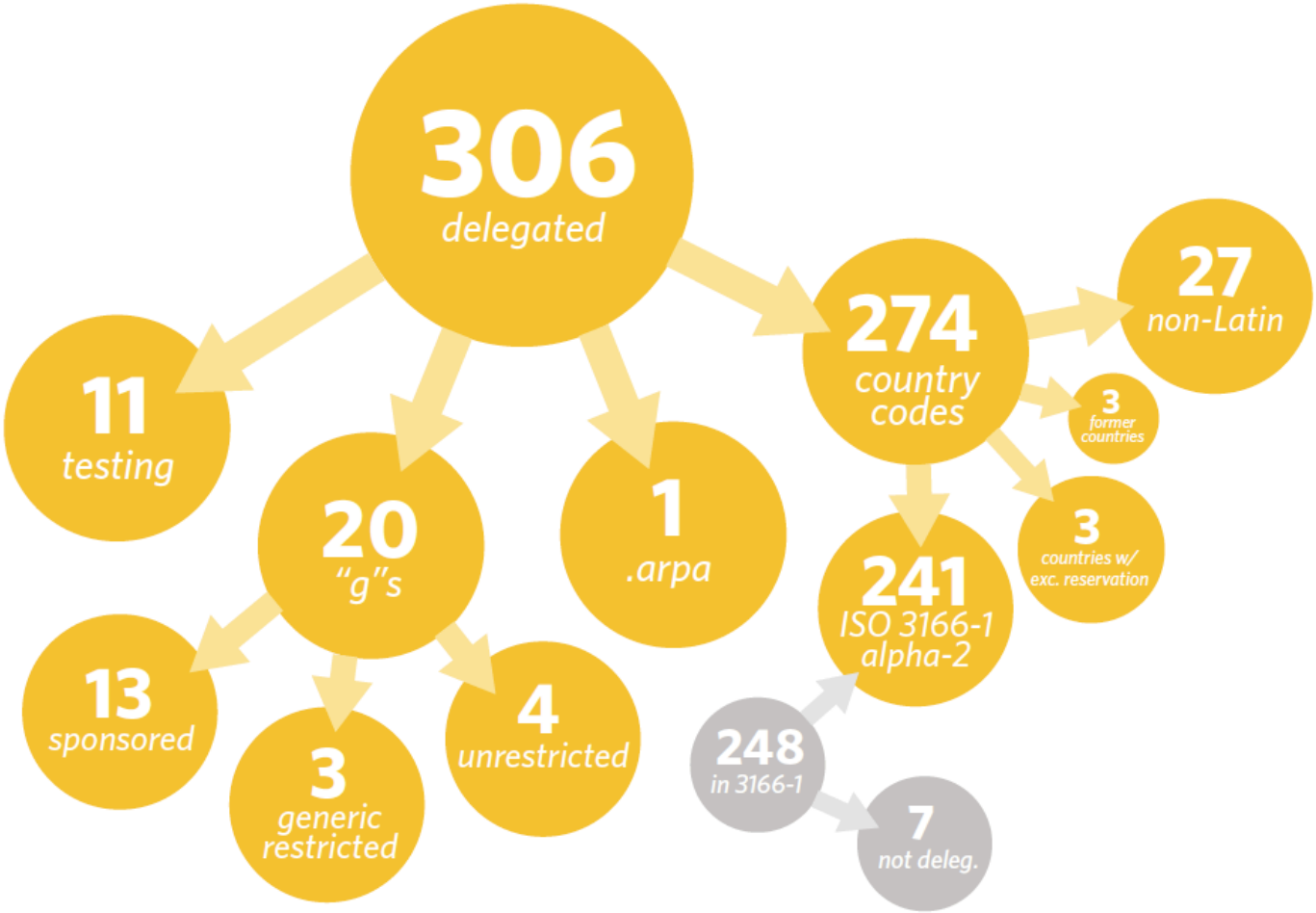
Agreements, Partnerships

- Affirmation of Commitments – US Department of Commerce
- IANA functions contract
- Internet Engineering Task Force MOU; Internet Architecture Board
- Number Resource Organization (NRO) MOU
- ccTLD Registry, Sponsorship, Accountability Frameworks and Exchange of Letters
- gTLD Registry Agreements
- Registrar Accreditation Agreements
- Escrow Agreements

Agreements, Partnerships

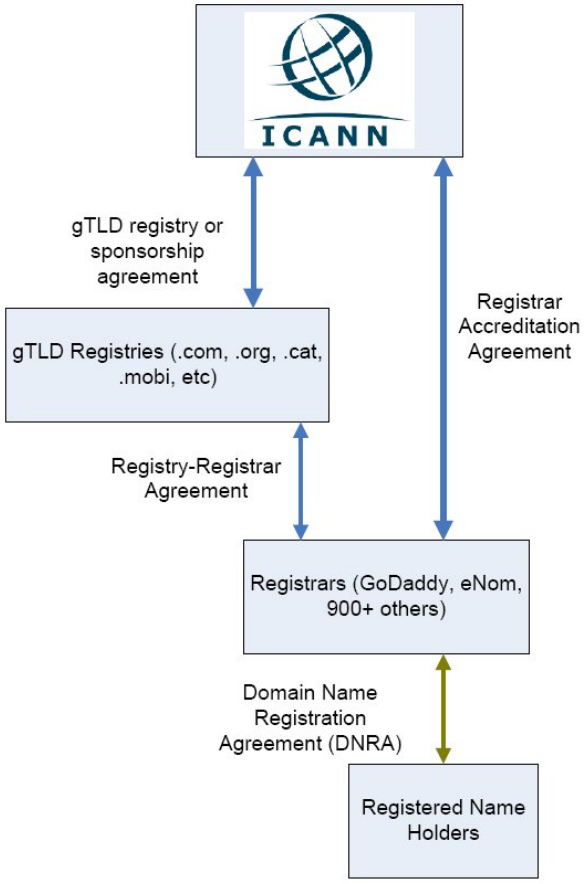
- UNESCO
- Russian Association of Networks and Services (RANS)
- Lomonosov Moscow State University Institute for Information Security Issues (IISI)
- Inter-American Telecommunications Commission of the Organization of American States (CITEL)
- African Telecommunications Union
- UN-ESCWA
- Commonwealth Telecommunications Organization
- Pacific Islands Telecommunications Association

