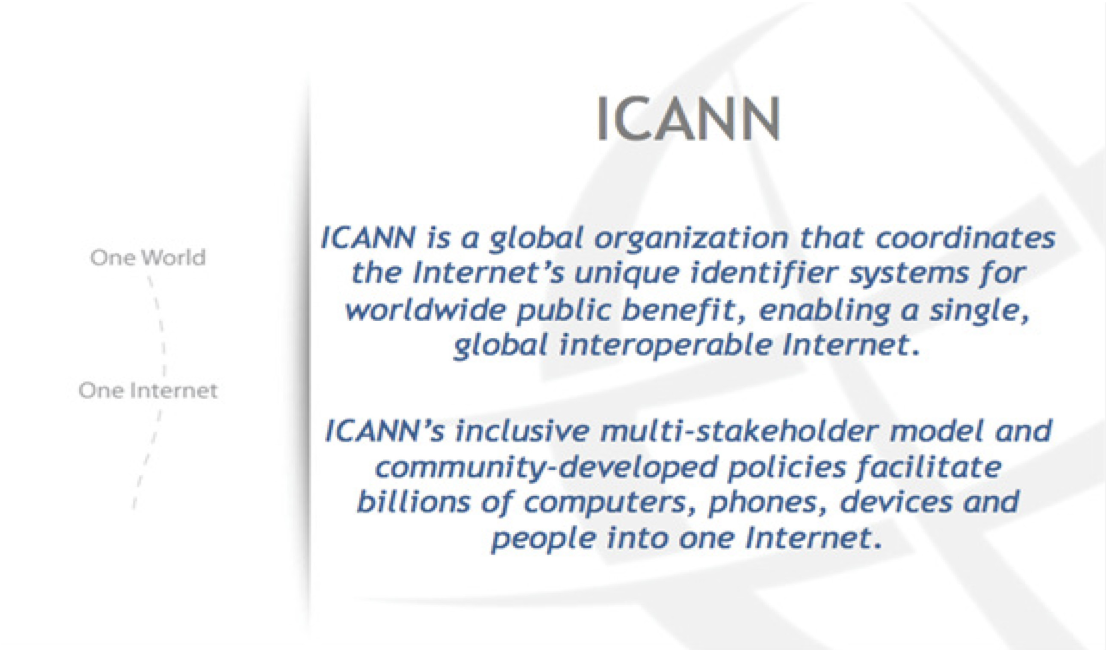
FY 12 Security, Stability, and Resiliency Framework

ICANN

May 2011

Table of Contents



One World

One Internet

ICANN

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

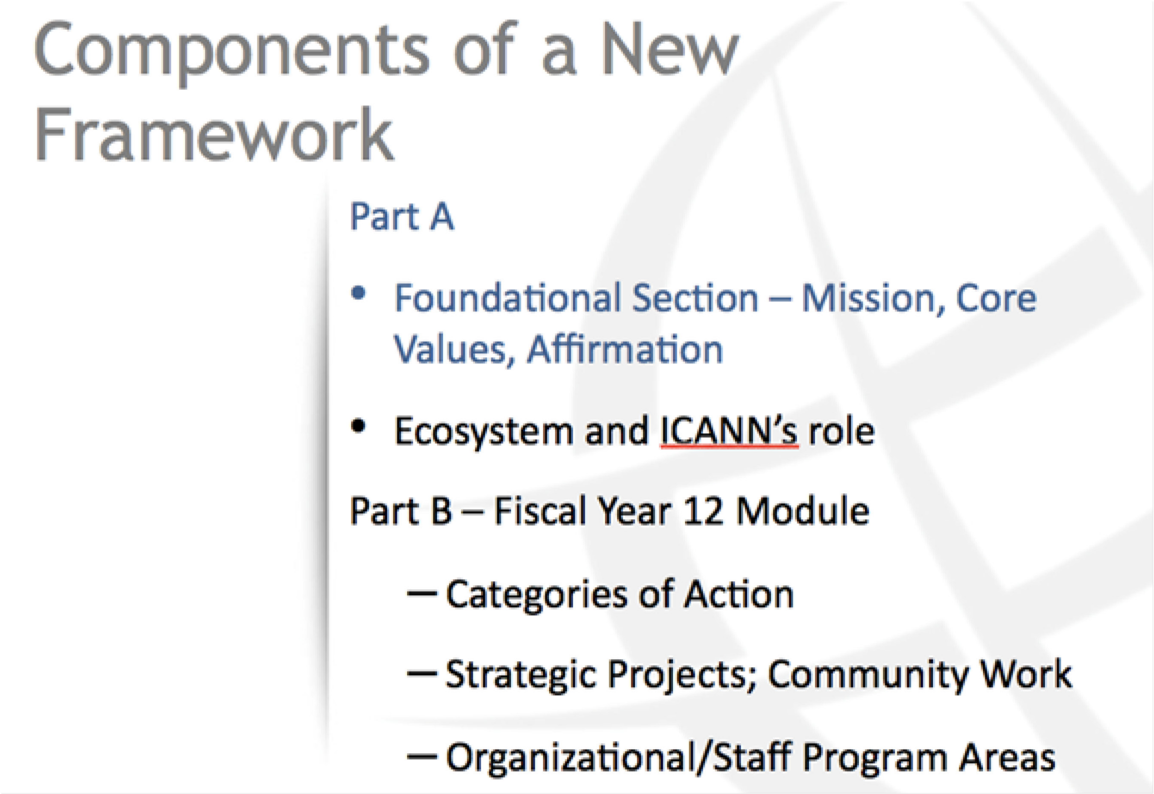
The Internet has thrived as an ecosystem engaging many stakeholders organizing through collaboration to foster communication, creativity and commerce in a global commons. The interoperability of the global commons depends on the operation and coordination of the Internet's unique identifier systems.[1]

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.

The ICANN Security, Stability and Resiliency (SSR) Framework describes ICANN's role and boundaries to a wide range of stakeholders on how ICANN will contribute to global efforts in addressing security, stability and resiliency as challenges for the Internet. The Framework provides an overview of the ecosystem, ICANN community and organizational structure, strategic objectives and planned activities through the FY 12 operational year (July 2011-June 2012).

The Framework builds on ICANN's two previous SSR Plans, published in May 2009 and September 2010, utilizes a more streamlined format over the previous Plans, while providing a clear overview of ICANN's priorities in SSR for the next year.

[1] According to the ICANN bylaws, ICANN coordinates the allocation and assignment of the three sets of unique identifiers for the Internet: the domain names (forming a system referred to as DNS); the Internet Protocol (IP) addresses and Autonomous System (AS) numbers; and the protocol port and parameter numbers.



Components of a New Framework

Part A

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

Part B – Fiscal Year 12 Module

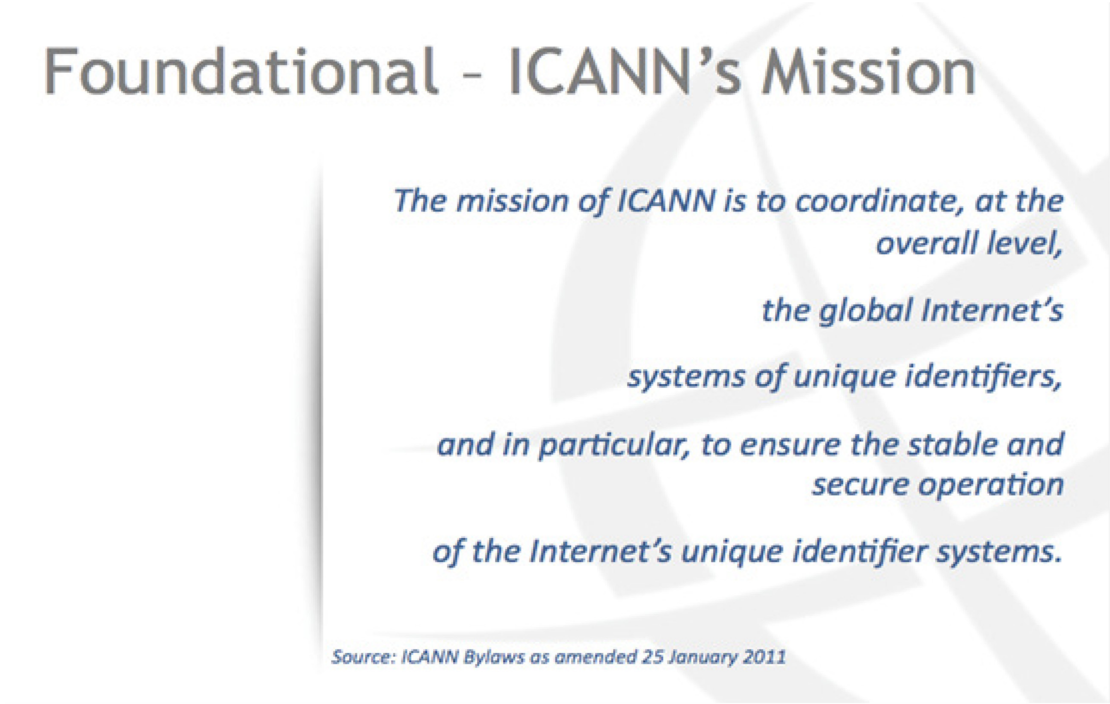
- Categories of Action
- Strategic Projects; Community Work
- Organizational/Staff Program Areas

Part A - Foundational

This section describes the foundation for ICANN's mission, core values related to SSR, and the mandate set in the Affirmation of Commitments. The remainder of the document details the ecosystem and ICANN's role, the community and ICANN organizational structure. Part B is the module for FY 12 and describes ICANN's operational priorities in SSR, areas of collaboration and areas of awareness of activity by others in the ecosystem.

The information in this section is a new addition to the FY 12 Framework and is intended to provide context for the SSR Framework and ICANN's contributions to a secure and stable unique identifier system.

For reference, see ICANN Bylaws – Mission & Core Values: http://www.icann.org/en/general/bylaws.htm#I.



Foundational – ICANN's Mission

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

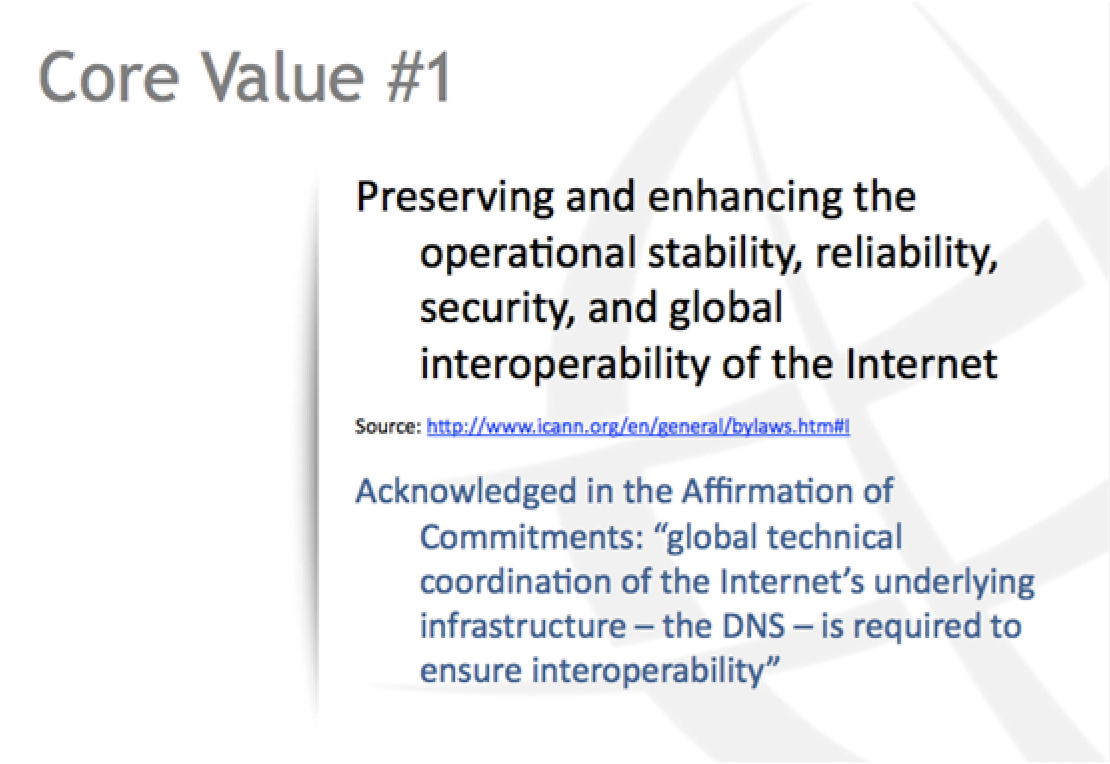
the global Internet's

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 and Resiliency

As described in this Framework, security, stability and resiliency are referenced using the following basic definitions.

