Security, Stability and Resiliency Framework

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

March 2013

Table of Contents

List of Figures

Executive Summary

The Internet has thrived as an ecosystem engaging many stakeholders through collaboration in an open and transparent environment. The Internet fosters the sharing of knowledge, 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, and on an Internet that is healthy, stable and resilient.[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.

Since 2009, ICANN has published an annual Security, Stability and Resiliency (SSR) Framework. The Framework is recognized in the Affirmation of Commitments[2], and has been analyzed favorably by the Security, Stability and Resiliency Review Team[3] as part of the Affirmation of Commitments review process.

The SSR Framework describes ICANN's role and boundaries in supporting a single, global interoperable Internet and the challenges for the Internet's unique identifier systems. The document is divided into two parts. Part A explains the foundation for ICANN's role in security, stability and resiliency, the Internet ecosystem, and ICANN community. Part B describes ICANN's strategic objectives for SSR and planned activities in the FY 14 operational year (July 2013-June 2014).

The major change from the FY 13 to FY 14 Framework is the adoption of the SSR Review Team recommendations in October 2012[4] and reactions to developments in the Internet ecosystem since the previous version was published in June 2012 (see Part B). Projected activities in FY 14 will focus on supporting a healthy ecosystem, to provide the foundation for a more stable, reliable and resilient Internet for the global community.

The FY 14 Framework is being made available as a single document for ease of translation and sharing at upcoming ICANN meeting in Beijing, China, 7-11 April 2013.

[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.

[2] Affirmation of Commitments by the United States Department of Commerce and ICANN, http://www.icann.org/en/about/agreements/aoc/affirmation-of-commitments-30sep09-en.htm.

[3] Final Report of the Security, Stability and Resiliency Review Team, 20 Jun 2012, http://www.icann.org/en/about/aoc-review/ssr/final-report-20jun12-en.pdf.

[4] Adoption of the SSR Review Team recommendations by the ICANN Board of Directors, 18 October 2012, http://www.icann.org/en/about/aoc-review/ssr/board-action.

Part A – Foundational Section for ICANN's Role

ICANN's Mission & Core Values

"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."

ICANN Bylaws, as amended 20 December 2012 (http://www.icann.org/en/about/governance/bylaws#I)

Core Value #1 – "Preserving and enhancing the operational stability, reliability, security and global interoperability of the Internet."

This core value is acknowledged in the Affirmation of Commitments, that "global technical coordination of the Internet's underlying infrastructure – the DNS – is required to ensure interoperability" and "preserving the security, stability and resiliency of the DNS" is a key commitment for the benefit of global Internet users.

ICANN's SSR Role and Remit

Under the Affirmation of Commitments review process, the SSR Review Team recommended that ICANN "publish a single, clear and consistent statement of its SSR remit and limited technical mission." (Recommendation 1, 20 June 2012).

A draft statement of ICANN's role and remit in security, stability and resiliency of the Internet's unique identifiers was published in May 2012 (http://www.icann.org/en/news/public-comment/draft-ssr-role-remit-17may12-en.htm), and revised following public comment and discussion at the ICANN meetings in Prague (June 2012) and Toronto (October 2012, http://toronto45.icann.org/meetings/toronto2012/presentation-draft-ssr-role-remit-04oct12-en.pdf).

The following description of ICANN's role and remit is intended to address Recommendation 1:

As a global multistakeholder organization, ICANN facilitates the security, stability and resiliency of the Internet's unique identifier systems through coordination and collaboration.

The community expects ICANN, as a global organization, to perform its role in an open, accountable and transparent manner and inclusive of the diversity of stakeholders in the greater Internet ecosystem.

Within its technical mission, ICANN's SSR role encompasses three categories of responsibilities:

1. ICANN's operational responsibilities (organizational risk management of internal operations including L-root, DNS operations, DNSSEC key signing operations, IANA functions, new TLD operations, Time Zone Database Management);
2. ICANN's involvement as a coordinator, collaborator and facilitator with the global community in policy and technical matters related to the Internet's unique identifiers;
3. ICANN's engagement with others in the global Internet ecosystem.

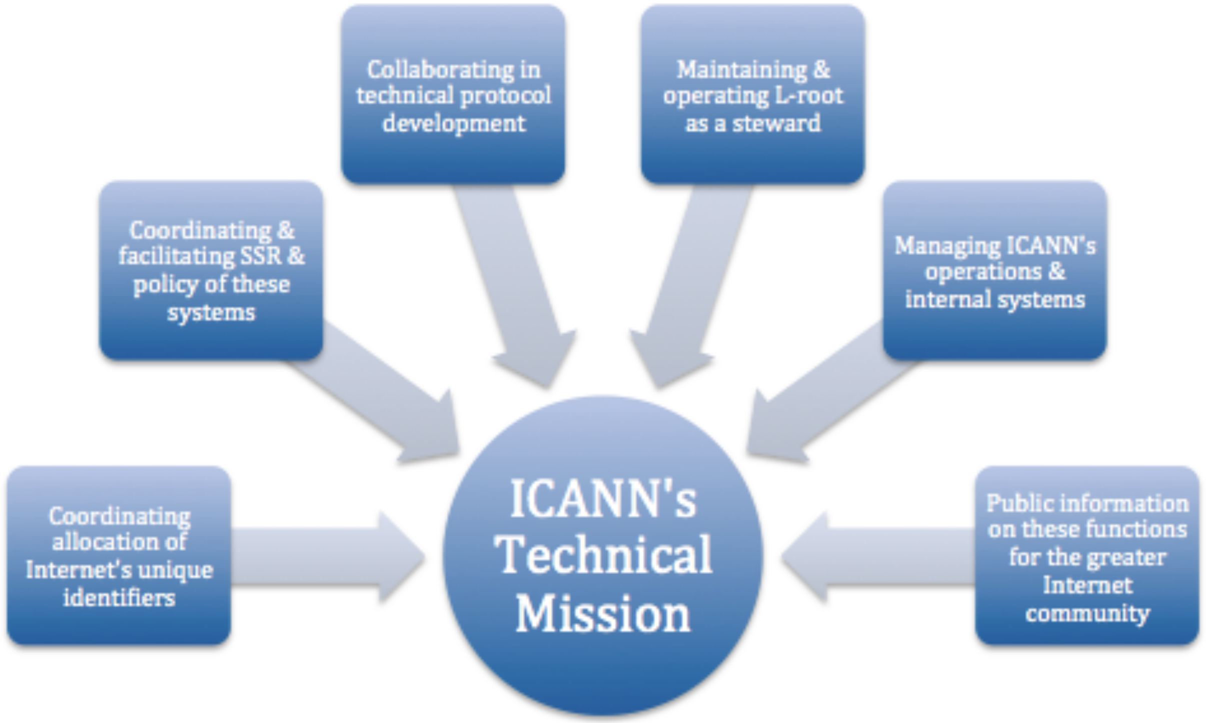

Collaborating in technical protocol development
Maintaining & operating L-root as a steward
Coordinating & facilitating SSR & policy of these systems
Managing ICANN's operations & internal systems
Coordinating allocation of Internet's unique identifiers
ICANN's Technical Mission
Public information on these functions for the greater Internet community

Figure 1 - ICANN's Technical Mission

Definitions for this Framework

Security – the capacity to protect and prevent misuse of Internet unique identifiers.

Stability – the capacity to ensure that the system operates as expected, and that users of the unique identifiers have confidence that the system operates as expected.

Resiliency – the capacity of the unique identifier system to effectively withstand/tolerate/survive malicious attacks and other disruptive events without disruption or cessation of service.

Note – These definitions are unchanged since the FY 12 SSR Framework published in 2011.

Based on the work from the 2nd DNS Security Symposium (conducted in Kyoto, Japan in 2010) and the 3rd DNS Security Symposium (conducted in Rome, Italy in 2011), an initial definition of **Unique Identifier Health** has been included in the FY 14 SSR Framework. This concept is adapted from the Kyoto Symposium report definition for DNS Health as:

> A state of general functioning of the Internet's unique identifiers that is within nominal technical bounds in the dimensions of coherency, integrity, speed, availability, vulnerability and resiliency.

A definition from the discipline of ecological economics defines ecosystem health as “a measure of the overall performance of a complex system that is built up from the behaviour of its parts.”[5]

Responsibilities that lie outside ICANN’s role in SSR include:

- ICANN does not play a role in policing the Internet or operationally combatting 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.

As an organization, ICANN is not a law enforcement agency, a court of law or government agency. Law enforcement and governments participate as stakeholders in ICANN’s processes and policy development.

ICANN does play a role in supporting the work of law enforcement or government agencies in carrying out legitimate actions at their request. ICANN participates with the operational security community in studying, analyzing and identifying malicious use or abuse of the DNS.

ICANN cannot unilaterally suspend or terminate domain names. ICANN is able to enforce its contracts with third parties, including domain name registration providers.

ICANN plays the same part as any interested stakeholder with regards to Internet protocols; evolution of Internet protocols and related standards are not under the purview of ICANN. ICANN supports open standards development through collaborative, multistakeholder processes.

The Challenge

Misuse of and attacks against the DNS and global networks challenge overall unique identifier security. DNS attacks target the broad range of users, individuals, businesses, civil society and governments.

As the frequency and sophistication of disruptive events and other malicious behaviour increases, ICANN and the global community must continue to collaborate toward a healthy ecosystem, improving the resilience of the unique identifier systems and strengthening its capabilities.

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

[5] This concept is adapted from "What is a healthy ecosystem?" by Robert Costanza and Michael Mageau, University of Maryland Institute for Ecological Economics, 1999, published in Aquatic Ecology, http://geminis.dma.ulpgc.es/profesores/personal/jmpc/Master08%28PrimeraEdici%F3n%29/Homeostasis/Homeo03s.pdf, http://books.google.com/books?id=YTeCxF5gqMQC&dq=ecosystem+and+health. The concept described has also been influenced by A Framework to Analyze the Robustness of Social-ecological Systems from an Institutional Perspective (2004), http://www.ecologyandsociety.org/vol9/iss1/art18/.

innovation at its edge, and allowed for the sharing of knowledge, creativity and commerce in a global commons.

In today's environment of collaborative multistakeholder Internet governance in a greater Internet ecosystem, traditional views of cybersecurity as led by one sector, whether that be by governments or the private sector, do not work. Neither governments nor individual actors in the private sector have adequate administrative or legal remit over the diverse set of interconnected systems and networks, and the scale of the task of operating and securing these resources is beyond the reach of any but a collaborative, multi-party endeavor.

All parties with a stake in cybersecurity must adopt a broader view. Security in the context of the Internet's unique identifiers should be addressed through a healthy Internet ecosystem. This approach focuses on an Internet that is sustainable or healthy, stable and resilient. A system that is sustainable for the future. We need to collectively concentrate on the ecosystem's "ability to maintain its structure and function over time in the face of external stress."[6]

This past year has seen an escalation in threats against the Internet's unique identifier systems. Attacks against top-level domain registry operators (see IEDR's statement from November 2012, https://www.iedr.ie/wp-content/uploads/2012/12/IEDR-Statement-D-issued-8Nov.pdf and a November 2012 *Techcrunch* article on PKNIC, http://ta.gg/5uf), registrars, the banking sector, law enforcement and threats against root server operators appeared in the news media in 2012. See Arbor Networks Worldwide Infrastructure Security Report, January 2013, http://www.arbornetworks.com/research/infrastructure-security-report.

Government intervention saw users lose connectivity to the outside world, for example in Syria (see http://www.renesys.com/blog/2012/11/syria-off-the-air.shtml). Hurricane Sandy impacted Internet connectivity for the Northeastern United States, showing the power of natural disasters on global networks (see a Preliminary Analysis of Network Outages During Hurricane Sandy, USC/ISI Technical Report ISI-TR-685b, November 2012, ftp://ftp.isi.edu/isi-pubs/tr-685.pdf).

Some inhibiting trends to improved unique identifier health have included the slow rate of DNSSEC adoption by registrars, browser and application developers and registrants. Increased awareness of criminal use of the DNS has stimulated interest in the development of tactics and tools to keep pace.

Additional trends have been observed:

- Continued growth in adoption of DNSSEC by TLD operators
- Expansion of root server instances worldwide
- Additional new ccTLDs (IDN and non-IDN) launched in a growing number of languages and character sets

[6] Costanza and Mageau, et al.

- Further progress with the evaluation of applications in the new gTLD program and anticipated introduction of new gTLDs in 2013
- Increased interest in cybersecurity capability building, stimulating the delivery of DNS training beyond operational communities to law enforcement and the legal community.