Top-Level Domains (as of 14 Apr 2011)



Contracted Parties

Parties in the domain registration process must work together to ensure decisions made related to the global technical coordination of the DNS are made in the public interest and are accountable and transparent.



Non Contracted Partners

- Internet Society (ISOC)
- Network Startup Resource Center (NSRC)
- Regional TLD organizations (AfTLD, APTLD, LACTLD, CENTR)
- UN Group of Experts on Geographic Names (UNGEGN)
- International Telecommunication Union (ITU), World Wide Web Consortium (W3C), European Telecommunications Standards Institute (ETSI)
- Domain Name Dispute Resolution Providers
  - Asian Domain Name Dispute Resolution Centre
  - Czech Arbitration Court
  - World Intellectual Property Organization
  - National Arbitration Forum

Non Contracted Partners

- Regional Internet Registries (AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC)
- International Organization for Standardization (ISO)
- Network Operator Groups
- DNS-OARC
- ENISA
- Internet Governance Forum
- Forum for Incident Response and Security Teams (FIRST)

Others in the Ecosystem

- IT Sector Coordinating Council
- Anti Phishing Working Group
- Messaging Anti Abuse Working Group
- Security Trusted Communities
- Computer Emergency Response Teams
- Research & Academic institutions
- Law enforcement entities

Note – this list is representative and not intended to cover the full field of ecosystem participants

ICANN Organization/Staff

- Executive
- Human Resources/Administrative/ Finance
- Legal and Compliance
- Global Partnerships/Government Affairs
- Security
- IANA, DNS Operations (includes L-root) and IT
- Communications, Marketing, Meetings
- Policy Development
- Stakeholder Relations

Components of a New Framework

- Foundational Section – Mission, Core Values, Affirmation
- Ecosystem and ICANN's role
- Annual Update – Fiscal Year Module
  - Community Work
  - Strategic Projects
  - Organizational/Staff Program Areas

Security, Stability & Resiliency

FY 12 Operational Module

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
- IPv6 rollout; IPv4 exhaustion risk management
- Resource Public Key Infrastructure (RPKI) deployment
- 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)

SSR Major Components

- IANA
- DNS Operations & L-root
- DNS SSR Collaboration
- gTLD Services
- IDN Program
- Global SSR Engagement
- Measurement, Metrics
- Corporate Security programs
- Continuity program
- Policy development support
- SSAC/RSSAC support
- DNS-OARC contribution
- RIPE Labs ATLAS sponsorship
- Fellowship program
- Compliance

Affirmation of Commitments SSR Areas, Section 9.2

- SSR matters, both physical and network, relating to secure and stable coordination of the DNS
- Ensuring appropriate contingency planning
- Maintaining Clear Processes

Affirmation of Commitments SSR Areas, Section 9.2 Reviews will assess

- The extent to which ICANN has successfully implemented its SSR plan
- The effectiveness of the plan to deal with actual and potential challenges and threats
- The extent to which the SSR plan is sufficiently robust to meet future challenges and threats to the security, stability and resiliency of the Internet DNS

SSR Work

- DNSSEC management, support for greater adoption, periodic key rollover
- Automation of root zone management process
- RPKI implementation with stakeholders
- Stable introduction of IDN ccTLDs and new gTLD process
- Secure & resilient L-root operations
- Improved contractual compliance and registration data accuracy
- Support of risk management framework and analysis for the DNS

SSR Work

- Enhancements to the Registrar Accreditation Agreement
- Contractual compliance (addition of 3+ staff to support activities)
- SSAC and RSSAC activities
- Improvement of relations and engagement with law enforcement
- Collaborative response to malicious abuse of the unique identifier system
- Policy development – such as Registration Abuse Working Group

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

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

- TLD failure
- Social engineering attacks
- Denial of Service attacks
- Route hijacking
- Disasters
- Certificate authority compromise
- Authentication compromise
- IDN implementation and application acceptance, variant issues, IDN tables
- Government interventions

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

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

SSR in the New gTLD Process

- Evaluation Criteria for Applicants
- Best Practices for Registries in the new gTLD Agreement
- Registry Transition Processes to ensure continuity & minimize harm to registrants and users
- Mitigating Malicious Conduct
- Updated data escrow specification
- Pre-delegation checks
- Continued root zone monitoring

SSR in the New gTLD Process

- Mitigating Malicious Conduct
  - Vetted Registry Operators
  - Demonstrated plan for DNSSEC deployment
  - Prohibition of wildcarding
  - Removal of Orphan Glue Records
  - Requirement for thick WHOIS records
  - Centralized zone file access
  - Documented abuse contacts and procedures
  - Expedited registry security request process
  - High Security Zone Verification program

FY 12 Resourcing

- Note – Detail on SSR resourcing in FY 12 ICANN Budget in process of finalization, figures to be added

One World

One Internet

More Information: icann.org/en/security