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[2]

Note – These definitions are based on general use from the 2009, 2010 SSR Plans.

The 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. According to a July 2010 report by the US Government Accountability Office, "the global interconnectivity provided by the Internet allows cyber attackers to easily cross national borders, access vast numbers of victims at the same time, and easily maintain anonymity."[3]
As the frequency and sophistication of disruptive attacks and other malicious behaviour increases, ICANN and the greater community must continue to collaborate toward improving the resilience of the unique identifier systems and strengthen its capabilities.

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.

[2] There are other definitions for these terms in other ICANN contexts, such as gTLD registry agreements. ICANN is also participating efforts such as ENISA's Resilience Metrics program. A general definition for resilience used by ENISA is "the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation" – see Resilience Metrics and Measurement Technical Report, February 2011, http://www.enisa.europa.eu/act/res/other-areas/metrics/reports/metrics-tech-report, page 12.

[3] US Government Accountability Office, GAO-10-606-Cyber, Cyberspace, United States Faces Challenges in Addressing Global Cybersecurity and Governance, www.gao.gov/products/GAO-10-606.

Routing hijacks, address registration and ASN hijacks continue to grow. Denial of Service attacks disrupts users of all types. Botnets enable malicious activity such as fraud, phishing and malware, viruses, and worms.

Affirmation of Commitments

The Affirmation of Commitments signed by ICANN and the US Department of Commerce on 30 September 2009 (http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm) recognized that a key commitment includes preserving the security, stability and resiliency of the DNS (Section 3b).

The Affirmation acknowledges in Section 9.2 that ICANN has adopted a Security, Stability and Resiliency (SSR) Plan, which will be regularly updated to reflect emerging threats to the DNS (including unique identifiers). This Plan will be reviewed no less than every three years.

Previous SSR Plans were published in May 2009 and September 2010. The 2009 Plan, which covered FY 10 (https://www.icann.org/en/topics/ssr/ssr-draft-plan-16may09-en.pdf), was acknowledged by the ICANN Board at its meeting in Sydney, Australia in June 2009 (http://www.icann.org/en/minutes/resolutions-26jun09.htm#1.7).

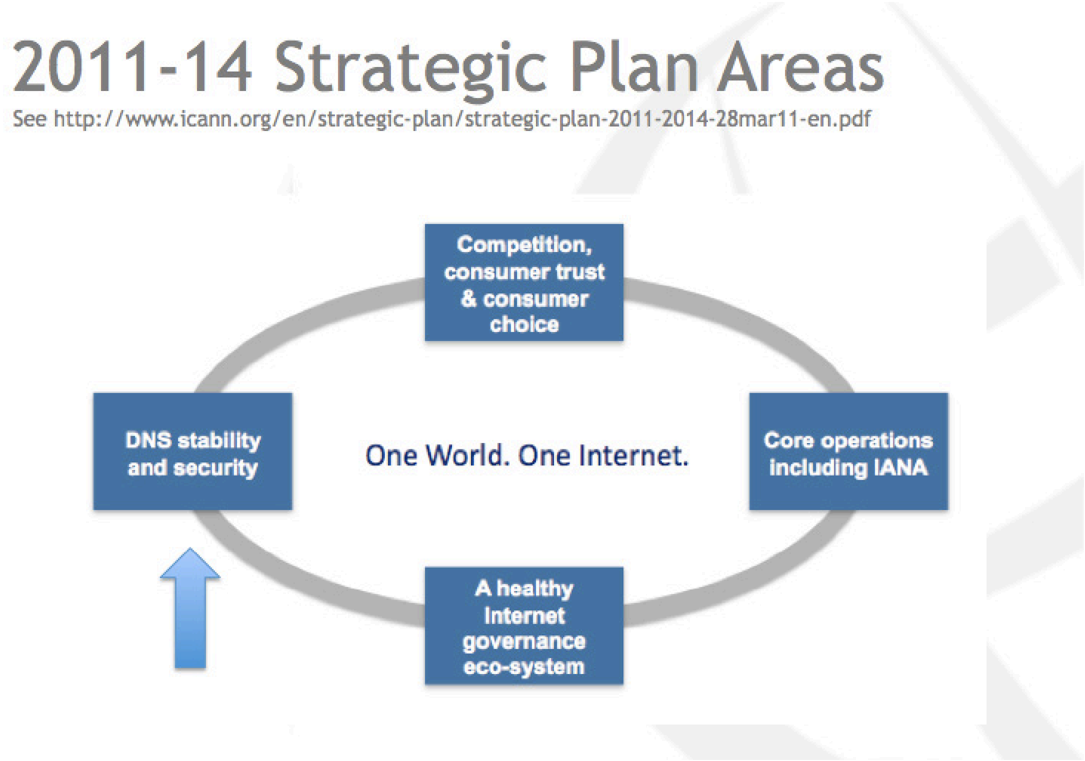
The 2010 Plan, which covered FY 11 (https://www.icann.org/en/topics/ssr/ssr-plan-fy11-clean-23nov10-en.pdf), was acknowledged by the ICANN Board at its meeting in Cartagena, Colombia in December 2010 (http://www.icann.org/en/minutes/resolutions-10dec10-en.htm#1.8).

The first SSR Review Team was announced in September 2010 and commenced its work at the ICANN meeting in Cartagena in December 2010. Information on the SSR Review Team is available at http://www.icann.org/en/reviews/affirmation/review-2-en.htm.

Particular attention in the review will focus on

- SSR matters, both physical and network, relating to secure and stable coordination of the DNS
- ICANN's efforts at ensuring appropriate contingency planning, and
- Maintaining clear processes.

The Review team 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; and 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.



2011-14 Strategic Plan Areas

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

Competition, consumer trust & consumer choice

DNS stability and security

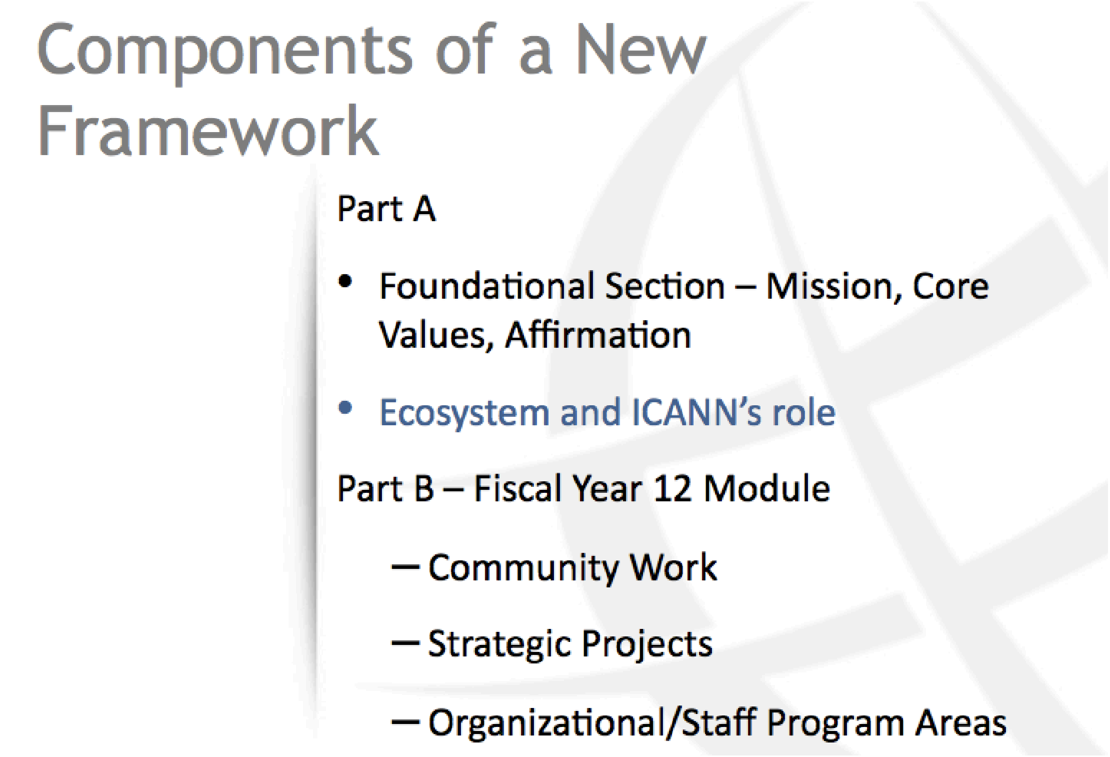
One World. One Internet.

Core operations including IANA

A healthy Internet governance eco-system

ICANN's 2011-2014 Strategic Plan (http://www.icann.org/en/strategic-plan/strategic-plan-2011-2014-28mar11-en.pdf) identifies DNS stability and security as one of ICANN's four key strategic focus areas. This aligns with the high importance given to SSR in the Affirmation of Commitments. The Strategic Plan separates the broad range of ICANN's security, stability and resiliency responsibilities into strategic objectives, community work, strategic projects and staff work.

The activities that fall into these four areas will be described in greater detail in Part B, the FY 12 module to the Framework.



Components of a New Framework

Part A

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

Part B – Fiscal Year 12 Module

– Community Work

– Strategic Projects

– Organizational/Staff Program Areas

The Ecosystem and 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 economic progress, government operations and global security activities, the profile of Internet governance has also elevated.

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.

ICANN recognizes that there is a distinction between areas in which ICANN has a limited operational role, areas in which ICANN serves as a collaborator and coordinating role, and areas in which ICANN has awareness or an observational 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.

ICANN is not

- A law enforcement agency
- A court of law
- A government agency

ICANN cannot unilaterally suspend domain names, transfer domain names or immediately terminate a registrar's contract (except under limited circumstances)

ICANN is able to enforce its contracts on registries and registrars. ICANN will address risks to Internet security, stability and resiliency within the boundaries of its responsibilities.

Examples of ICANN SSR Activities in the Ecosystem

Since ICANN's formation in 1999, ICANN has served as an organizer, collaborator, facilitator and observer in security, stability and resiliency of the Internet's unique identifiers. This section describes some examples of ICANN's role in SSR.

In November 2001, ICANN devoted an entire international public meeting on security and stability of the Internet naming and address allocation system (see http://www.icann.org/en/committees/security/sac002.htm, http://www.icann.org/en/meetings/mdr2001/schedule.htm#agenda)

In 2002, the Security and Stability Advisory Committee was formed, and it continues to play a key role for ICANN and the greater Internet community today (see http://icann.org/en/committees/security). SSAC produces substantial documents, not only as advice to the ICANN Board, but also on areas of interest for the greater community.

ICANN has supported the efforts of the ccTLD community to host technical days at ICANN meetings since 2006. The ccNSO tech day program has grown into a key information-sharing feature of ICANN meetings and included participation from DNS-OARC at the ICANN meeting in San Francisco in March 2011.