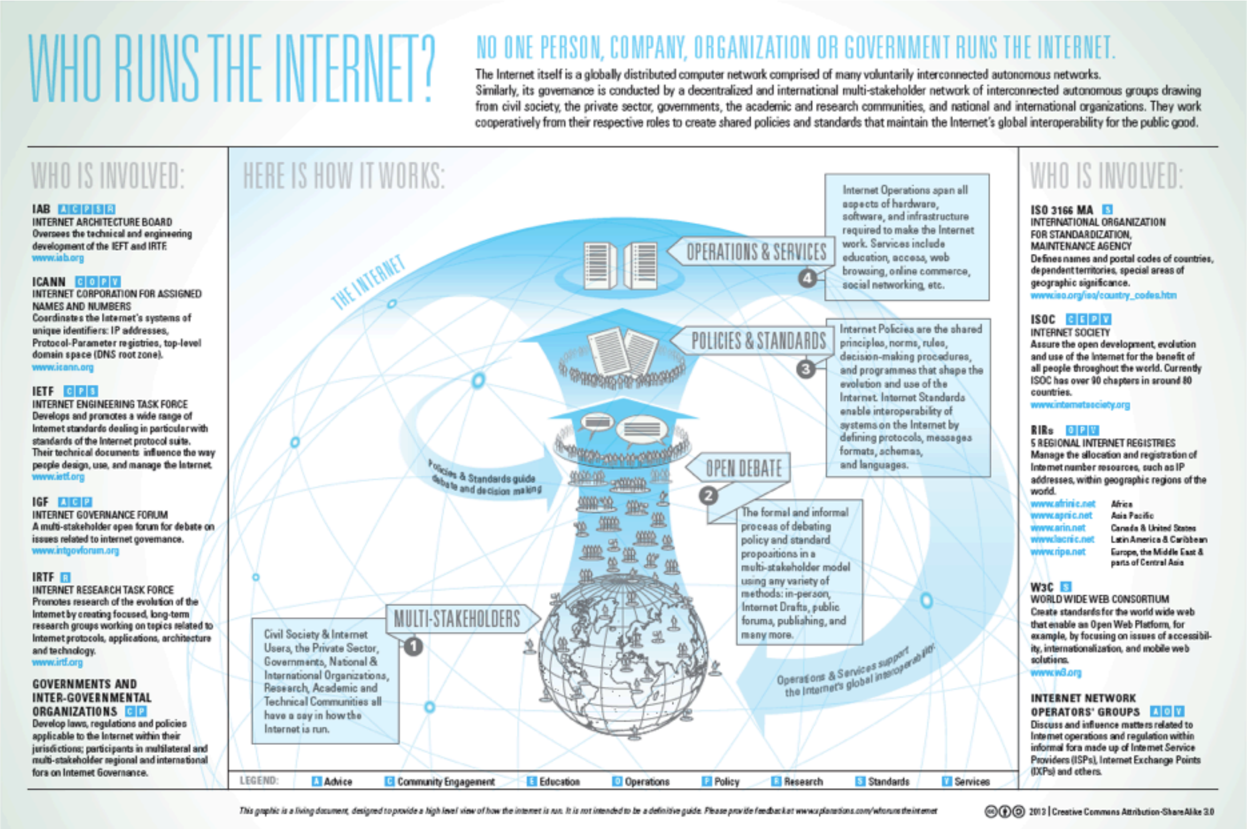
The Internet Ecosystem and ICANN Community

ICANN operates for the benefit of the Internet community as a whole. The public is a diverse collection of communities knitted together by the Internet and operating as a complex ecosystem. The Internet is now an essential enabler for global knowledge and information exchange, commerce and governance. UNESCO Vancouver Declaration, September 2012 (http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/mow/unesco_ubc_vancouver_declaration_en.pdf) and WSIS+10, Toward Knowledge Societies for Peace and Development, Final Statement, 27 February 2013 (http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/WSIS_10_Event/wsis10_final_statement_en.pdf).

The Internet is recognized as fundamental for supporting the world's economy and sustainable development (see OECD Internet Economy Outlook 2012, http://www.oecd.org/sti/interneteconomy/ieoutlook.htm).

The term "ecosystem" describes the natural world around us. It can be defined as the network of interactions among organisms and between organisms and their environment. Ecosystems are dynamic entities. The Internet is an ecosystem, and it is a network of organizations and communities. These organizations and communities work together and in their roles. The Internet is successful and thriving because its ecosystem is open, transparent and collaborative.

The Internet Ecosystem is made up of a number of organizations and processes that shape the coordination and management of the global Internet and enable its overall functioning. These organizations include: technology and engineering organizations, network operators, resource management organizations, users, civil society, commercial and non-commercial entities, educators, policy-makers, law enforcement and governments.



WHO RUNS THE INTERNET?

NO ONE PERSON, COMPANY, ORGANIZATION OR GOVERNMENT RUNS THE INTERNET.

The Internet itself is a globally distributed computer network comprised of many voluntarily interconnected autonomous networks. Similarly, its governance is conducted by a decentralized and international multi-stakeholder network of interconnected autonomous groups drawing from civil society, the private sector, governments, the academic and research communities, and national and international organizations. They work cooperatively from their respective roles to create shared policies and standards that maintain the Internet's global interoperability for the public good.

WHO IS INVOLVED:

IAB A C P S R
INTERNET ARCHITECTURE BOARD
Oversees the technical and engineering development of the IEFT and IRTF.
www.iab.org

ICANN C O P V
INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS
Coordinates the Internet's systems of unique identifiers: IP addresses, Protocol-Parameter registries, top-level domain space (DNS root zone).
www.icann.org

IETF C P S
INTERNET ENGINEERING TASK FORCE
Develops and promotes a wide range of Internet standards dealing in particular with standards of the Internet protocol suite. Their technical documents influence the way people design, use, and manage the Internet.
www.ietf.org

IGF A C P
INTERNET GOVERNANCE FORUM
A multi-stakeholder open forum for debate on issues related to internet governance.
www.intgovforum.org

IRTF R
INTERNET RESEARCH TASK FORCE
Promotes research of the evolution of the Internet by creating focused, long-term research groups working on topics related to Internet protocols, applications, architecture and technology.
www.irtf.org

GOVERNMENTS AND INTER-GOVERNMENTAL ORGANIZATIONS C P
Develop laws, regulations and policies applicable to the Internet within their jurisdictions; participants in multilateral and multi-stakeholder regional and international fora on Internet Governance.

HERE IS HOW IT WORKS:

THE INTERNET
OPERATIONS & SERVICES
4
POLICIES & STANDARDS
3
OPEN DEBATE
2
MULTI-STAKEHOLDERS
1
Policies & Standards guide debate and decision making
Operations & Services support the Internet's global interoperability

Internet Operations span all aspects of hardware, software, and infrastructure required to make the Internet work. Services include education, access, web browsing, online commerce, social networking, etc.

Internet Policies are the shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet. Internet Standards enable interoperability of systems on the Internet by defining protocols, messages formats, schemas, and languages.

The formal and informal process of debating policy and standard propositions in a multi-stakeholder model using any variety of methods: in-person, Internet Drafts, public forums, publishing, and many more.

Civil Society & Internet Users, the Private Sector, Governments, National & International Organizations, Research, Academic and Technical Communities all have a say in how the Internet is run.

WHO IS INVOLVED:

ISO 3166 MA S
INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, MAINTENANCE AGENCY
Defines names and postal codes of countries, dependent territories, special areas of geographic significance.
www.iso.org/iso/country_codes.htm

ISOC C E P V
INTERNET SOCIETY
Assure the open development, evolution and use of the Internet for the benefit of all people throughout the world. Currently ISOC has over 90 chapters in around 80 countries.
www.internetsociety.org

RIRs O P V
5 REGIONAL INTERNET REGISTRIES
Manage the allocation and registration of Internet number resources, such as IP addresses, within geographic regions of the world.

www.afrinic.net	Africa
www.apnic.net	Asia Pacific
www.arin.net	Canada & United States
www.lacnic.net	Latin America & Caribbean
www.ripe.net	Europe, the Middle East & parts of Central Asia

W3C S
WORLD WIDE WEB CONSORTIUM
Create standards for the world wide web that enable an Open Web Platform, for example, by focusing on issues of accessibility, internationalization, and mobile web solutions.
www.w3.org

INTERNET NETWORK OPERATORS' GROUPS A O V
Discuss and influence matters related to Internet operations and regulation within informal fora made up of Internet Service Providers (ISPs), Internet Exchange Points (IXPs) and others.

LEGEND: A Advice C Community Engagement E Education O Operations P Policy R Research S Standards V Services

This graphic is a living document, designed to provide a high level view of how the internet is run. It is not intended to be a definitive guide. Please provide feedback at www.xplanations.com/whorunstheinternet

Figure 2 - Internet Ecosystem Info Graphic

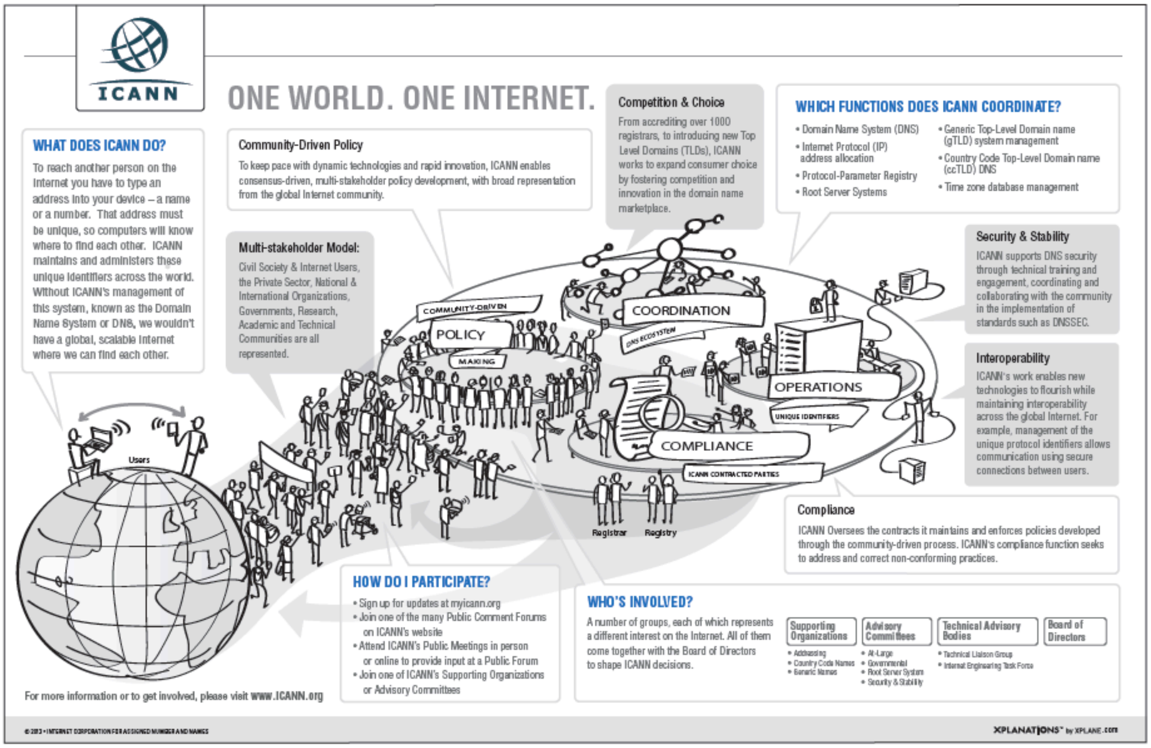
From an ICANN perspective, the Internet ecosystem can be viewed in three layers:

- the global community,
- the ICANN community,
- and ICANN as an organization.

The global community contains those who rely on a healthy, stable and reliable unique identifier system for the sharing of knowledge, commerce and innovation, but may not be aware of or participate in ICANN.

The ICANN community contains the greater community of actors involved in ICANN programs, processes and activities, who drive the multistakeholder policy development model for the benefit of global Internet users.

ICANN as an organization describes the operational structures, functions and support staff who support the greater ICANN community and multistakeholder coordination of the Internet's unique identifiers.



ONE WORLD. ONE INTERNET.

WHAT DOES ICANN DO?

To reach another person on the Internet you have to type an address into your device – a name or a number. That address must be unique, so computers will know where to find each other. ICANN maintains and administers these unique identifiers across the world. Without ICANN's management of this system, known as the Domain Name System or DNS, we wouldn't have a global, scalable Internet where we can find each other.

Community-Driven Policy

To keep pace with dynamic technologies and rapid innovation, ICANN enables consensus-driven, multi-stakeholder policy development, with broad representation from the global Internet community.

Multi-stakeholder Model:

Civil Society & Internet Users, the Private Sector, National & International Organizations, Governments, Research, Academic and Technical Communities are all represented.

Competition & Choice

From accrediting over 1000 registrars, to introducing new Top Level Domains (TLDs), ICANN works to expand consumer choice by fostering competition and innovation in the domain name marketplace.

WHICH FUNCTIONS DOES ICANN COORDINATE?

- Domain Name System (DNS)
- Internet Protocol (IP) address allocation
- Protocol-Parameter Registry
- Root Server Systems
- Generic Top-Level Domain name (gTLD) system management
- Country Code Top-Level Domain name (ccTLD) DNS
- Time zone database management

Security & Stability

ICANN supports DNS security through technical training and engagement, coordinating and collaborating with the community in the implementation of standards such as DNSSEC.

Interoperability

ICANN's work enables new technologies to flourish while maintaining interoperability across the global Internet. For example, management of the unique protocol identifiers allows communication using secure connections between users.

Compliance

ICANN Oversees the contracts it maintains and enforces policies developed through the community-driven process. ICANN's compliance function seeks to address and correct non-conforming practices.