ICANN has enhanced protections for registrants through the implementation of gTLD registrar data escrow in February 2008 (99.4% of all ICANN-accredited registrars are now depositing into escrow). A new Registrar Accreditation Agreement was adopted in May 2009, and ICANN is continuing to enhance its Contractual Compliance program.

ICANN has a contingency exercise program and has conducted annual exercises since 2008. The continuity and contingency exercise program began as part of ICANN's work on protections for registrants and the gTLD registry failover plan. The exercise program has grown to include joint exercises with gTLD registries (with Afilias, Neustar and VeriSign in 2009), on IANA and crisis communications (January 2010), root server operators (July 2010) and L-root operations (February 2011). ICANN has also participated in international cyber exercises over the last four years.

ICANN's support of the Conficker Working Group is described in https://www.icann.org/en/security/conficker-summary-review-07may10-en.pdf.

ICANN has supported two Global symposia on SSR, the first at Georgia Tech University in February 2009 (http://www.gtisc.gatech.edu/pdf/DNS_SSR_Symposium_Summary_Report.pdf), followed by a second symposium at Kyoto University in Japan in February 2010 (https://www.icann.org/en/topics/ssr/dns-ssr-symposium-report-1-3feb10-en.pdf).

Another example of efforts at supporting overall SSR enhancement for Internet and its unique identifiers has been the work conducted with the community to support signing of the root zone with Domain Name Security Extensions (DNSSEC) in 2010 with partners Verisign and NTIA. The implementation of DNSSEC in the root zone was a significant milestone in FY 11.

A limited, but growing number of Internationalized Domain Names have been entered into the root zone, initially covering test strings in eleven scripts, followed by IDNs requested by countries and territories through the IDN ccTLD Fast Track. ICANN has worked with linguistic and technical experts to ensure that requested strings satisfy the technical and confusability requirements in the Fast Track process. A secure and stable introduction of IDNs has been critical to meet the demands of Internet users in local communities whose language is rendered in a non-Latin script.

Responsibilities

ICANN is responsible for the 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.

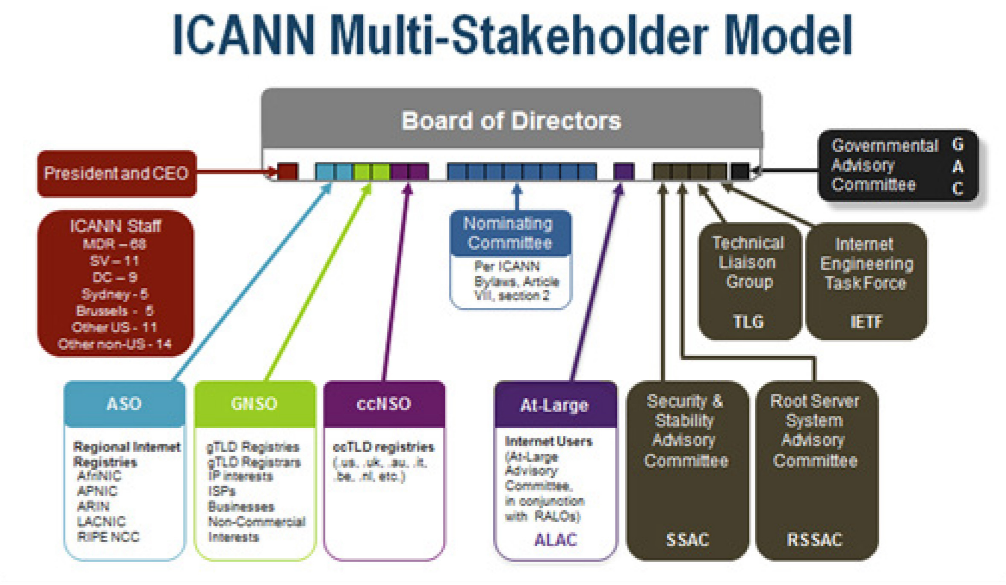
ICANN is an enabler and facilitator of the SSR activities conducted by DNS registries, registrars and other members of the community. Other key efforts focus on improving system-wide understanding of risks, enabling a Trust Anchor (TA) model implementation of Resource Public Key Infrastructure (RPKI), and cooperating with partners to enhance the security and resiliency practices of the TLD community.

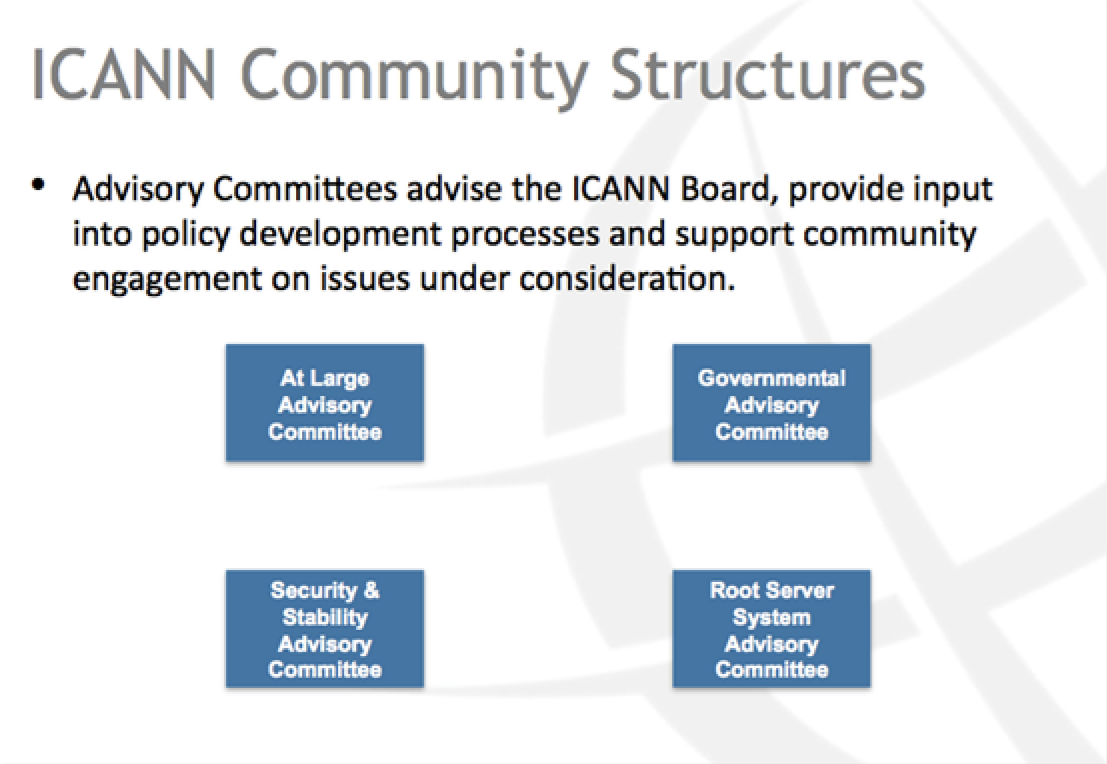
ICANN is responsible for the secure, stable and resilient operation of its own assets and services.

- ICANN maintains an internal Computer Incident Response Team, https://www.icann.org/en/cirt/, and has joined the Forum for Incident Response and Security Teams (FIRST)
- ICANN supports annual updating of its security plans and effective security controls and procedures
- ICANN ensures that internal staff have strong skills, appropriate tools and are current with security threats and best practices
- This work includes stable, continuous L-root operations and DNSSEC key management

Ecosystem Participants

Participants in the greater ecosystem include members of the technical community, registration infrastructure providers, governments and non-governmental organizations, businesses, the non-commercial and academic community, users and the At Large community, and law enforcement/operational security community.

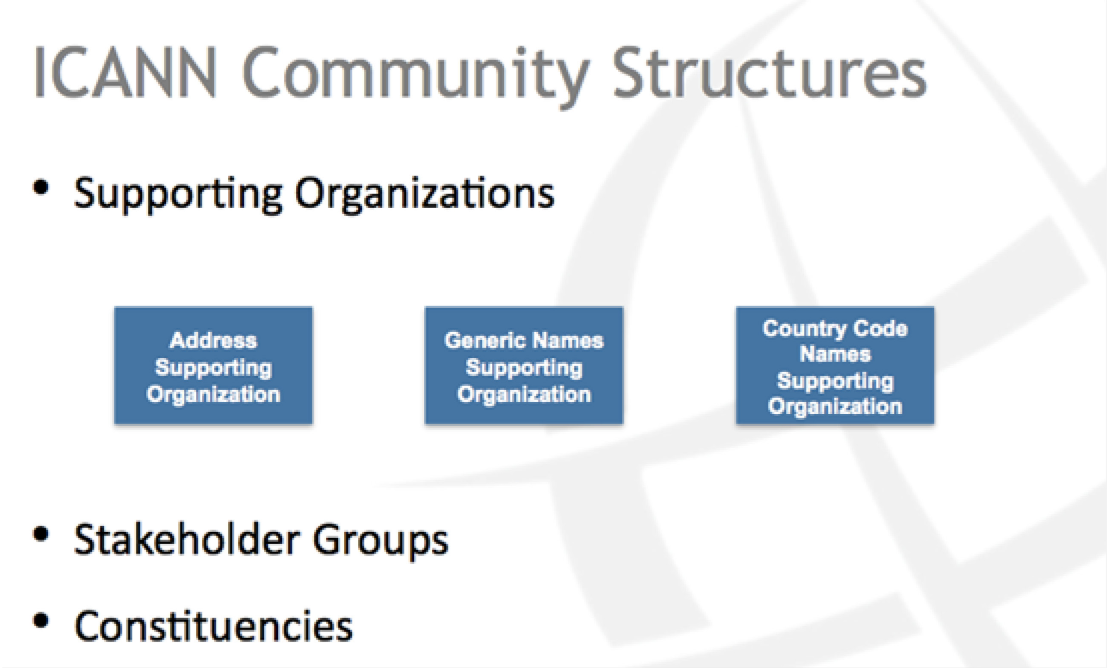




ICANN Community Structures

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

At Large Advisory Committee
Governmental Advisory Committee
Security & Stability Advisory Committee
Root Server System Advisory Committee



ICANN Community Structures

- Supporting Organizations

Address Supporting Organization
Generic Names Supporting Organization
Country Code Names Supporting Organization

- Stakeholder Groups
- Constituencies

ICANN supporting organizations, stakeholder groups and constituencies are key participants in broader forums and activities whose purposes range from improving resiliency in the face of disruptive attacks to collaborative efforts focused on combating malicious Internet

Agreements, Partnerships

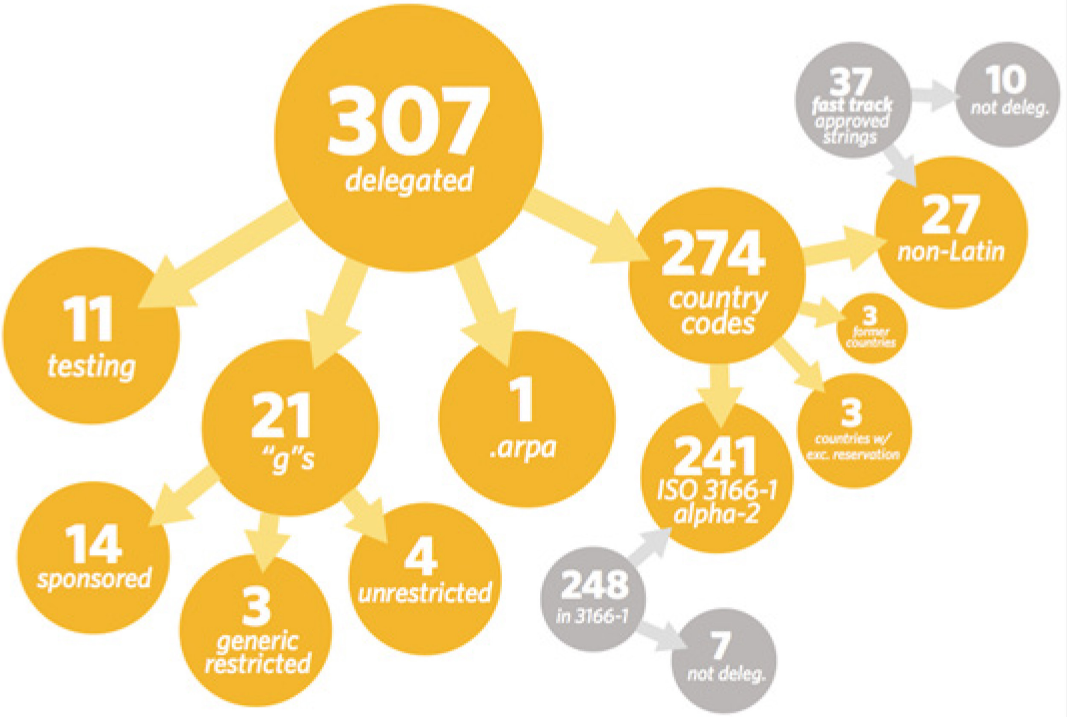
ICANN has formal agreements and partnerships with a broad range of institutions. These include:

- Affirmation of Commitments with the US Department of Commerce
- IANA functions contract with the National Telecommunications and Information Administration (NTIA)
- Internet Engineering Task Force (IETF) Memorandum of Understanding
- Internet Architecture Board (IAB) Memorandum of Understanding
- Number Resource Organization (NRO) Memorandum of Understanding
- ccTLD registry sponsorship agreements, Accountability Frameworks and Exchange of Letters
- gTLD Registry Agreements
- Registrar Accreditation Agreements
- Registration Data Escrow Agreements

Partnership Agreements include:

- United Nations Educational, Scientific and Cultural Organization (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
- United Nations Economic and Social Commission for Western Asia (UNESCWA)
- Commonwealth Telecommunications Organization
- Pacific Islands Telecommunications Association

Top-Level Domains

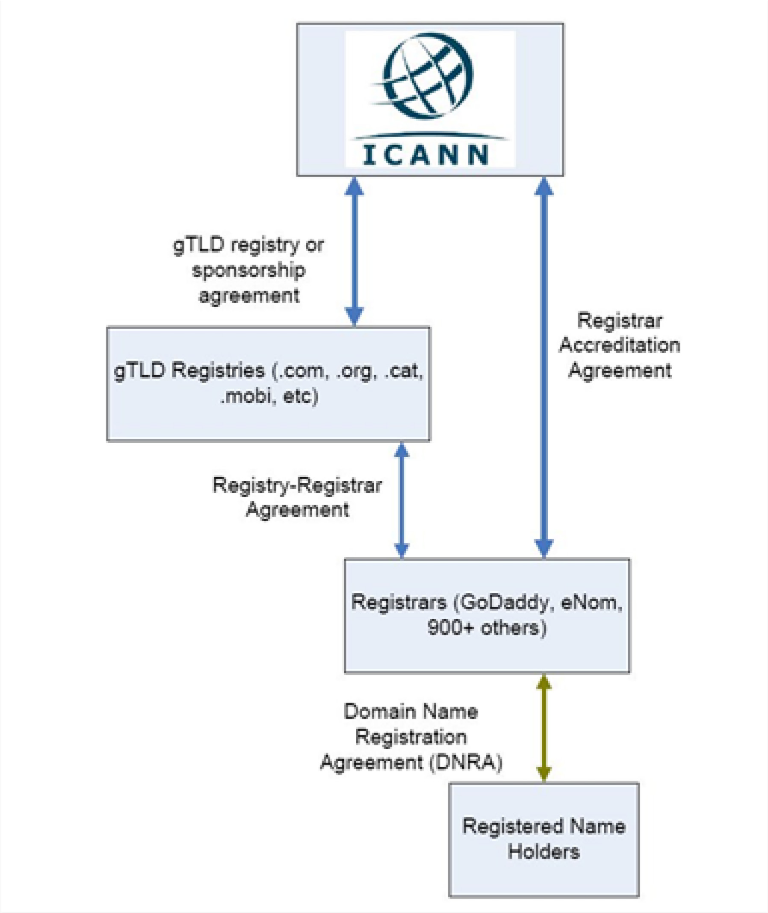


This image shows the composition of gTLD and ccTLD registries as of 19 April 2011 [Image credit – Kim Davies]

Contracted Parties

Parties in the domain name 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.

The image below describes the parties in the domain registration process and their relationships.


ICANN
gTLD registry or sponsorship agreement
Registrar Accreditation Agreement
gTLD Registries (.com, .org, .cat, .mobi, etc)
Registry-Registrar Agreement
Registrars (GoDaddy, eNom, 900+ others)
Domain Name Registration Agreement (DNRA)
Registered Name Holders

Non-Contracted Partners in the Ecosystem

While preserving the stability of the unique identifier system, ICANN recognizes the authority and participation of different actors with different remits such as law enforcement, regional TLD organizations, dispute resolutions providers, among others. In order to achieve its goals, ICANN will participate in constructive international fora, collaborate with international organizations such as the European Commission and OECD on standards and best practices, engage in offline discussions, write papers, and otherwise engage with industry participants.

The following is a non-exhaustive list of non-contracted partners in the ecosystem.

- Internet Society
- Network Startup Resource Center (NSRC)
- Regional TLD organizations – AfTLD, APTLD, CENTR, LACTLD
- Regional Internet Registries – AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC
- DNS-OARC
- Internet Governance Forum
- United Nations Group of Experts on Geographic Names (UNGEGN) (assisting in the IDN ccTLD Fast Track process)
- International Telecommunications Union (ITU), World Wide Web Consortium (W3C), European Telecommunications Standards Institute (ETSI)
- Domain Name Dispute Resolution Providers
    - Asian Domain Name Dispute Resolution Centre (ADNDRC)
    - Czech Arbitration Court (CAC)
    - National Arbitration Forum (NAF)
    - World Intellectual Property Organization (WIPO)
- International Organization for Standardization (ISO)
- Network Operator Groups
- ENISA
- Forum for Incident Response and Security Teams (FIRST)

Others in the Ecosystem

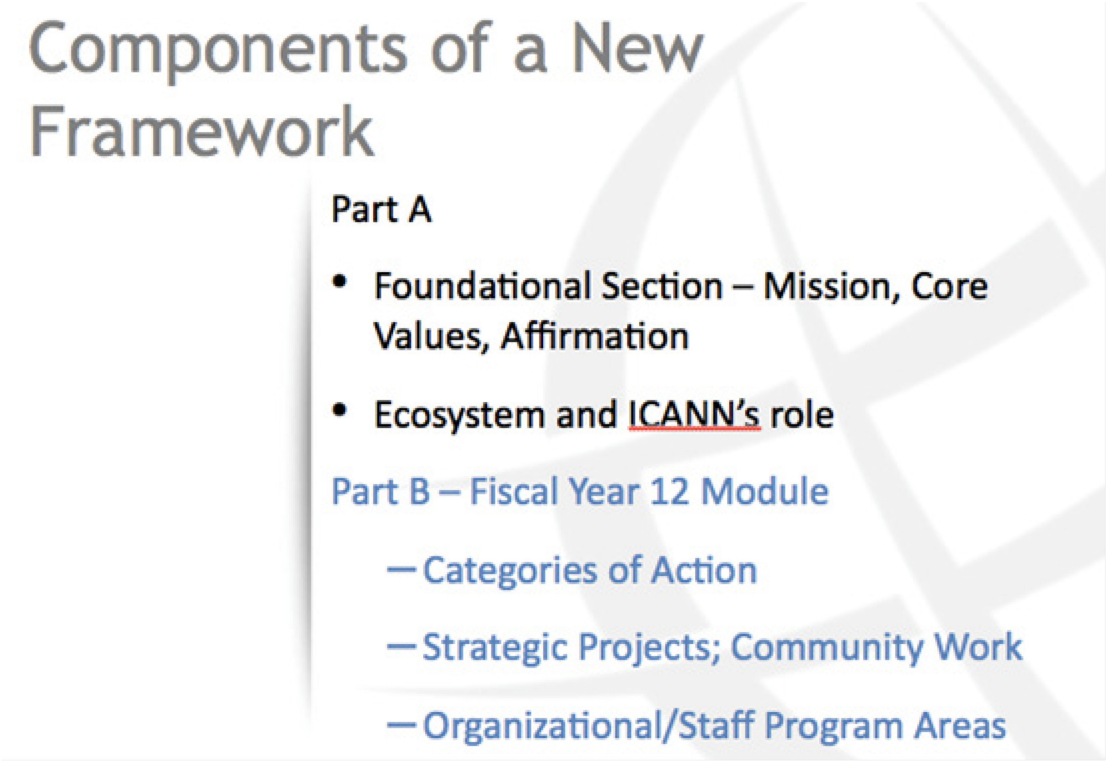
Other participants or forums in the ecosystem in which ICANN staff may be engaged, observing or participating as subject matter experts, or simply following for awareness. This list is representative and not intended to cover the full field of ecosystem participants.

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

ICANN Organization/Staff

Internally ICANN departments divide into the following areas to support ICANN's mission, strategic and operational priorities and community activities.