HOW DO I PARTICIPATE?

- Sign up for updates at myicann.org
- Join one of the many Public Comment Forums on ICANN's website
- Attend ICANN's Public Meetings in person or online to provide input at a Public Forum
- Join one of ICANN's Supporting Organizations or Advisory Committees

WHO'S INVOLVED?

A number of groups, each of which represents a different interest on the Internet. All of them come together with the Board of Directors to shape ICANN decisions.

Supporting Organizations
- Addressing
- Country Code Names
- Generic Names

Advisory Committees
- At-Large
- Governmental
- Root Server System
- Security & Stability

Technical Advisory Bodies
- Technical Liaison Group
- Internet Engineering Task Force

Board of Directors

For more information or to get involved, please visit www.ICANN.org

Figure 3 - ICANN Info Graphic

A full 11x17 copy of the info graphic above is available in 6 languages at https://community.icann.org/display/ISBM/Handouts+for+Speakers+Bureau.
The community participates in ICANN through stakeholder groups, constituencies, supporting organizations and advisory committees. Information on advisory committees can be found on their pages below:

1. At Large Advisory Committee - http://www.atlarge.icann.org/alac
2. Governmental Advisory Committee - https://gacweb.icann.org/
3. Root Server System Advisory Committee - http://www.icann.org/en/groups/rssac
4. Security and Stability Advisory Committee - http://www.icann.org/en/groups/ssac

These committees provide advice to the ICANN Board of Directors, provide input into policy development processes and support community engagement.

Policy development derives from three Supporting Organizations:

1. Address Supporting Organization (ASO) - http://aso.icann.org/ (IP addresses)
2. Country Code Names Supporting Organization (ccNSO) - http://ccnso.icann.org/ (ccTLDs)
3. Generic Names Supporting Organization – http://gnso.icann.org (gTLDs)

Since ICANN's formation in 1998, 15 years ago, the DNS has grown from several hundred thousand domain names, distributed among seven generic top-level domains and approximately 250 hundred country-code TLDs, into a DNS with over 250 million domain names, used by 2.5 billion Internet users, across 316 TLDs. This space is set to grow dramatically with the introduction of new generic TLDs in 2013.

As of March 2013, there are 316 TLDs delegated in the Root Zone. The graphic below explains how these TLDs are categorized.

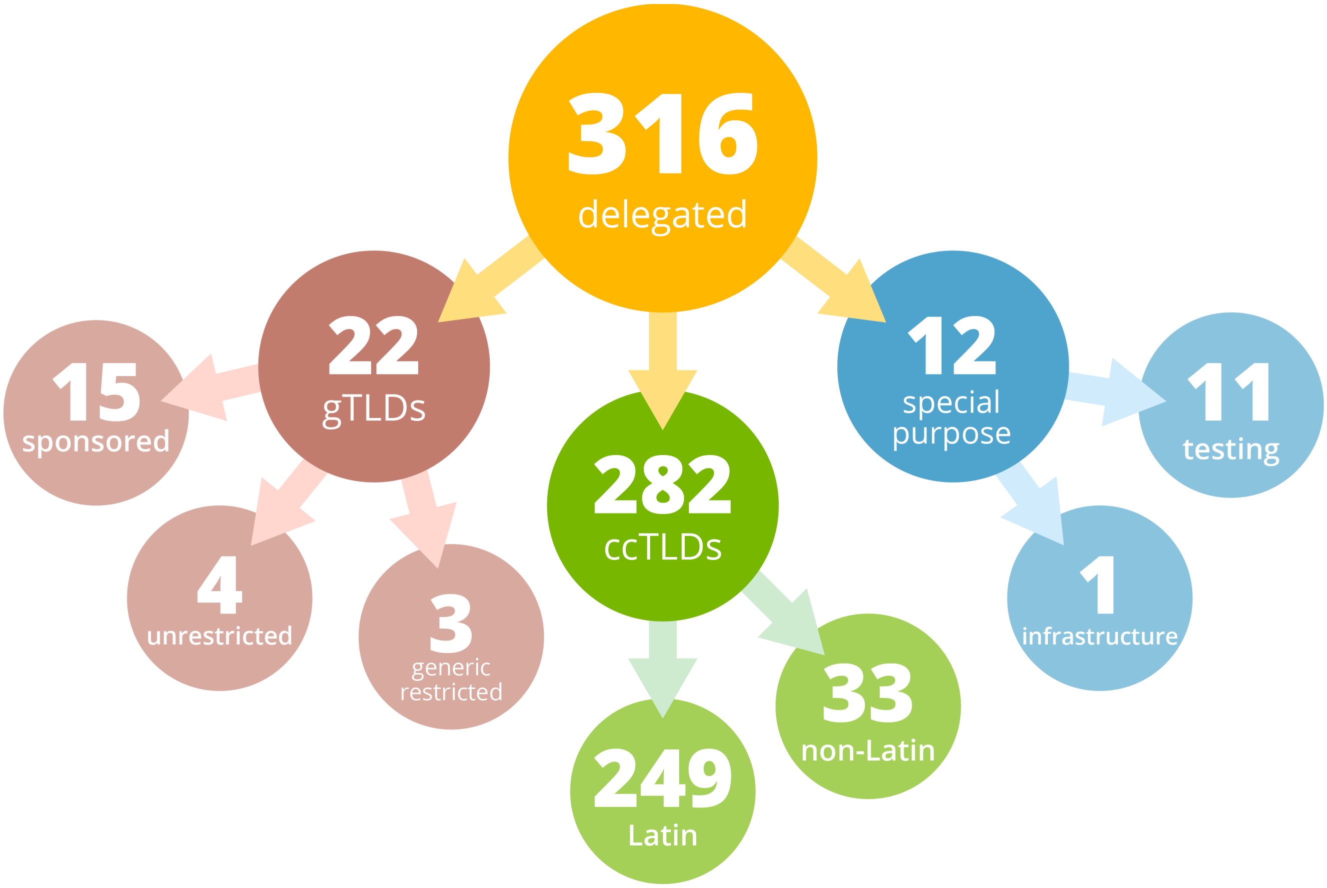


Figure 4 - TLDs in the Root Zone (Image credit: Kim Davies, IANA)

Relationships in SSR

ICANN maintains relationships with contracted parties (domain name registries and registrars, escrow providers and others), and partnerships, memoranda of understanding, accountability frameworks or exchange of letters. Other relationships may be less formal or unstructured, between ICANN and other international organizations or stakeholders in the ecosystem. https://www.icann.org/en/about/agreements.

Parties in the domain name registration process must work together to ensure decisions made related to the global technical coordination of the Internet's unique identifiers are made in the public interest and are accountable and transparent.

The image below depicts the nature of relationships in the domain registration process.

As part of SSR Review Team Recommendations 4 and 5, ICANN is in the process of documenting and defining the nature of its SSR relationships within the ICANN community. This will help provide a single focal point for understanding the interdependencies between the various organizations and entities, within their respective roles, and enable ICANN to maintain effective working arrangements in support of ICANN's SSR goals and strategic objectives.

Part B – FY 14 SSR Module

This section of the Security, Stability and Resiliency Framework centers on projected activities and initiatives in SSR for Fiscal Year 2014, covering the period from 1 July 2013 to 30 June 2014.

Security in the ICANN Strategic Plan

The ICANN Strategic Plan identifies DNS stability and security as one of the four key strategic focus areas for the organization. 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.

ICANN's 2012-2015 Strategic Plan will be unchanged for 2013 (see https://www.icann.org/en/news/announcements/announcement-28jan13-en.htm). This is the same Strategic Plan published prior to the FY 13 SSR Framework (June 2012). It has been recognized from feedback in the 2013 planning cycle that there is continued demand from the community for training and capability building activities. This shows support for the technical engagement provided by ICANN's Security Team.

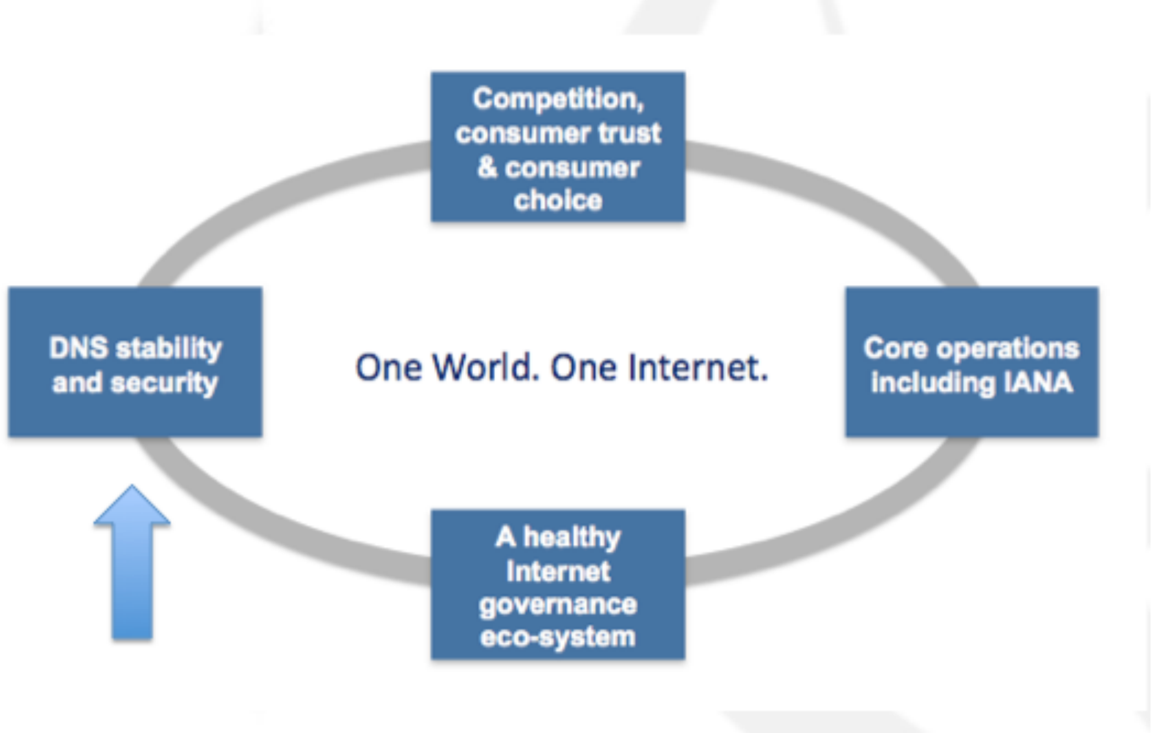

Competition, consumer trust & consumer choice
DNS stability and security
One World. One Internet.
Core operations including IANA
A healthy Internet governance eco-system

Figure 5 - ICANN Strategic Plan

The 2012-2015 Strategic Plan described 5 Strategic Objectives for DNS Security and Stability:

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

ICANN will commence a Strategic Planning process to focus on a long-term plan for the next five years, beginning in June 2013. More information will be made available on this new approach. As security is foundational to the organization, unique identifier security, stability and resiliency will remain one of the key strategic areas for ICANN.

Affirmation of Commitments Review

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 also "institutionalized and memorialized the technical coordination of the Internet's domain name and addressing system (DNS) globally by a private sector led organization."

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.

The first SSR Review was concluded in June 2012, "finding areas in which ICANN is working well, areas in which there is room for improvement, and other areas where key elements of SSR should be defined and implemented." SSR RT Final Report, June 2012.

The ICANN Board of Directors approved the final report and recommendations in October 2012.[7] Since the ICANN Toronto meeting, ICANN has moved forward with implementation of the SSR Review Team recommendations.

An update on ICANN's implementation progress was published on 19 December 2012 (http://blog.icann.org/2012/12/tracking-the-ssr-review-implementation/). Two recommendations have already been implemented (Recommendations 18 and 24). For the remainder of FY 13 through FY 15 and the start of the next SSR Review process, ICANN will track its implementation along with the other Affirmation of Commitments reviews (http://www.icann.org/en/news/in-focus/accountability).

The twenty-eight recommendations have been aligned with ICANN's Management Delivery structure unveiled at the ICANN meeting in Toronto. These are:

- Affirmation of Purpose [Recommendations 1, 2, 18, 24]

[7] http://www.icann.org/en/groups/board/documents/resolutions-18oct12-en.htm#1.e

- Operations Excellence [Recommendations 7, 8, 17, 20, 21, 9, 10, 11, 22, 25, 26, 27, 15, 28]
- Internationalization [Recommendations 3, 4, 5, 14, 16]
- Multistakeholder Model Evolution [Recommendations 6, 12, 13, 19, 23]

Further detail on the implementation of the individual recommendations can be found in Appendix A. ICANN's previous SSR Plans and Frameworks covering the Fiscal Years of 2010, 2011, 2012 and 2013, are available at https://www.icann.org/en/about/staff/security/archive.

A New Season – Moving to a Matrix Organization

In October 2012 at the ICANN meeting in Toronto, ICANN CEO Fadi Chehade unveiled the new ICANN Management Delivery Structure. This applies a matrix organization to ICANN's functions. Security is part of the Technical Functions within ICANN, paired with IANA, IT and ICANN's DNS Operations teams.