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



Components of a New Framework

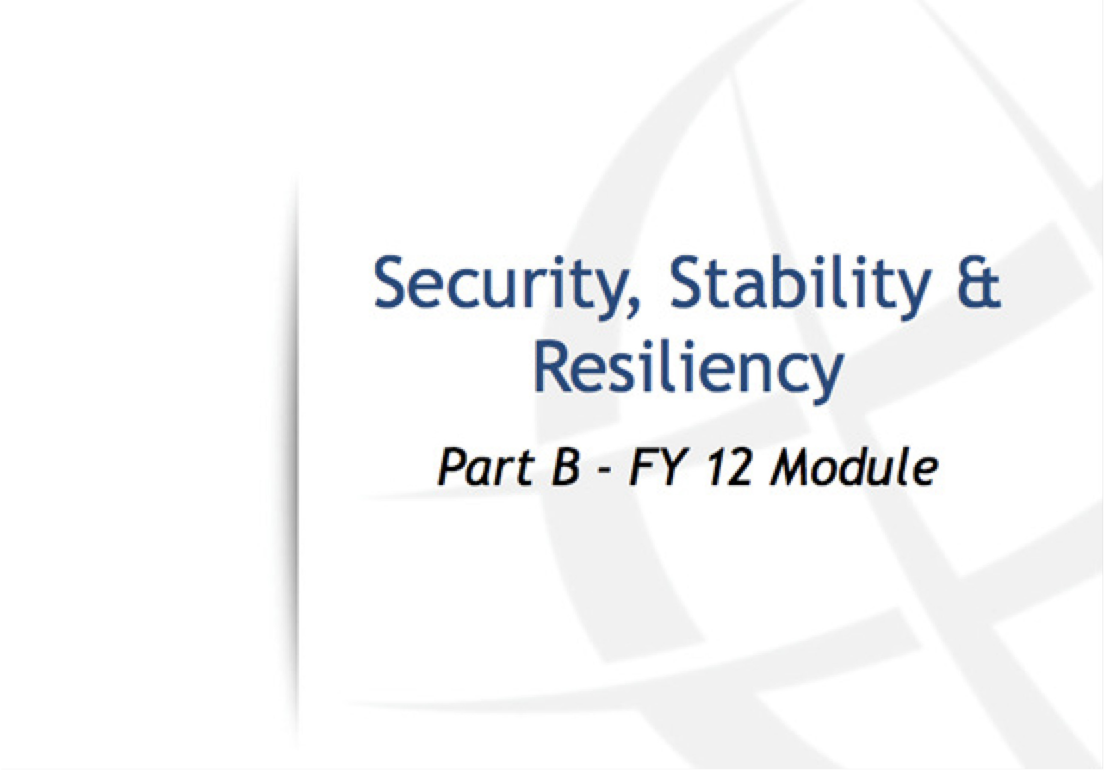
Part A

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

Part B – Fiscal Year 12 Module

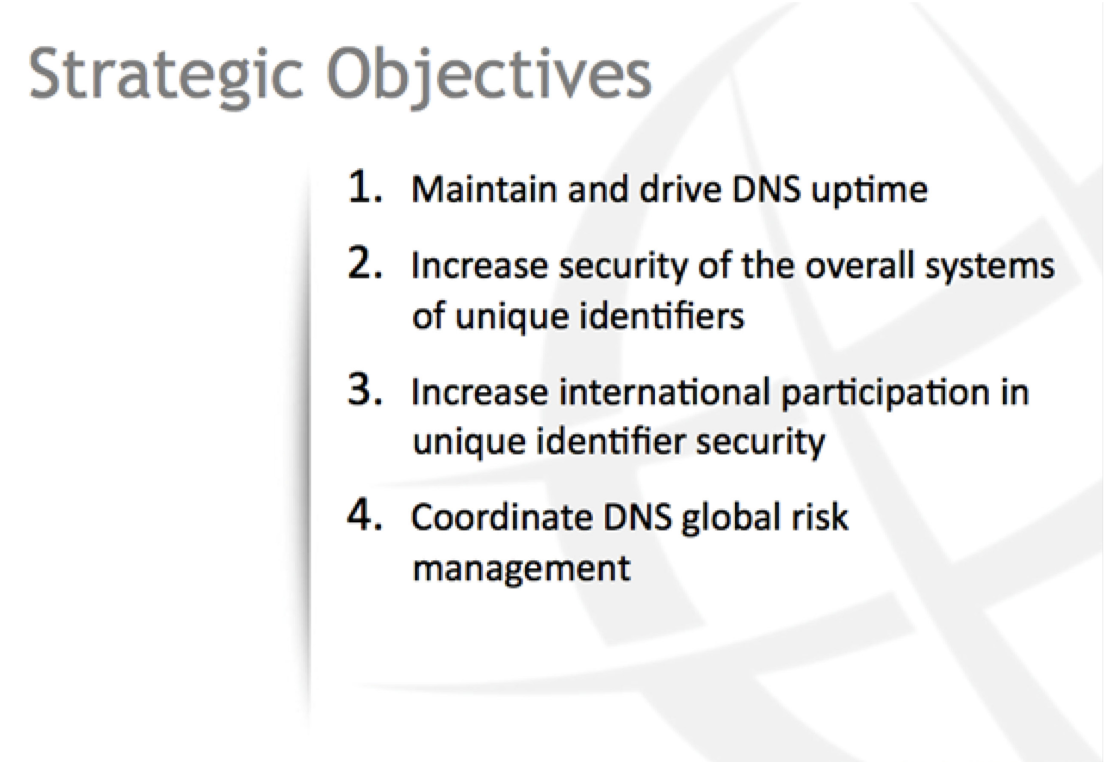
- —Categories of Action
- —Strategic Projects; Community Work
- —Organizational/Staff Program Areas

Part B – FY 12 Modual



Security, Stability & Resiliency

Part B - FY 12 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

The ICANN Board of Directors adopted the 2011-2014 Strategic Plan[4] at the ICANN meeting in San Francisco on 18 March 2011[5]. Ensuring security and stability of the Internet's unique identifier systems is one of the four main focus areas. The Strategic Plan represents a balancing of those areas in which ICANN has direct influence and operation with those areas in which ICANN is a facilitator, participant, and observer.

Within the security and stability focus area, four strategic objectives have been identified (see above).

Strategic activities are further divided into community work, organizational/staff work, and ICANN Security team core areas.

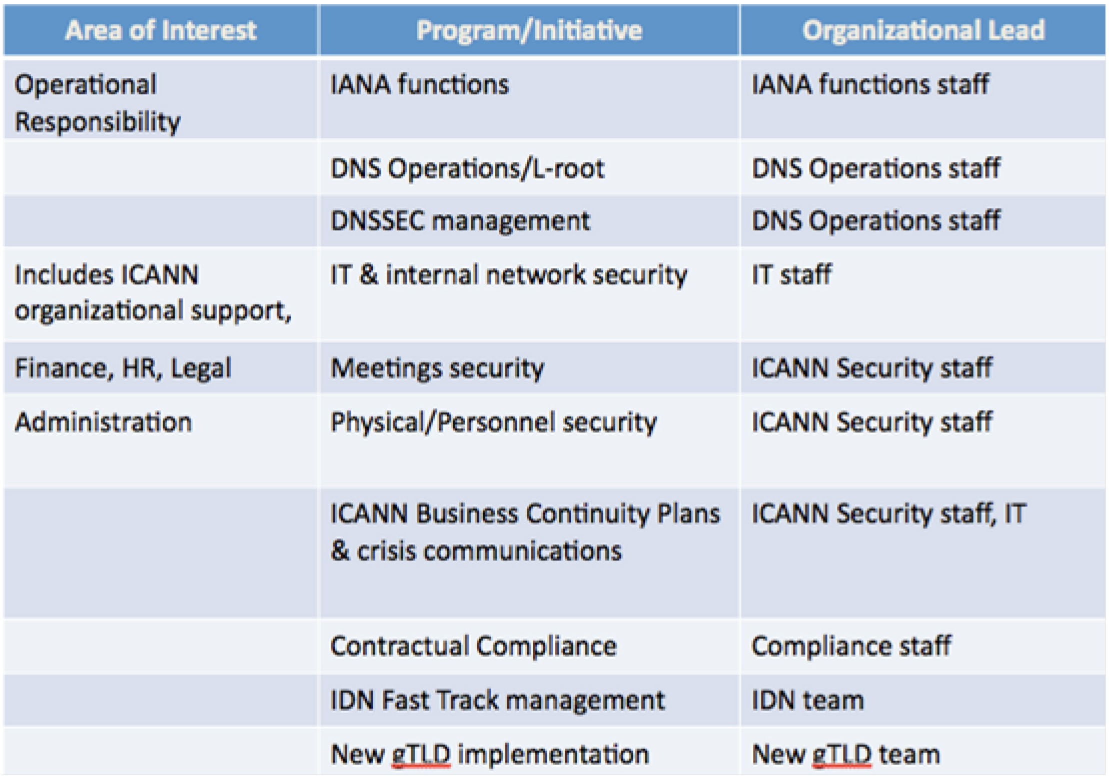
Matrix of Activities: Areas of ICANN Operation; Areas of ICANN Collaboration, Coordination; Areas of Awareness

ICANN's efforts in SSR can be divided into three areas –

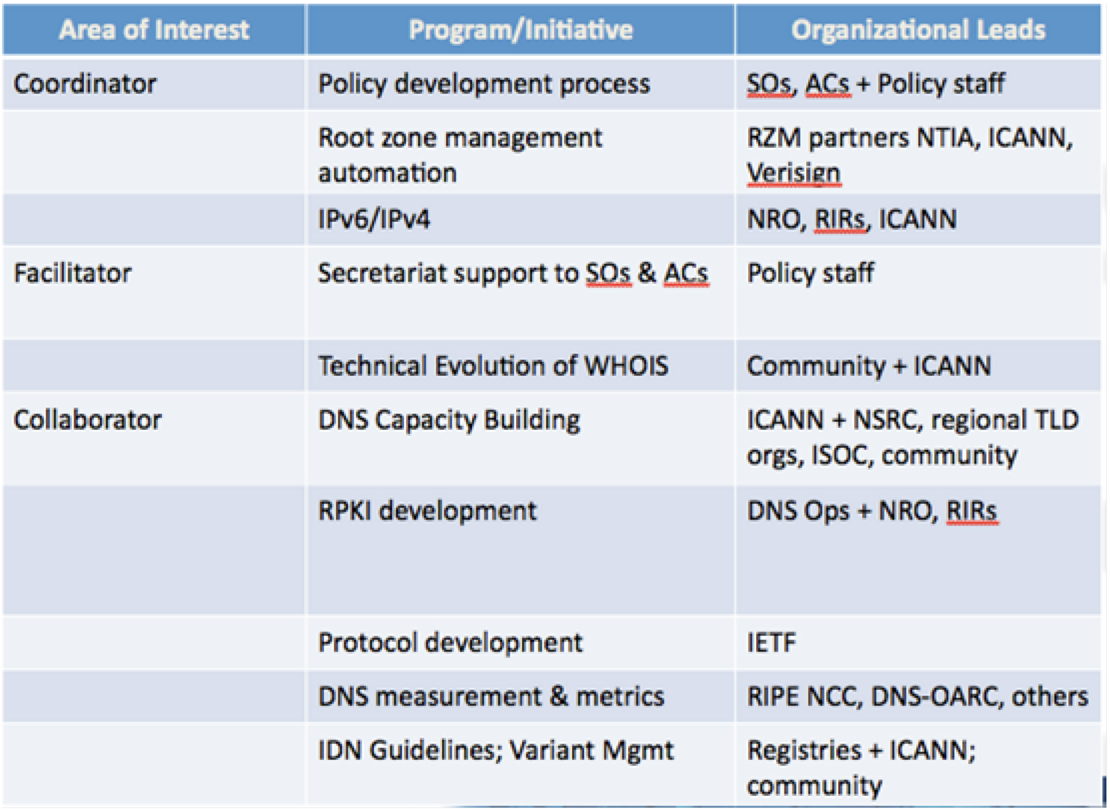
1. Areas where ICANN has operational responsibility,
2. Areas where ICANN is a collaborator, facilitator or coordinator
3. Areas where ICANN has awareness or an observer role, but others lead

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

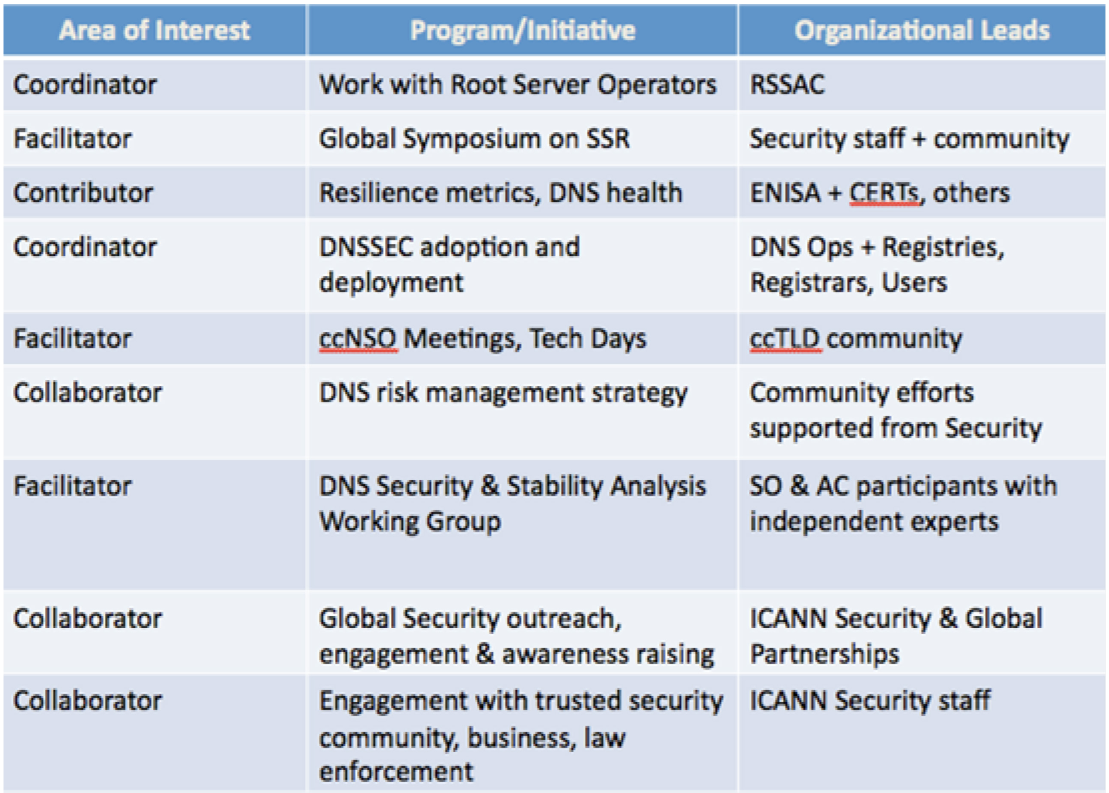
[5] http://www.icann.org/en/minutes/resolutions-18mar11-en.htm#2.



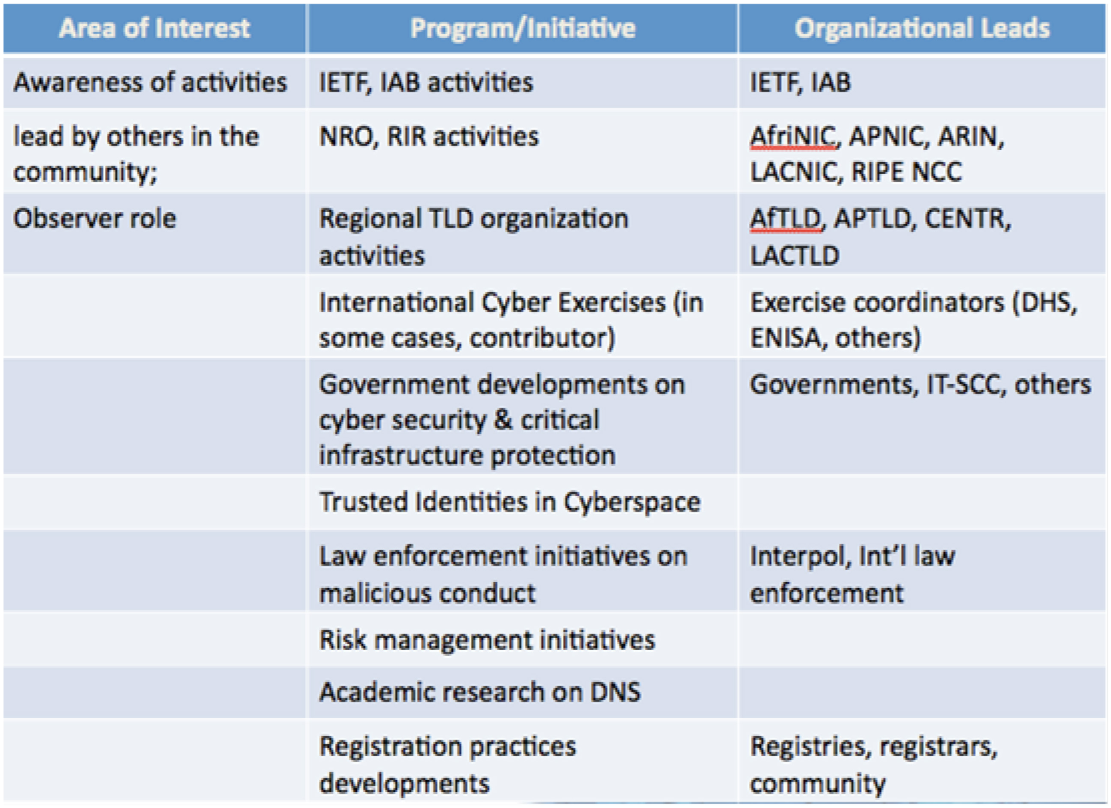
Area of Interest	Program/Initiative	Organizational Lead
Operational Responsibility	IANA functions	IANA functions staff
	DNS Operations/L-root	DNS Operations staff
	DNSSEC management	DNS Operations staff
Includes ICANN organizational support,	IT & internal network security	IT staff
Finance, HR, Legal	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



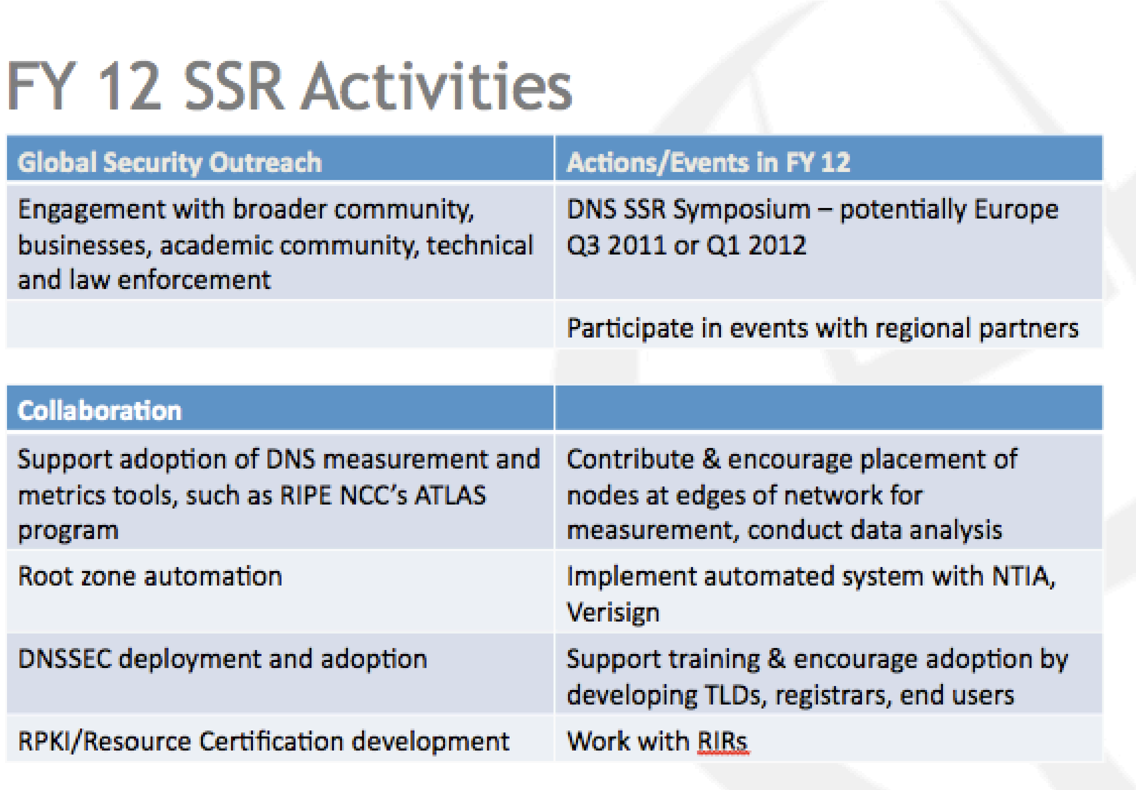
Area of Interest	Program/Initiative	Organizational Leads
Awareness of activities	IETF, IAB activities	IETF, IAB
lead by others in the community;	NRO, RIR activities	AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC
Observer role	Regional TLD organization activities	AfTLD, APTLD, CENTR, LACTLD
	International Cyber 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

Security Team Core Areas

ICANN’s Security team is a distributed team, with global reach and expertise in technical and policy issues impacting the Internet’s unique identifier systems. The team serves as a bridge between DNS operators, infrastructure providers, technical community, policy development, internally and externally. The team coordinates across the range of ICANN efforts to support ICANN’s mission of preserving and enhancing the operational stability, reliability & global interoperability of the Internet.

The Security team’s work can be divided into five main program areas:

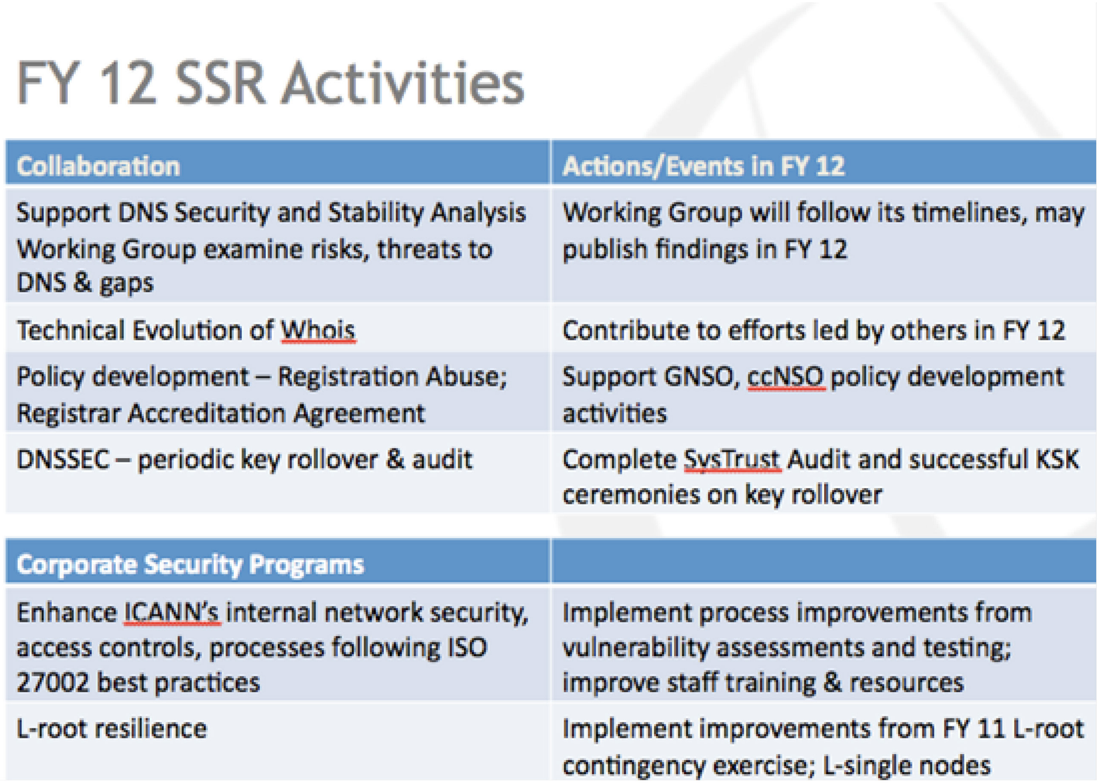
1. Global Security Engagement and Awareness
2. Security Collaboration
3. DNS Capacity Building
4. Corporate Security, Business Continuity, Risk Management
5. Cross-Organizational Support – this includes contributions as subject matter experts and support to new gTLD program, IDN ccTLD Fast Track, DNSSEC implementation & management, Policy development support, Compliance, Global Partnerships/Government Affairs support