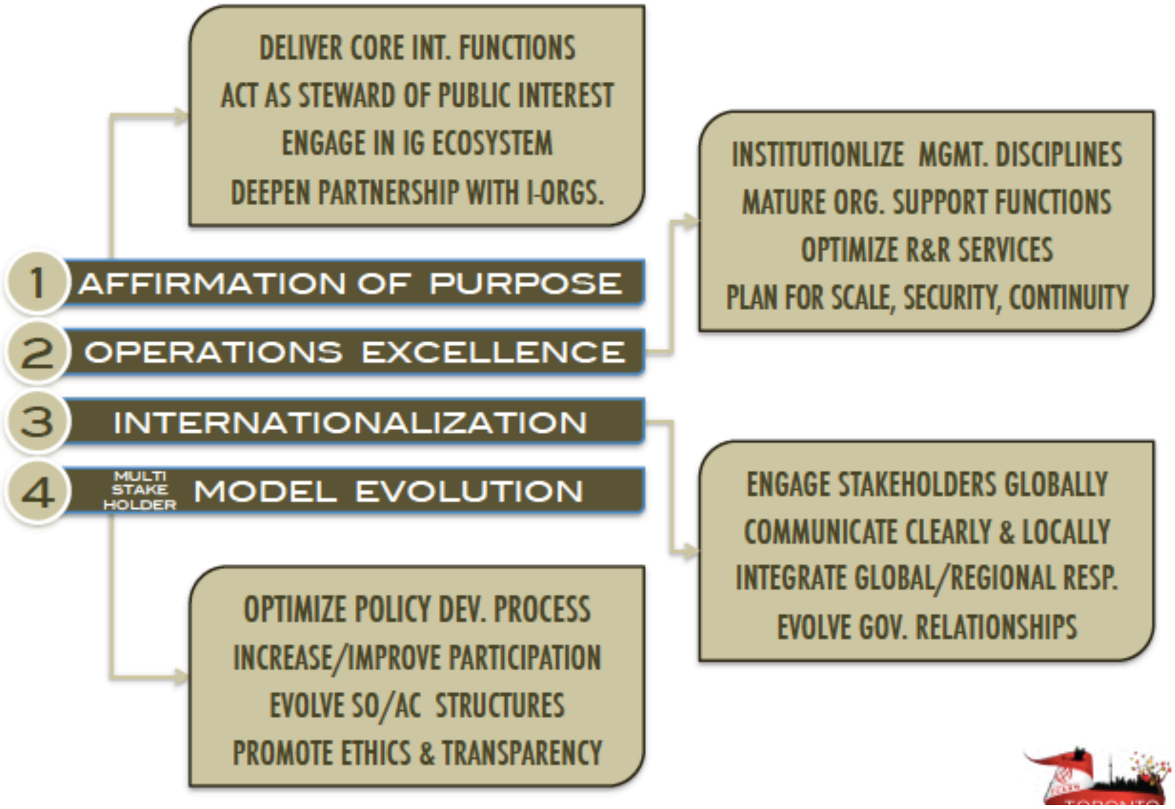

DELIVER CORE INT. FUNCTIONS
ACT AS STEWARD OF PUBLIC INTEREST
ENGAGE IN IG ECOSYSTEM
DEEPEN PARTNERSHIP WITH I-ORGS.
INSTITUTIONLIZE MGMT. DISCIPLINES
MATURE ORG. SUPPORT FUNCTIONS
OPTIMIZE R&R SERVICES
PLAN FOR SCALE, SECURITY, CONTINUITY
1 AFFIRMATION OF PURPOSE
2 OPERATIONS EXCELLENCE
3 INTERNATIONALIZATION
4 MULTI STAKE HOLDER MODEL EVOLUTION
ENGAGE STAKEHOLDERS GLOBALLY
COMMUNICATE CLEARLY & LOCALLY
INTEGRATE GLOBAL/REGIONAL RESP.
EVOLVE GOV. RELATIONSHIPS
OPTIMIZE POLICY DEV. PROCESS
INCREASE/IMPROVE PARTICIPATION
EVOLVE SO/AC STRUCTURES
PROMOTE ETHICS & TRANSPARENCY

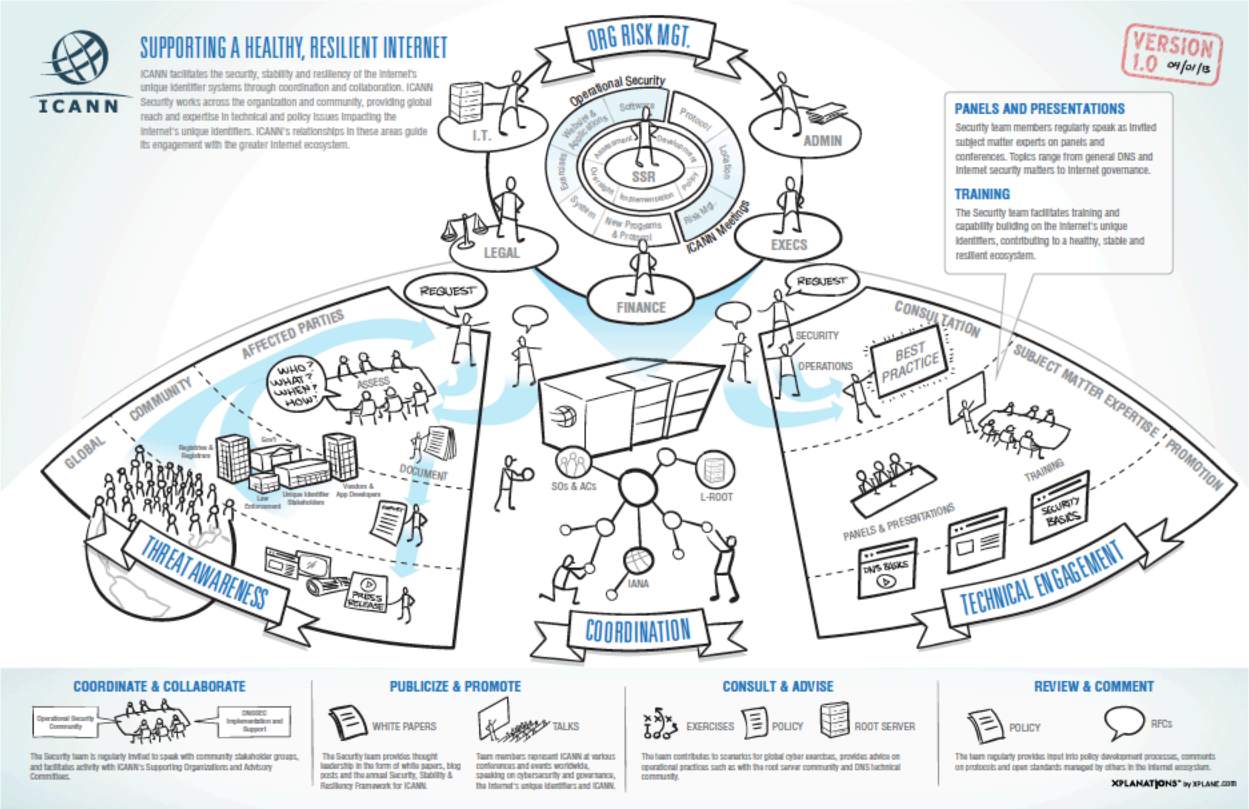
Figure 6 - ICANN's Management Delivery Areas

The Security team activity cuts across the organization, supporting each of the 4 management delivery areas. This includes support for Operations Excellence and ICANN's Global Stakeholder Engagement team (GSE) in Internationalization, Multistakeholder Model evolution and contributions to the greater Internet governance discussions with the broader community.

The matrix model will be implemented by distributing the work of ICANN among three main hubs – Los Angeles, Singapore and Istanbul. ICANN will also maintain engagement offices in Brussels, Washington, DC and other locations, to move closer to its stakeholders.

A Visualization of ICANN Security

As part of explaining ICANN's role and remit, the following draft graphic provides a visualization of ICANN's functions in security, stability and resiliency.



SUPPORTING A HEALTHY, RESILIENT INTERNET

ICANN facilitates the security, stability and resiliency of the Internet's unique identifier systems through coordination and collaboration. ICANN Security works across the organization and community, providing global reach and expertise in technical and policy issues impacting the Internet's unique identifiers. ICANN's relationships in these areas guide its engagement with the greater Internet ecosystem.

PANELS AND PRESENTATIONS

Security team members regularly speak as invited subject matter experts on panels and conferences. Topics range from general DNS and Internet security matters to Internet governance.

TRAINING

The Security team facilitates training and capability building on the Internet's unique identifiers, contributing to a healthy, stable and resilient ecosystem.

COORDINATE & COLLABORATE

The Security team is regularly invited to speak with community stakeholder groups, and facilitates activity with ICANN's Supporting Organizations and Advisory Committees.

PUBLICIZE & PROMOTE

WHITE PAPERS: The Security team provides thought leadership in the form of white papers, blog posts and the annual Security, Stability & Resiliency Framework for ICANN.

TALKS: Team members represent ICANN at various conferences and events worldwide, speaking on cybersecurity and governance, the Internet's unique identifiers and ICANN.

CONSULT & ADVISE

The team contributes to scenarios for global cyber exercises, provides advice on operational practices such as with the root server community and DNS technical community.

REVIEW & COMMENT

The team regularly provides input into policy development processes, comments on protocols and open standards managed by others in the Internet ecosystem.

Figure 7 - ICANN Security Info Graphic

This graphic shows the primary functions of ICANN Security, supporting organizational risk management, facilitating threat awareness of the Internet's unique identifiers, collaborating and coordinating with partners in the Internet community, and providing subject matter expertise in technical engagement, including training, thought leadership and consultation on technical and policy matters. (Note – this is a work in progress and will be revised prior to ICANN Beijing).

How Security, Stability & Resiliency Fits into ICANN's Functional Areas

Security at ICANN can be viewed as

- A Core Value for ICANN, in the Affirmation of Commitments
- One of the Four Focus Areas of the Strategic Plan
- An overall thematic area cutting across the organization

- A department within ICANN
- An essentially element in projects and activities

ICANN Security is a distributed team, with global reach and expertise in technical and policy issues impacting the Internet's unique identifiers. The Security team has an internal and external role, working across the organization and community to support ICANN's mission of preserving and enhancing the operational stability, reliability and global interoperability of the Internet. This work may not always be visible or public, but it does play an important role for ICANN and its commitments. The team serves as a bridge between DNS operators, the technical community, law enforcement, the operational security community and stakeholder groups.

ICANN Security team members

As of publication of this document, the Security team includes:

- Jeff Moss – Vice President & Chief Security Officer (Team Lead & Member of ICANN Executive Team; Technical Engagement and frequent speaker on Internet & Security issues)
- Geoff Bickers – Director of Security Operations (Corporate Security Programs, Meetings Security, ICANN Physical & Personnel Security, liaison with ICANN IT)
- John Crain – Senior Director, Security, Stability & Resiliency (Technical Engagement, Lead on Threat Awareness & Monitoring and Root Server representative on the DNS-OARC Board)
- Patrick Jones – Senior Director, Security (Team coordination, Member of ICANN Executive Team, SSR RT implementation, liaison to ICANN GSE and engagement in Internet governance)
- Richard Lamb – Senior Program Manager, DNSSEC (Technical Engagement in DNSSEC adoption & training; collaboration with community on DNSSEC; Policy Management and Practices for DNSSEC deployment)
- Dave Piscitello – Senior Security Technologist (Technical Engagement, training & thought leadership; Lead with law enforcement & operational security community; member of Executive Management Group for the Commonwealth Cybercrime Initiative)
- Sean Powell – Information Security Engineer (Organizational security; Network and information security; collaboration with ICANN IT and support to Director of Security Operations)

Picture 1- Jeff Moss at the Russian IGF

Picture 2 - John Crain, Rick Lamb (ICANN) and Revil Wooding (PCH) at CaribNOG 3

Picture 3 - Patrick Jones at the OAS Cyber Security Dialogue, December 2012

Picture 4 - Dave Piscitello speaking at ICLN, The Hague, December 2012

Engagement Criteria

In February 2012, the Security team formalized its criteria for outreach and engagement. The criteria has been influential in other parts of ICANN and is intended to provide guidance to ICANN's Security team and Executive Management on the types of collaborative and community activities supported by the Security team.

Table 1 – Security Criteria for Outreach and Engagement

Types of Events	Examples
ICANN Public Meetings	ICANN Beijing, Durban, Buenos Aires
ICANN Internal Meetings	Executive Meeting, Security Team, Board Workshop, Staff Training, Budget, Other
Meetings relevant to operational aspects of ICANN/IANA/L-root/DNSSEC, etc	IETF, DNS-OARC, RIPE NCC, NOGs, SSAC, RSSAC, others
Meetings where ICANN collaborates on global threats/mitigation	APWG, MAAWG, Interpol Underground Economy, cyber exercises, OAS
Technical Engagement – Trainings & Capability Building	Attack & Contingency Response training (ACRP), Secure Registry Ops, DNSSEC, Law Enforcement & Govt, Commonwealth Cybercrime Initiative
Symposia, Invited SME conferences, continuing education	SATIN, SSR Symposium, Security Confab, RSA, BlackHat, FIRST, ICLN
Engagement in Ecosystem, Multistakeholder model	IGF & regional IGFs, RANS, OECD, WSIS Forum, Pan Arab Cybersecurity, CTU

Engagement Criteria	✓
Does the event support an ICANN Strategic Objective	1. Maintain, Drive DNS Availability 2. Enhance Risk Management & Resilience of the DNS 3. Promote broad DNSSEC adoption 4. Enhance international DNS cooperation 5. Improve responses to DNS security incidents
Does the event fit within one of the following areas:	1. Operational/Organizational 2. Collaboration 3. Technical Engagement
In support of a partnership, MOU or stakeholder relationship?	
Does this support or add to ICANN's organizational reputation?	
How frequently does the event occur?	
Can other stakeholders be met nearby?	Who else is attending?
Where does this fit in the Budget?	Is this to support another team?

With the creation of the new matrix structure, the Security team provides support to ICANN's Global Stakeholder Engagement (GSE) team, and other teams across the organization. Examples of the types of events and activities supported by the ICANN Security team is below:

- IETF Meetings in Vancouver & Atlanta
- X-Con, CNNIC and CONAC meetings in China
- BlackHat & DefCon in Las Vegas, Abu Dhabi and Amsterdam
- UN Group of Experts on Geographic Names/UN Conference on Standardization of Geographic Names in New York
- Interpol Underground Economy in Lyon, France
- CIS Registries Meeting in Budva, Montenegro
- DNS training with the Serious Organized Crime Agency and Office of Fair Trading in London, UK
- DNSSEC training in Colombia with .CO; in Peru with .PE and the Network Startup Resource Center; in Hong Kong
- DNS capability building training with LACTLD in St. Maarten & Paraguay
- Asia-Pacific Telecommunity in Macau
- MENOG in Jordan
- LACNIC/LACNOG in Uruguay
- DNS training with Europol
- MAAWG, APWG, RIPE NCC and DNS-OARC
- OAS CICTE launch of their CyberLab for exercises
- APNIC 34
- ION Mumbai and Interop
- Providing talks via remote presentation, such as Caribbean IGF in St. Lucia in August 2012 and the Nepalese ICT Conference in February 2013

A key part of the technical engagement provided by the Security team is in DNS training in response to community requests. The team has developed a curriculum, which includes modules on:

- DNS Basics (including an overview of participating in ICANN)
- Attack and Contingency Response Program for TLD operators
- DNS training for law enforcement and the operational security community
- DNSSEC training
- Secure Registry Operations course

ICANN regularly partners with the Network Startup Resource Center (http://nsrc.org/), based at the University of Oregon, to provide technical engagement with regional TLD organizations, universities and operators worldwide. ICANN also partners with AfTLD, APTLD, LACTLD in this training.

International Developments

In the global arena, significant activity has occurred in FY 13. ICANN signed the World Economic Forum's Principles for Cyber Resilience, http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf, and participated at the World Economic Forum events in Davos, Switzerland and Washington DC in 2012 and 2013.

ICANN hosted the Commonwealth Cybercrime Initiative (CCI) at the ICANN meeting in Prague, Czech Republic in June 2012. Dave Piscitello of ICANN's Security team was appointed to the CCI Executive Management Group in November 2012 (http://blog.icann.org/2012/11/icann-security-team-members-appointed-to-lead-roles-in-global-community-initiatives/).

ICANN supported DNSSEC training in Latin America and the Caribbean (Trinidad, Colombia, Chile, Peru and Paraguay).

In July, the US Department of Commerce announced that it had awarded the IANA functions contract to ICANN, http://www.ntia.doc.gov/press-release/2012/commerce-department-awards-contract-management-key-internet-functions-icann. ICANN published a redacted version of its proposal for the IANA functions contract on 9 July 2012: https://www.icann.org/en/news/announcements/announcement-2-09jul12-en.htm. The period of performance is from 1 October 2012 to 30 September 2015, with two separate two-year option periods for a total contract period of seven years.

In July 2012, ICANN participated in the OAS Hemispheric Cybersecurity meeting in Uruguay and the OAS Cybersecurity Dialogue in Washington DC on 13 December 2012, http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-465/12.

In August 2012, the IAB, IEEE-SA, IETF, Internet Society and W3C launched Open Stand (http://open-stand.org/) as an open model for the collaborative, bottom-up development of standards for innovation and interoperability. This initiative is in alignment with ICANN principles for bottom-up, consensus-driven, multistakeholder collaboration.

ICANN contributed to the US FCC Communications Security, Reliability and Interoperability Council III (CSRIC III). Working Group 4 published its report on Network Security Best Practices in September 2012 (http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRICIII_9-12-12_WG4-FINAL-Report-DNS-Best-Practices.pdf). Contributions were also provided to Working Group 3, DNSSEC and Working Group 7, Anti-Bot Code of Conduct for ISPs.

ICANN participated at the Budapest Conference on Cyberspace in October 2012 (http://www.cyberbudapest2012.hu/), the follow-up event to the 2011 London Conference (https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement).

ICANN co-hosted its 4th Global DNS SSR Symposium with the AntiPhishing Working Group (APWG) at its eCOS event in Las Croabas, Puerto Rico in October 2012 (http://docs.apwg.org/events/2012_ecrime.html).

OECD published an analysis of national cybersecurity strategies in October 2012, describing support for a multistakeholder dialogue on cybersecurity in several national strategy documents. The citation for this paper is OECD (2012), "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", OECD Digital Economy Papers, No. 211, OECD Publishing. http://dx.doi.org/10.1787/5k8zq92vdgtl-en.

ICANN was well represented at the 7th Internet Governance Forum in Baku, Azerbaijan in November 2012 (http://blog.icann.org/2012/10/icann-at-internet-governance-forum-2012-2/), where Internet security was one of the main tracks of discussion (http://www.intgovforum.org/cms/component/content/article/114-preparatory-process/927-igf-2012). ICANN also attended regional IGF events in Latin America & the Caribbean, Russia, United Arab Emirates, and the United States.

In December 2012, ICANN CEO Fadi Chehade spoke at the opening of the World Conference on International Telecommunications in Dubai (http://www.itu.int/en/wcit-12/Pages/speech-chehade.aspx). In February 2013, ICANN participated in the Informal Experts Group preparation for the upcoming World Telecommunications Policy Forum in Geneva in May 2013.

ICANN participated in the Pan Arab Cybersecurity Observatory in Tunis, Tunisia in December 2012, sharing information with participants on ICANN's role and remit in security, stability and resiliency activities. ICANN also participated in December at the International Criminal Law Network conference at The Hague, Netherlands, and engaged with Europol to facilitate DNS training with the launch of the new European Cybercrime Center (EC3).

In January 2013, ICANN Security published a thought paper titled the Value of Assessing Collateral Damage Before Requesting a Domain Seizure, http://blog.icann.org/2013/01/the-value-of-assessing-collateral-damage-before-requesting-a-domain-seizure/. This is a follow-up to the March 2012 thought paper on Domain Seizures and Takedowns, http://blog.icann.org/2012/03/thought-paper-on-domain-seizures-and-takedowns/. This is related to SAC 056, SSAC Advisory on Impacts of Content Blocking via the Domain Name System, http://www.icann.org/en/groups/ssac/documents/sac-056-en.pdf, published in October 2012.

ICANN has followed the development of the EU Cybersecurity Strategy (Jan 2013), http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security and US Cybersecurity Executive Order (Feb 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0. Both documents represent the growing interest in establishing mechanisms for information sharing and collaboration in response to cybersecurity threats.

Key global Internet events prior to the publication of this document also included:

- APRICOT 2013 (Asia Pacific Regional Internet Conference on Operational Technologies) in Singapore, 19 February-1 March 2013, http://www.apricot2013.net/.
- WSIS+10, Toward Knowledge Societies for Peace and Sustainable Development (hosted by UNESCO), in Paris, 25-27 February 2013, http://www.unesco.org/new/en/communication-and-information/flagship-project-activities/wsis-10-review-event-25-27-february-2013/.
- Arab Multistakeholder Internet Governance event in Dubai, UAE and African Multistakeholder Internet Governance event in Addis Ababa, Ethiopia, http://www.icann.org/en/news/announcements/announcement-07feb13-en.htm.
- IETF 86, Orlando, Florida, 10-15 March 2013, http://www.ietf.org/meeting/86/index.html.

FY 14 Activities

For FY 14, ICANN's activities supporting a healthy, stable and resilient ecosystem will center on the following:

- Supporting Operational Excellence in activities led by IANA, IT, DNS Ops
- Providing Technical Engagement (through subject matter expertise and thought leadership, community engagement, conducting DNS training and capability building activities where requested with partners)
- Encouraging adoption and awareness of DNSSEC by enterprises, users and operators
- SSR Review Team recommendations implementation
- Supporting further L-root capacity, publication of data and measurement by ICANN's DNS Operations team
- Delivery of a DNS Risk Management Framework and completion of an assessment cycle
- Growing ICANN's enterprise risk management expertise to better support the Board Risk Committee and ICANN's evolving organizational risk management needs
- Supporting the establishment of new ICANN hub office locations in Singapore and Istanbul and expanding the Security team's capabilities in those locations to better serve the community
- Serving as a resource for the Global Stakeholder Engagement team in Internet governance and cybersecurity discussions, representing ICANN in conferences and meetings
- Facilitating and encouraging broader participation from the law enforcement and operational security community in ICANN
- Engaging with Civil Society on privacy and free expression issues as related to unique identifier security and a healthy Internet ecosystem (expanding outreach and engagement from ecosystem participants on SSR issues)
- Strengthening ICANN's internal networks, IT processes and information security

- Collaborating with the technical community, root server operators, application and browser developers on DNS issues
- Supporting ICANN's Policy and Stakeholder Relations teams where needed (SSAC, RSSAC, and SSR issues when discussed in SOs and ACs
- Supporting successful ICANN meetings in Durban, Buenos Aires, Singapore and London

In order to deliver on these initiatives, ICANN needs to grow its Security team in FY 14 with additional expertise and skills. This is necessary to meet the needs of the community and the matrix structure being implemented in this Fiscal Year. Explanation in support of the projected FY 14 SSR activities will be provided in the upcoming FY 14 budget and operating plan, to be published after the ICANN Beijing meeting. This will follow guidance in SSR Recommendations 20 and 21, that ICANN increase the transparency of information about the organization and budget related to the SSR Framework and ICANN provide a more structured process for showing how the organization and budget decisions relate to the SSR Framework.

Appendices

Appendix A- SSR RT Recommendations Tracking

This section provides detail on the implementation approaches for the 28 SSR Review Team recommendations, as aligned with the 4 management delivery areas.

Affirmation of Purpose – ICANN's Remit, Mission

SSR RT Recommendation	Implementation & Status
#1 - ICANN should publish a single, clear and consistent statement of its SSR remit and limited technical mission.	Public comment was taken on a draft statement between May-Sept 2012 [link: http://www.icann.org/en/news/public-comment/draft-ssr-role-remit-17may12-en.htm]. The draft statement was revised on 4 Oct 2012 [http://toronto45.icann.org/meetings/toronto2012/presentation-draft-ssr-role-remit-04oct2012-en.pdf]. An updated version appears in the FY 14 SSR Framework.
#2 - ICANN's definition and implementation of its SSR remit and limited technical mission should be reviewed in order to maintain consensus and elicit feedback from the Community.	The updated role and remit statement will be reviewed with the next SSR RT in 2015.
#24 - ICANN must clearly define the charter, roles and responsibilities of the Chief Security Office Team.	**Implemented** with updated Security team page [link: https://www.icann.org/security] on 4 October 2012 and publication of the FY 13 SSR Framework. Roles and responsibilities to be further refined with implementation of the new Management Delivery structure in 2013.
#18 - ICANN should conduct an annual operational review of its progress in implementing the SSR Framework and include this assessment as a component of the following year's SSR Framework.	**Implemented** as part of the FY 13 SSR Framework and will be repeated annually. Tracking of progress will be added to a new Dashboard page on the Security team page on the ICANN website.

Operations Excellence – Objectives

SSR RT Recommendation	Implementation & Status
#7 - ICANN should build on its current SSR Framework by establishing a clear set of objectives and prioritizing its initiatives and activities in accordance with these objectives.	The new Management Delivery structure will be used to align ICANN's objectives and initiatives with the annual SSR Framework, and support the development of the FY 14 budget, operating plan and next ICANN Strategic Plan. ICANN is working to align its objectives and activities to this structure.
#8 - ICANN should continue to refine its Strategic Plan objectives, particularly the goal of maintaining and driving DNS availability. Clear	This is connected with the next Strategic Plan. An alignment of objectives and activities in the Strategic Plan is needed with the annual SSR Framework and the SSR Review Team recommendations.

alignment of Framework & Strategic Plan.	