FY 12 SSR Activities

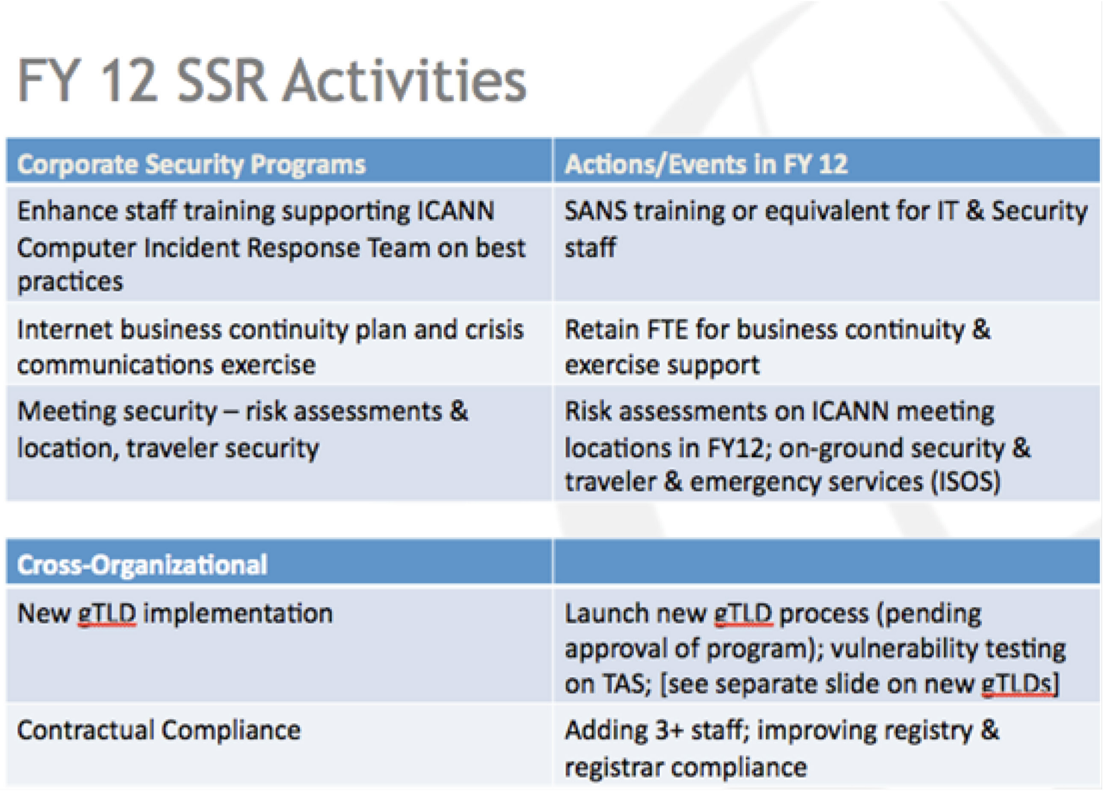
Global Security Outreach	Actions/Events in FY 12
Engagement with broader community, businesses, academic community, technical and law enforcement	DNS SSR Symposium – potentially Europe Q3 2011 or Q1 2012
	Participate in events with regional partners

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



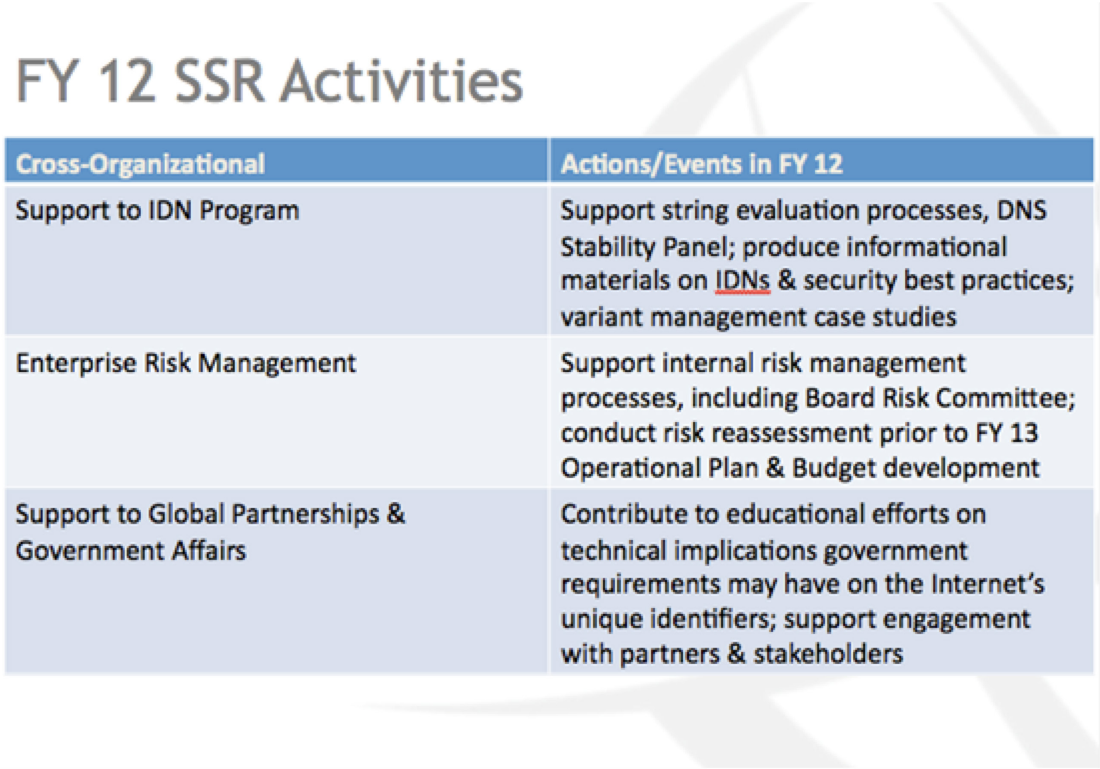
FY 12 SSR Activities

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

Tracking the Affirmation of Commitments: Continuity and Contingency Work

The Affirmation of Commitments identifies three areas of emphasis – continuity and contingency work, maintaining clear processes, focus on emerging threats and issues. On continuity and contingency work, ICANN has been quite active, supporting annual contingency exercises and participating in larger International exercises as a contributor or observer.

In FY 12, ICANN will continue to support a DNS Capacity Building with partners in the greater ecosystem. Over the life of the program, these efforts have focused on best practices, Attack and Contingency Response training for ccTLD managers, and Secure Registry Operations. The community has also expressed an interest in DNSSEC and IPv6 training. ICANN intends to continue working with partners in the regions that have expressed a need and interest in capacity building training and education. This includes contributing to events led by the regional TLD organizations (AfTLD, APTLD, CENTR and LACTLD).

Since 2008, ICANN has conducted annual contingency and continuity exercises. This has included an internal registry failover exercise, Joint ICANN-gTLD registry continuity exercise with Afilias, Neustar and Verisign in 2009, an IANA Continuity Exercise in 2010, an L-root contingency exercise in February 2011, root server operators communication exercises, internal communications exercises, IDN ccTLD Fast Track System Test and a registry data escrow exercise. ICANN will continue and expand its contingency exercises in FY 12, including vulnerability testing on internal processes and systems in conjunction with the new gTLD program.

Tracking the Affirmation of Commitments: Maintaining Clear Processes

Under the category of maintaining clear processes, ICANN supports on-going work such as the Registry Services Technical Evaluation Panel for the review of proposed registry services, and the string evaluation processes in the IDN ccTLD Fast Track (including the DNS Stability Panel). ICANN intends to further work on the implementation of the new gTLD process and technical evolution of WHOIS. ICANN's internal enterprise risk management processes will continue as a process in FY 12, with support to the Board Risk Committee and program risk management.

Tracking the Affirmation of Commitments: Emerging Threats and Issues

Under the category of emerging threats and issues, ICANN recognizes that some of this work is led by others in the ecosystem. ICANN may be following these activities as an observer or may play a larger collaborative or facilitating role, depending on the topic and community interest.

Threats may be divided into those that 1) leverage the DNS and unique identifiers, such as botnets, denial of service attacks, social engineering attacks for fraud or malicious conduct, or route hijacking attacks, and 2) threats on the underlying infrastructure. Infrastructure threats may include TLD and registrar failure, disasters, authority or authentication compromise, and government interventions.

Emerging issues worthy of different levels of focus in FY 12 include:

- IDN variant case studies, IDN implementation and application acceptance, issues with IDN tables
- DNSSEC implementation and adoption
- IPv6/IPv4 address space issues
- Interactions between the DNS and applications (mobile applications, social media applications
- Increasing understanding of unique identifier security issues with users, including law enforcement & businesses

A specific example of community work related to emerging threats and risks is the DNS Security and Stability Analysis Working Group (DSSA-WG). This is a cross-community working group whose charter was adopted by the ALAC, ccNSO, GNSO, and NRO. The DSSA-WG includes participants from ICANN's Supporting Organization stakeholder groups, Advisory Committees, the Regional Internet Registries, as well as independent experts from the broader community. These organizations approved the Charter for the DSSA-WG during the ICANN meeting in Cartagena, Colombia in December 2010. Information on the DSSA-WG is available at https://community.icann.org/display/AW/Joint+DNS+Security+and+Stability+Analysis+Working+Group.

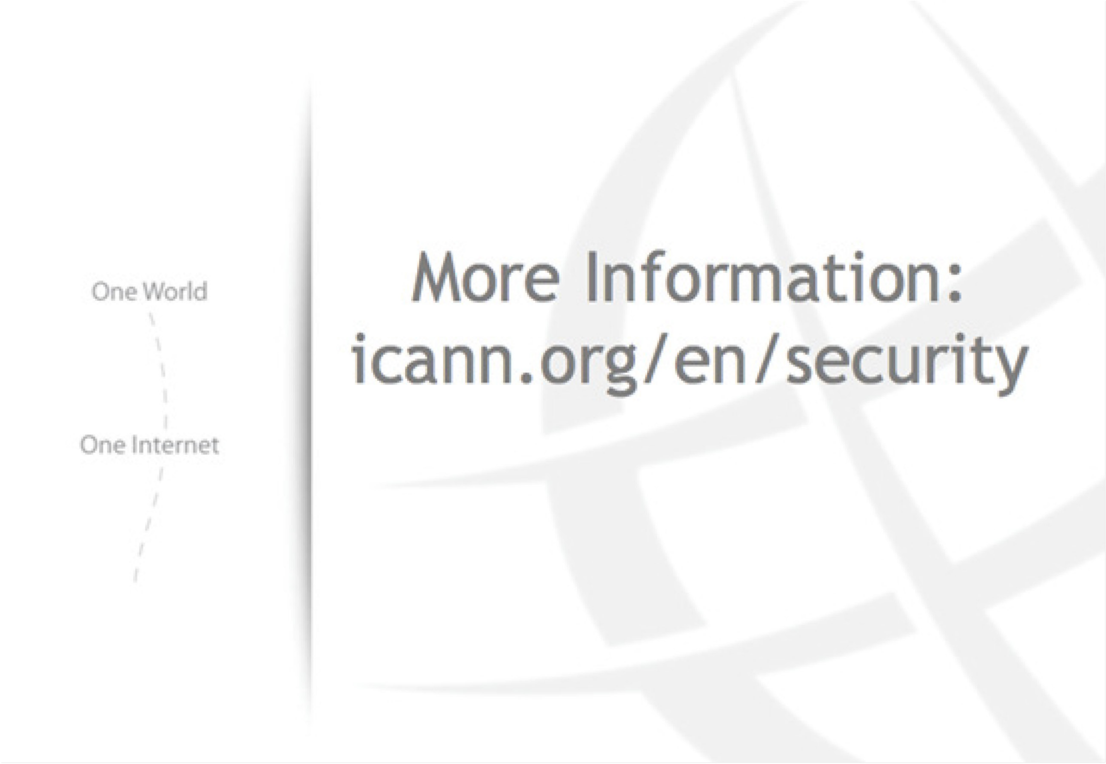
The objective of the DSSA-WG is to draw upon the collective expertise of the participating Supporting Organizations and Advisory Committees, solicit expert input and advice and report:

- The actual level, frequency and severity of threats to the DNS;
- The current efforts and activities to mitigate these threats to the DNS; and
- The gaps (if any) in the current security response to DNS issues.

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 recognition of ICANN's capacity limitations and willingness to collaborate for the benefit of the greater community.