Operations Excellence – Transparency

SSR RT Recommendation	Implementation & Status
#17 - ICANN should establish a more structured internal process for showing how activities and initiatives relate to specific strategic goals, objectives and priorities in the SSR Framework.	The Management Delivery structure has been useful for addressing this recommendation, creating a mechanism for an internal process that will show how ICANN's SSR activities and initiatives relate to goals, objectives and priorities. More information on this process will be made available to the community through MyICANN and on the ICANN website between the ICANN Beijing and Durban meetings in 2013.
#20 - ICANN should increase the transparency of information about organization and budget related to implementing the SSR Framework and performing SSR-related functions.	This will be implemented through the FY 14 SSR Framework and FY 14 Operating Plan and Budget process. The new Security team Dashboard page will also be used to address this recommendation.

Operations Excellence – Structure

SSR RT Recommendation	Implementation & Status
#21 - ICANN should establish a more structured internal process for showing how organization and budget decisions relate to the SSR Framework, including the underlying cost-benefit analysis.	ICANN will use the Management Delivery work as the structured process for identifying the organization and budget decisions and align with SSR activities in the annual Framework. This will be implemented in the FY 14 Operating Plan & Budget.

Operations Excellence – Standards & Compliance

SSR RT Recommendation	Implementation & Status
#9 – ICANN should assess certification options with commonly accepted international standards (e.g. ITIL, ISO and SAS-70) for its operational responsibilities. ICANN should publish a clear roadmap towards certification.	ICANN's implementation of DNSSEC in the root has achieved SysTrust certification [link: https://www.iana.org/dnssec/systrust and https://cert.webtrust.org/icann.html]. Other certification processes are being led by ICANN's IANA functions team, IT and DNS Operations teams, with support from Security.
#10 - ICANN should continue its efforts to step up contract compliance enforcement and provide adequate resources for this function. ICANN also should develop and implement a more structured process for monitoring	This recommendation is being led by ICANN's Compliance team and through implementation of the recommendations from the WHOIS Review Team.

compliance issues and investigations.	

Operations Excellence – nTLDs

SSR RT Recommendation	Implementation & Status
#11 - ICANN should finalize and implement measures of success for new gTLDs and IDN fast track that expressly relate to its SSR-related program objectives, including measurements for the effectiveness of mechanisms to mitigate domain name abuse.	Staff is exploring the full implications of this Recommendation. Security team expects this will involve community-staff collaboration for full implementation. As this relates to the Competition, Consumer Trust and Consumer Choice Review and measurements for both new gTLDs and IDN ccTLDs delegated via the IDN ccTLD Fast Track, there will be engagement with stakeholders from across the community. The focus of this recommendation is mechanisms related to mitigating domain name abuse. Staff is supporting efforts in Advisory Committees and community on abuse metrics.
#22 - ICANN should publish, monitor and update documentation on the organization and budget resources needed to manage SSR issues in conjunction with introduction of new gTLDs.	This is related to Recommendation 21 (budget and organization decisions) as well as to the development of monitoring with the introduction of new gTLDs.

Operations Excellence – Risk Management & Threat Mitigation

SSR RT Recommendation	Implementation & Status
#25 – ICANN should put into place mechanisms for identifying both near and longer-term risks and strategic factors in its Risk Management Framework	This is underway and tied to the delivery of a Risk Management Framework under Recommendation 26.
#26 – ICANN should prioritize the timely completion of a Risk Management Framework.	This is underway. ICANN has retained Westlake Governance to assist with its DNS Risk Management Framework project. Westlake conducted an open session in Toronto, will be providing a draft framework in the near future and will provide a briefing on the framework concept at the ICANN Beijing meeting.
#27 – ICANN's Risk Management Framework should be comprehensive within the scope of its SSR remit and limited missions	The Risk Management Framework will be aligned with ICANN's activities in support of its technical mission and the community. This will be comprehensive in that scope, and will be accomplished with the delivery of the Framework under Recommendation 26.
#15 – ICANN should act as a facilitator in the responsible disclosure and dissemination of DNS security threats and mitigation techniques.	A draft Coordinated Disclosure document is being developed by ICANN's Security team. Staff collaborates with operators and trusted security community entities on DNS security threats and mitigation techniques. This is related to Recommendation 28.

#28 – ICANN should continue to actively engage in threat detection and mitigation, and participate in efforts to distribute threat and incident information.	This recommendation supports a continuation of ICANN efforts, including root zone monitoring, threat detection and mitigation related to ICANN's DNS Operations and to DNS threats and incidents in general.

Internationalization – Terminology & Relationships

SSR RT Recommendation	Implementation & Status
#3 - Once ICANN issues a consensus-based statement of its SSR remit and limited technical mission, ICANN should utilize consistent terminology and descriptions of this statement in all materials.	The Security team will work across the organization to use consistent terminology and descriptions related to ICANN's SSR role and remit in ICANN's materials. A first step is to conduct training with ICANN staff, then offer a webinar for community participation. We will also use these terminology and description in ICANN presentations and engagement.
#4 - ICANN should document and clearly define the nature of the SSR relationships it has within the ICANN Community in order to provide a single focal point for understanding the interdependencies between organizations.	Work has commenced to document and define these relationships. The visualization of ICANN's Security functions will be used to map relationships to the coordination and collaboration functions, threat awareness and technical engagement areas.
#5 - ICANN should use the definition of its SSR relationships to maintain effective working arrangements and to demonstrate how these relationships are utilized to achieve each SSR goal.	The Security team will work with ICANN's Global Stakeholder Engagement team to maintain and enhance effective working arrangements and relationships. The Security team has established relationships with law enforcement & the operational security community worldwide, and has provided past training in the Czech Republic, France, Netherlands, UK, US, among others.

Internationalization – Outreach & Engagement

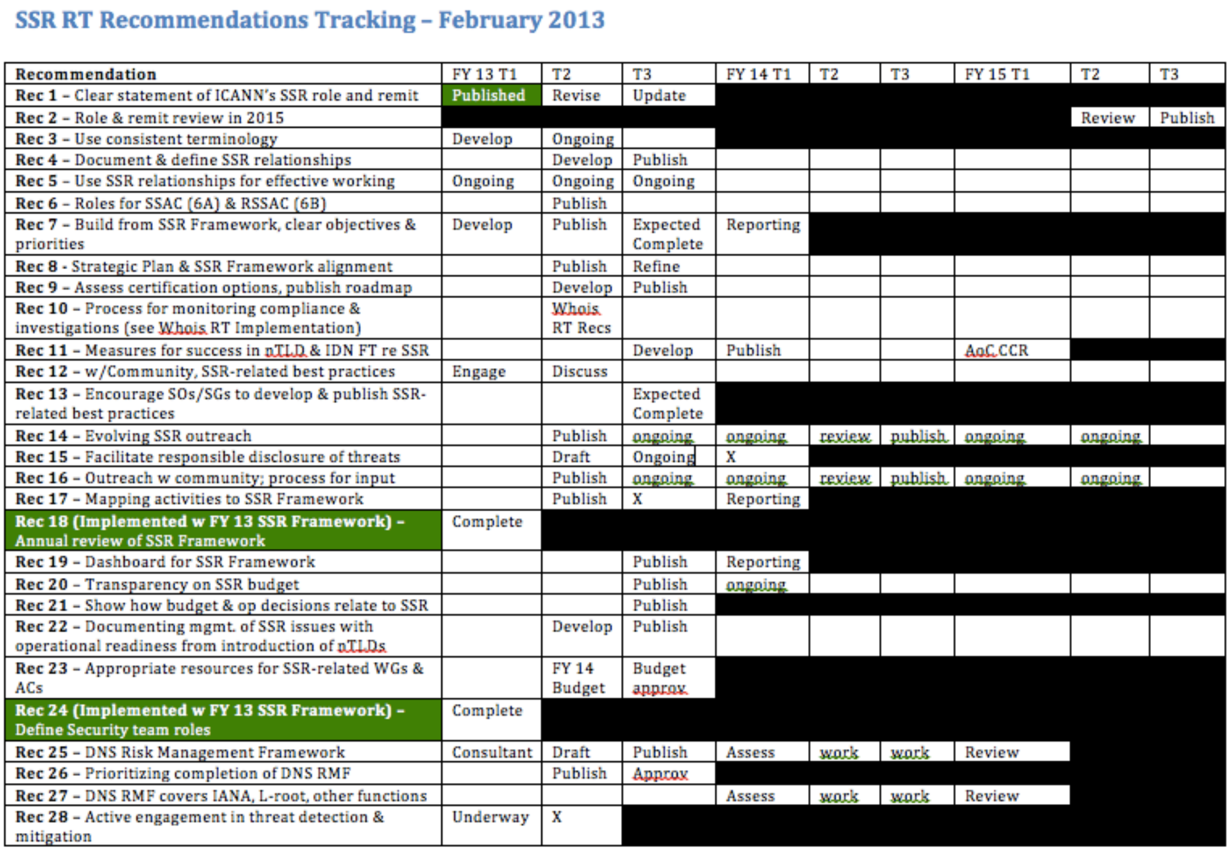
SSR RT Recommendation	Implementation & Status
#14 – ICANN should ensure that its SSR-related outreach activities continuously evolve to remain relevant, timely and appropriate.	Outreach activities have been expanded and will be reviewed annually. The Security team provides both a service function to ICANN's Global Stakeholder Engagement team as subject matter experts, and a community function in outreach and engagement in SSR matters.
#16 – ICANN should continue its outreach efforts to expand Community participation and input into the SSR Framework development process. ICANN also should establish a process for obtaining more systematic input from other ecosystem participants.	Outreach activities and processes have been expanded and will be reviewed annually. The Security team's ongoing work with security communities such as APWG, MAAWG has resulted in participation by members of those communities in SSAC. Through engagement with ICLN and CCI, the Security team emphasizes the value of multistakeholder approaches to cybersecurity issues. This is related to Recommendations 4, 5 and 14. The Security team supports a variety of capability building

	initiatives at the request of stakeholders, such as DNSSEC training, ccTLD attack and contingency response training, law enforcement training, outreach at Network Operator Group meetings such as CaribNOG, MENOG, among others.

Multistakeholder Model Evolution

SSR RT Recommendation	Implementation & Status
#6 - ICANN should publish a document clearly outlining the roles and responsibilities for both the SSAC and RSSAC in order to clearly delineate the activities of the two groups.	This recommendation will require community-staff collaboration. For tracking this has been divided into 6A [SSAC] and 6B [RSSAC]. 6A - Roles and Responsibilities of SSAC are defined in SSAC's Operating Procedures. SSAC is examining its operating procedures for 2013 and is also interested in aligning these the roles and responsibilities of RSSAC. 6B – Roles and Responsibilities for RSSAC are in development, following the end of public comment on proposed amendments to the ICANN Bylaws on the purpose of RSSAC. See http://www.icann.org/en/news/public-comment/bylaws-03jan13-en.htm.
#12 – ICANN should work with the Community to identify SSR-related best practices and support the implementation of such practices through contracts, agreements and MOUs and other mechanisms.	Implementation of Rec 12 will involve community-staff collaboration. Further discussion of this area will occur at the ICANN Beijing meeting in an Experts Panel on DNS Security and with the ccNSO Tech Working Group on non-contract best practices. The Security team has worked with the APWG Internet Policy Committee to publish recommendations for web application protection, has engaged in development of resources for security awareness (through SANS Securethehuman.org activities and with NCA Stop.Think.Connect). The current public comment period on the revised new gTLD registry agreement (see http://www.icann.org/en/news/public-comment/base-agreement-05feb13-en.htm) contains additional language on best practices.
#13 – ICANN should encourage all Supporting Organizations to develop and publish SSR-related best practices for their members.	This recommendation will involve community-staff collaboration through the ASO, ccNSO and GNSO on appropriate best practices related to the unique identifiers in their respective roles.
#19 - ICANN should establish a process that allows the Community to track the implementation of the SSR Framework. Information should be provided with enough clarity that the Community can track ICANN's	The Security team will soon release a Dashboard on its team page to show status tracking of the SSR Framework and ICANN's SSR initiatives.

execution of its SSR responsibilities	
#23 - ICANN must provide appropriate resources for SSR-related Working Groups and Advisory Committees, consistent with the demands placed upon them. ICANN also must ensure decisions reached by Working Groups and Advisory Committees are reached in an objective manner that is free from external or internal pressure.	Staff is conducting an inventory [23A] of activity in the existing SSR-related working groups and Advisory Committees (SSAC and RSSAC). This will be followed by a description or documentation of the budget process for SO/AC input [23B]. 23C will describe a standard operating process step to show that SO/AC/Working Group decisions are reached in an objective manner.



SSR RT Recommendations Tracking – February 2013

Recommendation	FY 13 T1	T2	T3	FY 14 T1	T2	T3	FY 15 T1	T2	T3
Rec 1 – Clear statement of ICANN's SSR role and remit	Published	Revise	Update	■	■	■	■	■	■
Rec 2 – Role & remit review in 2015	■	■	■	■	■	■	■	Review	Publish
Rec 3 – Use consistent terminology	Develop	Ongoing		■	■	■	■	■	■
Rec 4 – Document & define SSR relationships		Develop	Publish						
Rec 5 – Use SSR relationships for effective working	Ongoing	Ongoing	Ongoing						
Rec 6 – Roles for SSAC (6A) & RSSAC (6B)		Publish							
Rec 7 – Build from SSR Framework, clear objectives & priorities	Develop	Publish	Expected Complete	Reporting	■	■	■	■	■
Rec 8 - Strategic Plan & SSR Framework alignment		Publish	Refine						
Rec 9 – Assess certification options, publish roadmap		Develop	Publish						
Rec 10 – Process for monitoring compliance & investigations (see Whois RT Implementation)		Whois RT Recs							
Rec 11 – Measures for success in nTLD & IDN FT re SSR			Develop	Publish			AoC CCR	■	■
Rec 12 – w/Community, SSR-related best practices	Engage	Discuss							
Rec 13 – Encourage SOs/SGs to develop & publish SSR-related best practices			Expected Complete	■	■	■	■	■	■
Rec 14 – Evolving SSR outreach		Publish	ongoing	ongoing	review	publish	ongoing	ongoing	
Rec 15 – Facilitate responsible disclosure of threats		Draft	Ongoing	X	■	■	■	■	■
Rec 16 – Outreach w community; process for input		Publish	ongoing	ongoing	review	publish	ongoing	ongoing	
Rec 17 – Mapping activities to SSR Framework		Publish	X	Reporting	■	■	■	■	■
Rec 18 (Implemented w FY 13 SSR Framework) – Annual review of SSR Framework	Complete	■	■	■	■	■	■	■	■
Rec 19 – Dashboard for SSR Framework			Publish	Reporting	■	■	■	■	■
Rec 20 – Transparency on SSR budget			Publish	ongoing					
Rec 21 – Show how budget & op decisions relate to SSR			Publish	■	■	■	■	■	■
Rec 22 – Documenting mgmt. of SSR issues with operational readiness from introduction of nTLDs		Develop	Publish						
Rec 23 – Appropriate resources for SSR-related WGs & ACs		FY 14 Budget	Budget approx	■	■	■	■	■	■
Rec 24 (Implemented w FY 13 SSR Framework) – Define Security team roles	Complete	■	■	■	■	■	■	■	■
Rec 25 – DNS Risk Management Framework	Consultant	Draft	Publish	Assess	work	work	Review	■	■
Rec 26 – Prioritizing completion of DNS RMF		Publish	Approx	■	■	■	■	■	■
Rec 27 – DNS RMF covers IANA, L-root, other functions				Assess	work	work	Review	■	■
Rec 28 – Active engagement in threat detection & mitigation	Underway	X	■	■	■	■	■	■	■

Figure 8 - SSR RT Recommendations Tracking

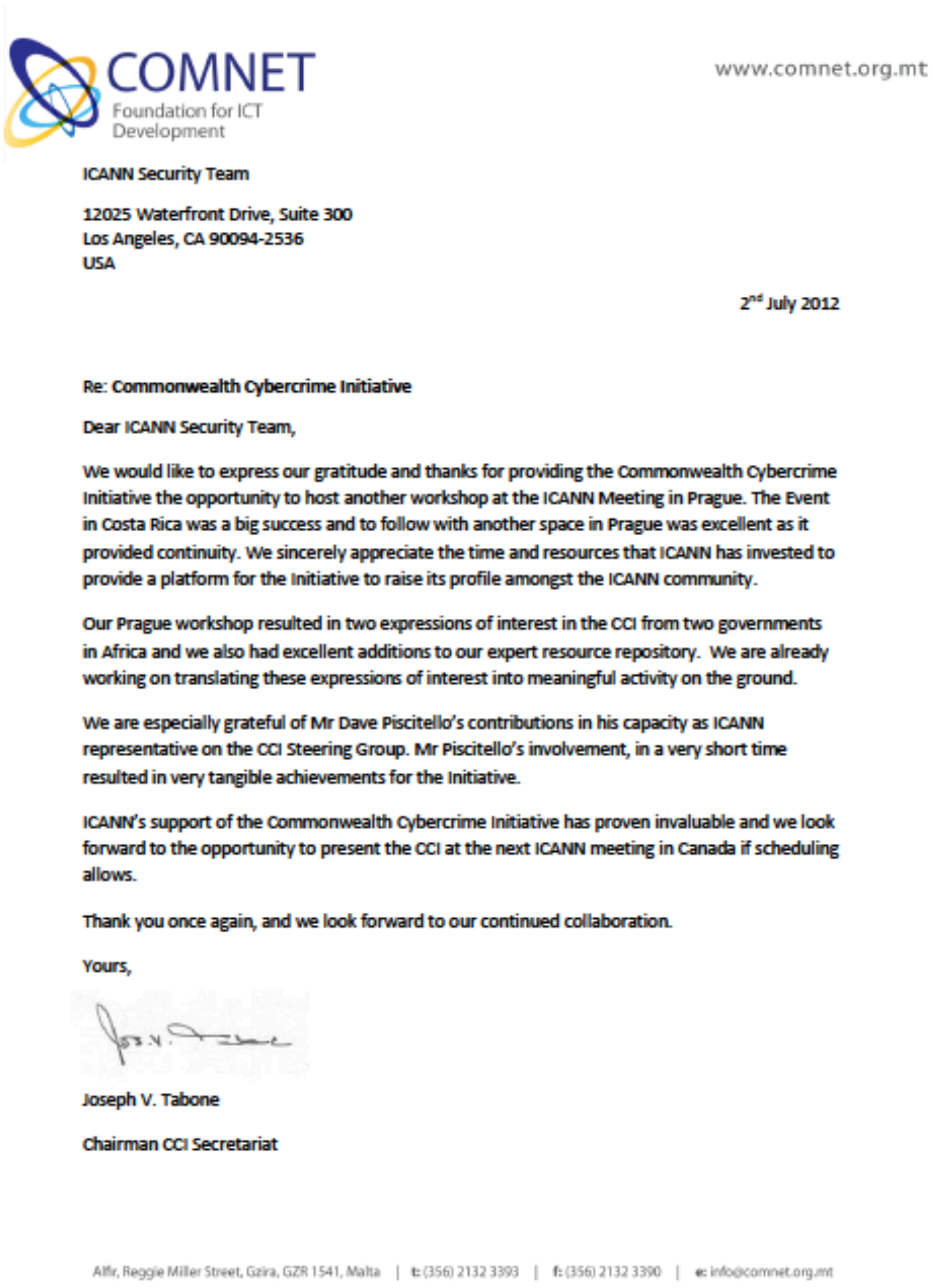
]

Appendix B – FY 13 Status Report

Overall Area	Program/Initiative	Status
Global Security Engagement	Engagement with the broader community, businesses, academic community, technical community and law enforcement on DNS Security issues	Conducted 4th Global DNS SSR Symposium, partnering with APWG at eCOS, Puerto Rico, October 2012
		Commonwealth Cybercrime Initiative workshops at ICANN Costa Rica & Prague, CCI Steering Group & EMG meetings
		BlackHat/Defcon in July 2012
		Internet Governance Forum & regional IGF events
		Speaking to the Business Constituency in Washington DC & contributing to the BC Newsletter for ICANN Toronto
Collaboration	Further support for DNS measurement & metrics tools, such as RIPE NCC's ATLAS	Contributed to RIPE NCC for further deployment of ATLAS nodes and data analysis. https://atlas.ripe.net/
	Root zone automation	The Root Zone Management (RZM) system used by IANA with NTIA and Verisign turned one year old in August 2012 (see http://blog.icann.org/2012/08/rzm-is-one-year-old/). The IANA team is working on additional secure processes, such as a Secure Notification system. See http://www.icann.org/en/news/public-comment/iana-secure-notification-12dec12-en.htm.
	Technical training with law enforcement & operational security community	The Security team hosted law enforcement at ICANN Prague and Toronto, as well as provided DNS training at Europol in the Netherlands and SOCA, OFT & the Metropolitan Police in the UK.
	Security & Stability Advisory Committee	Collaboration with SSAC in DNSSEC workshops at ICANN meetings; work parties and SSAC Advisories and Reports. SSAC's work has been substantial in FY 13.
	Support DNS Security & Stability Analysis WG	The DSSA completed its Phase 1 Report in August 2012. http://www.icann.org/en/news/public-comment/dssa-phase-1-report-14aug12-en.htm. The DSSA will meet again at the ICANN meeting in Beijing. ICANN also engaged with Westlake Governance for the DNS Risk Management Framework activity.
	Technical Evolution of WHOIS	ICANN announced an expert group on gTLD Directory Services in February 2013 (https://www.icann.org/en/news/announcements/announcement-14feb13-en.htm). In October 2012, ICANN announced it had engaged with CNNIC to implement an open-source RESTful WHOIS server, http://blog.icann.org/2012/10/cnnic-selected-to-implement-an-open-source-restful-whois-server/.
	Policy development – Registration Abuse;	ICANN has an open comment period on a preliminary report on Uniformity of Reporting, https://www.icann.org/en/news/public-

	Registrar Accreditation Agreement	comment/uofr-20feb13-en.htm. This report followed from GNSO Council action in response to the Registration Abuse Policies Working Group. On the Registrar Accreditation Agreement, negotiations continue. CEO Fadi Chehade provided an update on 7 February 2013, http://blog.icann.org/2013/02/registrar-accreditation-agreement-negotiation-session/.
	DNSSEC – key rollover work party in SSAC	The SSAC root key rollover work party is continuing its activities in 2013. Additional information will be made available at the ICANN Beijing meeting. Successful key ceremonies were conducted in Culpeper, Virginia and El Segundo, California.
	DNSSEC – SysTrust audit	The DNSSEC SysTrust certification is available at https://www.iana.org/dnssec/systrust.
	DNSSEC training with community	ICANN supported DNSSEC training in Colombia, Peru, Paraguay, Hong Kong, Chile and has upcoming training in Lebanon (March 2013) and Tunisia (April 2013).
	L-root Resilience	ICANN has supported the growth and distribution of L-root instances worldwide. In particular, partnerships have been announced to provide L-root instances in Africa with AfriNIC, in Latin America & the Caribbean with LACNIC, in Brazil with CGI.Br, in Korea with KISA, and in other locations.
Corporate Security Programs	Enhance ICANN's internal network security and processes	The Security team has been working with ICANN IT to strengthen ICANN's internal networks. The team has supported SANS training for IT staff and provided basic security training to ICANN staff in Los Angeles and Brussels.
	Improve business continuity and conduct internal exercises	Security has supported root resilience exercises and internal communications processes.
	Meetings security – risk assessments, traveler security	Conducted assessments on ICANN meeting locations; provided on-the-ground health and emergency services at ICANN meetings (ISOS)
Cross-Organizational	New gTLD Operations support	Provided support for the new gTLD team with Prioritization Draw; reviewing processes
		Assisting with Pre-delegation check system review with .SE, http://www.icann.org/en/news/announcements/announcement-21dec12-en.htm.
	Contractual Compliance	The Compliance Team has continued its growth in FY 13, publishing its audit plan (see http://www.icann.org/en/resources/compliance/audits)
	IDN Program	Attended the UNGEGN/UNCSGN meetings in New York in July & August 2012 at UN Headquarters, supported the continued work with the IDN Variant Program.
	Enterprise Risk Management	ICANN has engaged Westlake Governance on a DNS Risk Management Framework initiative. Further developments on Westlake's progress will be provided at the ICANN Beijing meeting.

The work in technical engagement performed by ICANN's Security team is collaborative. We do this for the benefit of the greater community. It is nice to receive letters of support for our work, but it is not something we seek in order to merely collect congratulatory statements. The following letters are a sampling of support that ICANN has received in FY 13 for its security engagement in the community.



COMNET
Foundation for ICT
Development

www.comnet.org.mt

ICANN Security Team

12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
USA

2nd July 2012

Re: Commonwealth Cybercrime Initiative

Dear ICANN Security Team,

We would like to express our gratitude and thanks for providing the Commonwealth Cybercrime Initiative the opportunity to host another workshop at the ICANN Meeting in Prague. The Event in Costa Rica was a big success and to follow with another space in Prague was excellent as it provided continuity. We sincerely appreciate the time and resources that ICANN has invested to provide a platform for the Initiative to raise its profile amongst the ICANN community.

Our Prague workshop resulted in two expressions of interest in the CCI from two governments in Africa and we also had excellent additions to our expert resource repository. We are already working on translating these expressions of interest into meaningful activity on the ground.

We are especially grateful of Mr Dave Piscitello's contributions in his capacity as ICANN representative on the CCI Steering Group. Mr Piscitello's involvement, in a very short time resulted in very tangible achievements for the Initiative.

ICANN's support of the Commonwealth Cybercrime Initiative has proven invaluable and we look forward to the opportunity to present the CCI at the next ICANN meeting in Canada if scheduling allows.

Thank you once again, and we look forward to our continued collaboration.