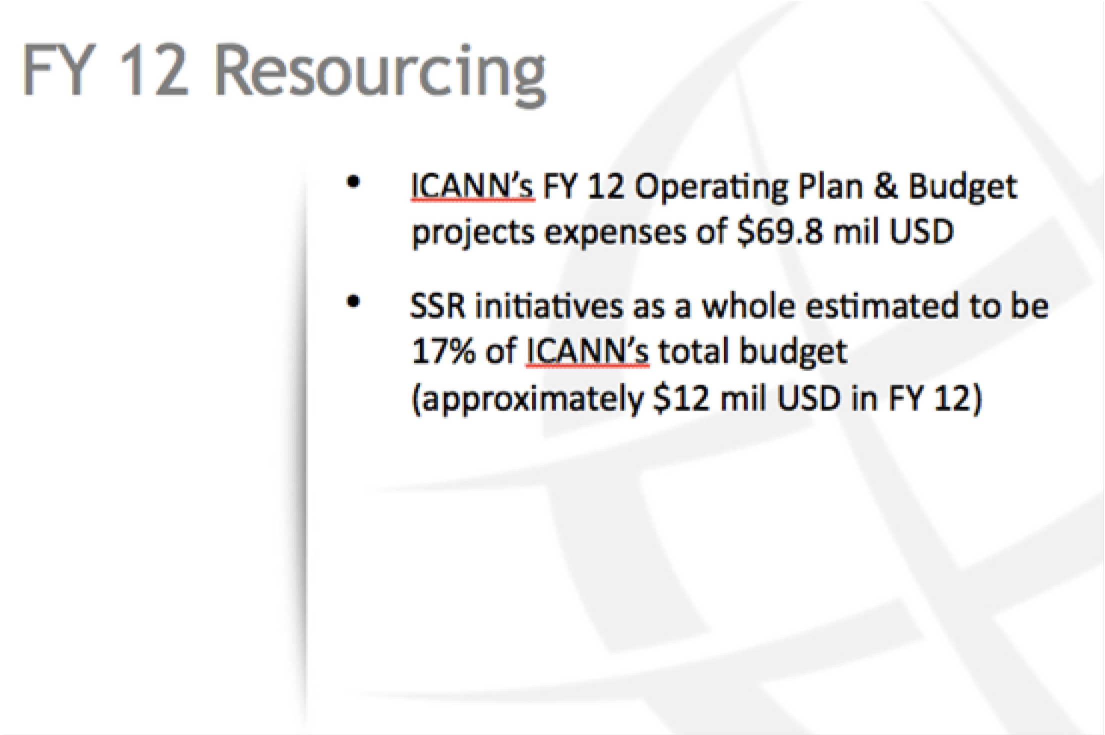


One World

One Internet

More Information:
icann.org/en/security

Appendix A



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)

Appendix B – Glossary of SSR Terms and Acronyms

ACRP – Attack Contingency Response Planning

Add Grace Period – a five-day option period at the beginning of the registration of an ICANN-regulated second-level domain. Registrants may opt to cancel their registration during this five day time period, when registration fees must be fully refunded by the domain name registry.

APWG – Anti Phishing Working Group

ASN – Autonomous System Numbers: within the Internet, an Autonomous System (AS) is a collection of connected IP routing prefixes that presents a common, clearly defined routing policy to the Internet. Internet Service Providers (ISPs) must have an Autonomous System Number (ASN) officially registered through IANA.

ccNSO - Country Code Names Supporting Organization of ICANN is the policy development body for a narrow range of global country code Top Level Domain issues within the ICANN structure.

ccTLD – country code Top Level Domain

CENTR – Council of European National Top Level Domain Registries is an association of Internet country code Top Level Domain Registries such as .uk in the United Kingdom and .es in Spain. Full Membership is open to organizations, corporate entities or individuals that operate a country code Top Level Domain registry.

CSIS - Center for Strategic and International Studies provides strategic insights and policy solutions to decision makers in government, international institutions, the private sector, and civil society.

FIRST – Forum of Incident Response and Security Teams

gTLD – generic Top Level Domain

IANA – Internet Assigned Numbers Authority

IDN – Internationalized Domain Name

IETF - Internet Engineering Task Force

IP – Internet Protocol specifies the format of packets and the addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source. By itself IP is something like the postal system. It allows you to address a package and send it using the system, but there's no direct link between your packet and the recipient. TCP/IP creates the connection between two hosts so that they can send messages back and forth.

IPv4 - Internet Protocol version 4 is the fourth revision in the development of the Internet Protocol (IP) and it is the first version of the protocol to be widely deployed. Together with IPv6, it is at the core of standards-based internetworking methods of the Internet, and is still by far the most widely deployed Internet Layer protocol.

IPv6 - Internet Protocol version 6 is the next-generation Internet Layer protocol for packet-switched internetworks and the Internet. In December 1998, the Internet Engineering Task Force (IETF) designated IPv6 as the successor to version 4 by the publication of a Standards Track specification, RFC 2460.

ISOC – Internet Society

IT – Information Technology

Botnets – most commonly created by duping ordinary users into opening an attachment on their computer that appears to do nothing but actually installs hidden software to be used later for an attack. The now compromised computers, or "bots," are combined to form networks which can then be directed as desired, most often for malicious attacks.

Cache Poisoning – exploiting a flaw in the DNS software to make it accept incorrect information which then causes the server to cache the false entry thereby sending all subsequent server requests to the new, falsely verified domain.

Denial of Service attack (DoS) – malicious code which causes a flood of incoming messages, essentially forcing the targeted system to shut down, thereby denying use by legitimate users.

Distributed Denial-of-Service attack (DDoS) – a type of denial of service attack in which an attacker uses malicious code installed on multiple systems in order to attack a single target. This method has a greater effect on the target than is possible with just a single attacking machine. On the Internet, a distributed denial-of-service attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. DDoS attacks are most effective when launched via a large number of open recursive servers: distribution increases the traffic and decreases the focus on the sources of the attack. The impact on the misused open recursive servers is generally low, but the effect on the target is high. The amplification factor is estimated at 1:73. Attacks based on this method have exceeded 7 Gigabits per second.

DNS – Domain Name System which translates domain names (alpha) into IP addresses (numeric). Because they're easier to remember domain names are alphabetic. The Internet, however, is based on numeric IP addresses (e.g. 198.123.456.0). When you use a domain name (www.examplir.gratis.com), a DNS service translates the alphabetic name into the corresponding numeric IP address.

DNSSEC – Domain Name System Security Extensions provide a way for software to validate that Domain Name System (DNS) data have not been modified during Internet transit. This is done by incorporating public-private signature key pairs into the DNS hierarchy to form a chain of trust originating at the root zone. Importantly, DNSSEC is not a form of encryption. It is backward compatible with existing DNS, leaving records as they are—unencrypted. DNSSEC ensures record integrity through the use of digital signatures that attest to their authenticity.

At the core of DNSSEC is the concept of a chain of trust. ICANN's proposal to sign the root zone file with DNSSEC (of October 2008) builds on that notion and, based on security advice, recommends that the entity responsible for making changes, additions and deletions to the root zone file and confirming those changes are valid, should generate and digitally sign the resulting root zone file update. This signed file should then be passed to another organization (presently VeriSign Corporation) for distribution. In other words, the organization responsible for the initial basis of trust—validating root zone changes with top level domain operators—should also authenticate the validity of the final product before it is distributed.

Domain Name Front Running – the questionable practice employed by some domain name registrars of using insider information to register domain names in advance with the intent to sell the name, at a premium, to registrants who would logically benefit from having the name for their own use

Domain tasting – the practice of a domain name registrant using the five-day Add Grace Period at the beginning of the registration of an ICANN-regulated second-level domain to test the marketability of a domain name. During this period a cost-benefit analysis is conducted by the registrant on the viability of deriving income from advertisements being placed on the domain's website.

Domain tasting should not be confused with **domain kiting**, which is the process of deleting a domain name during the five-day add grace period and immediately re-registering it for another five-day period. This process is repeated any number of times with the end result of having the domain registered without ever actually paying for it.

Double flux – Of particular concern to ICANN is a variant of fast flux called double flux where the attacker not only changes addresses that point to illegal web sites, but the addresses of the DNS name servers that the attacker uses for the "user friendly" names he embeds in phish emails. In both cases, the changes occur very quickly, on the order of 3 minutes, leaving virtually no time for investigators to respond. ICANN's SSAC is working closely with the brand defenders and law enforcement as well as registries and registrars to identify countermeasures, especially ones that take DNS out of the fast flux equation.

Fast flux – an evasion technique used by phishers, identity thieves and other e-criminals to frustrate incident response team and law enforcement agency efforts to track down and take down illegal web sites. The fast flux technique closely resembles a three-card Monte shell game, where a "tosser" lays three folded playing cards on a table and a victim is lured into betting on his ability to "follow the red queen" (the British call this scam "Find the Lady"). The tosser moves all three cards at blinding speed while simultaneously distracting the victim with conversation, clever quips, and sleights of hand. Fast flux, however, is a high stakes trick, and has become a worrisome and omnipresent attack technique. In fast flux hosting, the tosser rapidly changes the addresses that point to illegal web sites.

Malware – an amalgamation of the words "malicious" and "software" often used as a catchall phrase to include computer viruses, worms, trojans , rootkits, spyware, adware, crimeware and any other unwanted software introduced to a user's computer with or without their consent. Malware is deemed to be such based on the perceived intent of the creator rather than any particular features of the software.

NOC – a Network Operations Center is a physical location from which a typically large network is managed, monitored and supervised. NOCs also provide network accessibility to users connecting to the network from outside of the physical space.

NOG – Network Operations Group

NRO – Number Resource Organization

Patches – programs designed to fix software flaws, often installed automatically to reduce need for end-user participation and increase ease of use.

Phishing – a form of Internet fraud that aims to steal valuable information such as credit cards, social security numbers, user IDs and passwords by creating a website similar to that of a legitimate organization, then directing email traffic to the fraudulent site to harvest what should be private information for financial or political gain.

RAA – Registrar Accreditation Agreements

Registry – an organization that manages the registration of top-level Internet domain names

Registrar - a company authorized to register Internet domain names

RIR – Regional Internet Registry

RPKI – Resource Public Key Infrastructure

RSEP – Registry Services Evaluation Process

RSTEP – Registry Services Technical Evaluation Panel

Spam – any unsolicited email. Usually considered a costly nuisance, spam now often contains malware. Malware is a class of malicious software—viruses, worms, trojans, and spyware—that is designed to infect computers and systems and steal critical information, delete applications, drives and files, or convert computers into an asset for an outsider or attacker.

Spoofing – an attack situation where one person or program masquerades as another by falsifying data. The falsified data is in turn trusted as valid by the individual system attempting to connect with the legitimate system or program.

TLD – Top-level domain

Trojan - a class of malicious software (malware) that appears to perform a desirable function but instead performs undisclosed malicious functions allowing unauthorized access to the host machine, giving Trojan users the ability to save their files onto the unwitting computer user's machine or even watch the user's screen and control the computer.

Virus –a program or string of code that is loaded onto a computer without the user's knowledge and runs malicious software (malware). Even a simple virus can replicate itself, making it more damaging because it will quickly use all available memory on an infected computer system.

Worm – similar to a virus by design a Worm is considered to be a variant of a virus, but is more dangerous due to its ability to transmit itself across networks. Worms spread from computer to computer, but unlike viruses, have the ability to travel without any human action intentional or unintentional. A worm takes advantage of file or information transport features on a computer system, which is what allows it to travel unaided. For example, a worm can send a copy of itself using an unknowing user's email address book. It would then replicate on the newly infected computers and propagate yet again through the newly compromised systems' email address books and continue on eventually consuming so much memory and bandwidth that it causes entire networks to come to a halt.