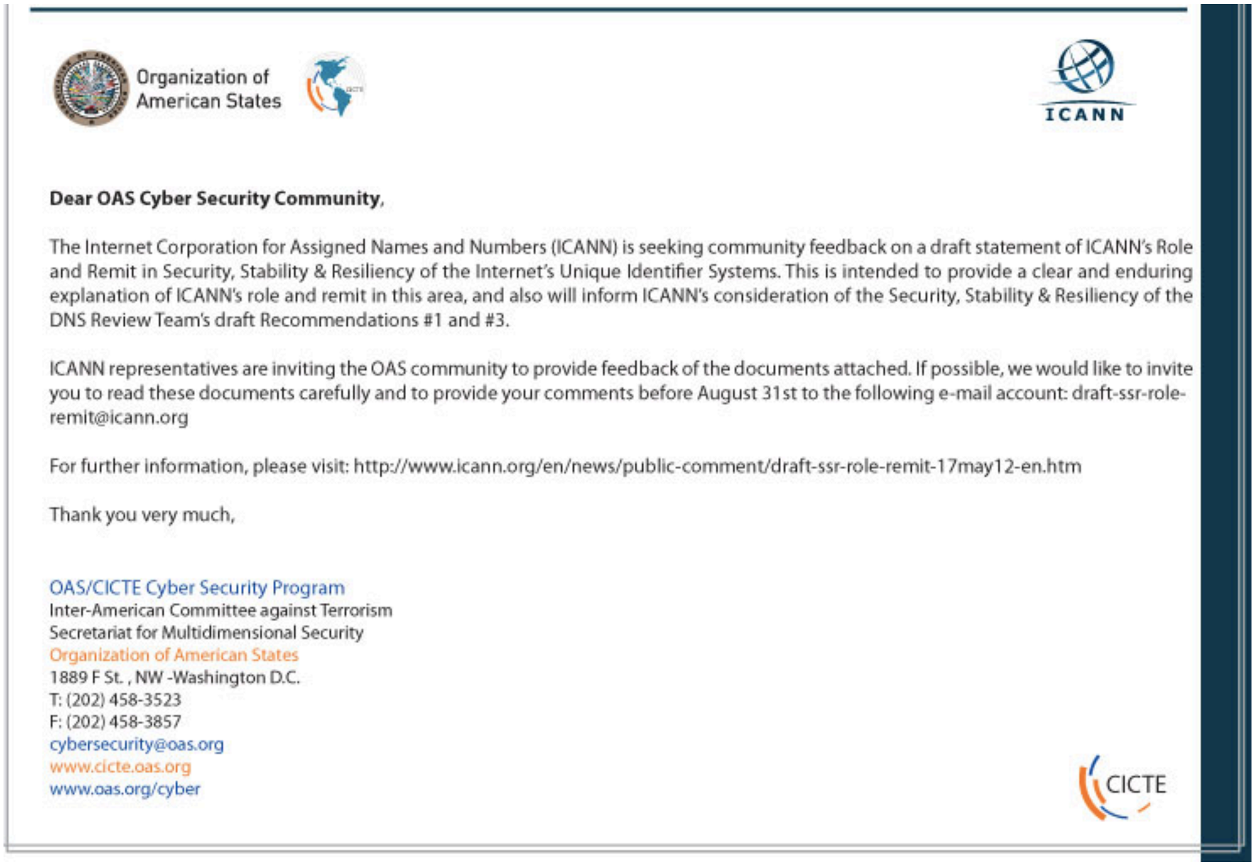
Yours,

Joseph V. Tabone

Chairman CCI Secretariat

Alfir, Reggie Miller Street, Gzira, GZR 1541, Malta | t: (356) 2132 3393 | f: (356) 2132 3390 | e: info@comnet.org.mt

Appendix C – Letter to ICANN from COMNET



Organization of American States

ICANN

Dear OAS Cyber Security Community,

The Internet Corporation for Assigned Names and Numbers (ICANN) is seeking community feedback on a draft statement of ICANN's Role and Remit in Security, Stability & Resiliency of the Internet's Unique Identifier Systems. This is intended to provide a clear and enduring explanation of ICANN's role and remit in this area, and also will inform ICANN's consideration of the Security, Stability & Resiliency of the DNS Review Team's draft Recommendations #1 and #3.

ICANN representatives are inviting the OAS community to provide feedback of the documents attached. If possible, we would like to invite you to read these documents carefully and to provide your comments before August 31st to the following e-mail account: draft-ssr-role-remit@icann.org

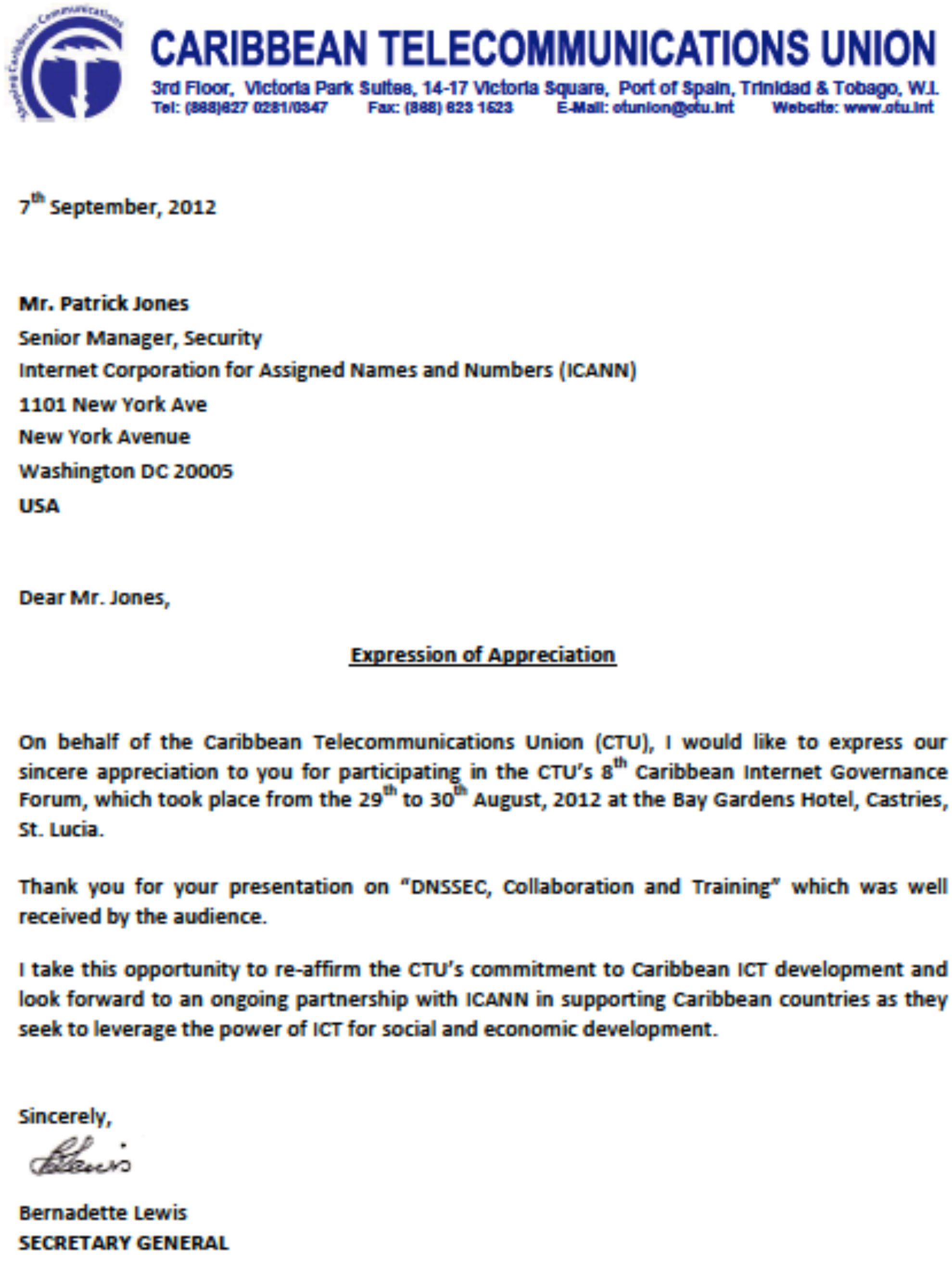
For further information, please visit: http://www.icann.org/en/news/public-comment/draft-ssr-role-remit-17may12-en.htm

Thank you very much,

OAS/CICTE Cyber Security Program
Inter-American Committee against Terrorism
Secretariat for Multidimensional Security
Organization of American States
1889 F St. , NW -Washington D.C.
T: (202) 458-3523
F: (202) 458-3857
cybersecurity@oas.org
www.cicte.oas.org
www.oas.org/cyber

CICTE

Appendix D – Request for Public Comment to OAS Community



CARIBBEAN TELECOMMUNICATIONS UNION

3rd Floor, Victoria Park Suites, 14-17 Victoria Square, Port of Spain, Trinidad & Tobago, W.I.
Tel: (868)627 0281/0347 Fax: (868) 623 1523 E-Mail: ctunion@ctu.int Website: www.ctu.int

7th September, 2012

Mr. Patrick Jones
Senior Manager, Security
Internet Corporation for Assigned Names and Numbers (ICANN)
1101 New York Ave
New York Avenue
Washington DC 20005
USA

Dear Mr. Jones,

Expression of Appreciation

On behalf of the Caribbean Telecommunications Union (CTU), I would like to express our sincere appreciation to you for participating in the CTU's 8th Caribbean Internet Governance Forum, which took place from the 29th to 30th August, 2012 at the Bay Gardens Hotel, Castries, St. Lucia.

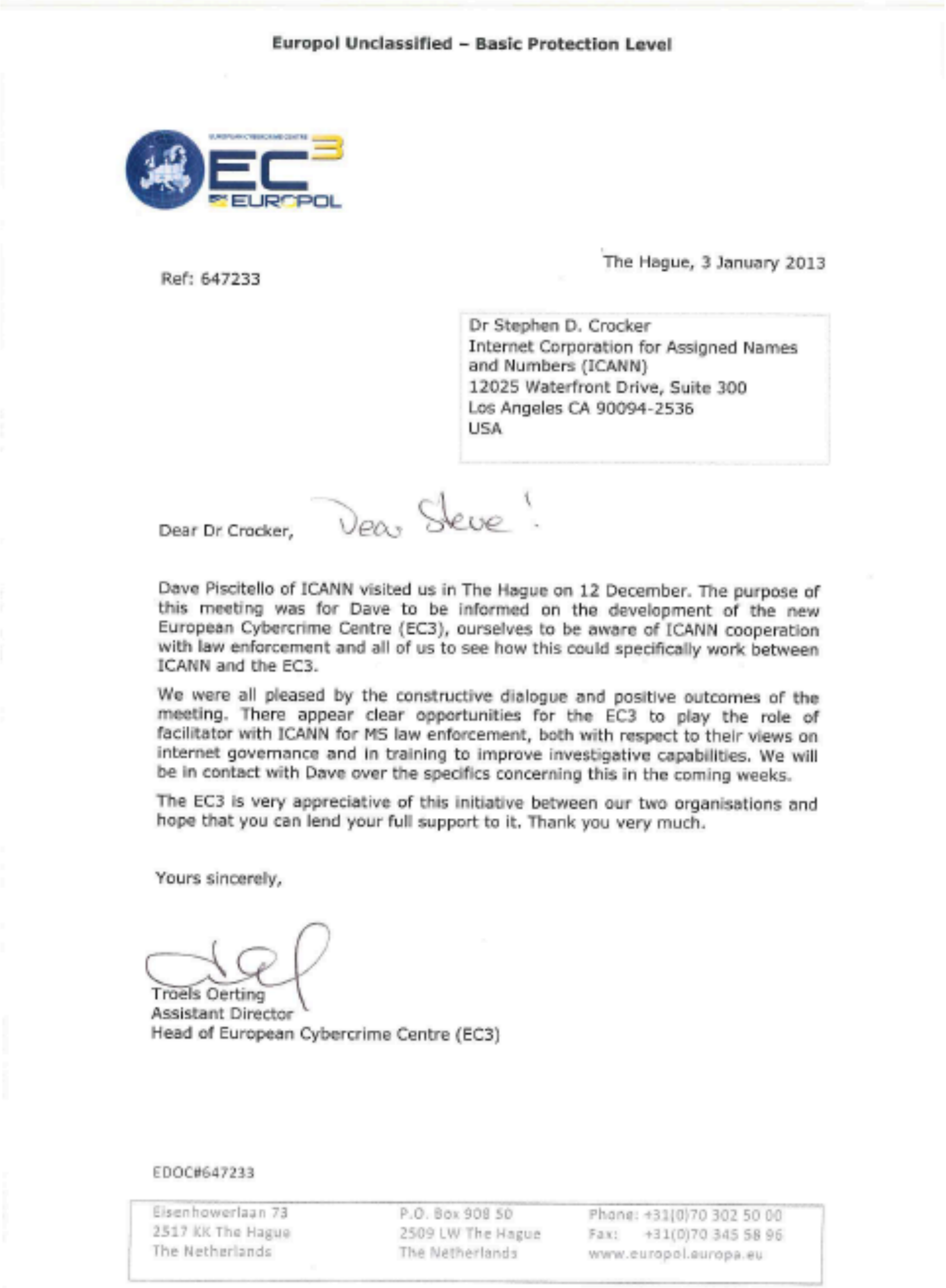
Thank you for your presentation on "DNSSEC, Collaboration and Training" which was well received by the audience.

I take this opportunity to re-affirm the CTU's commitment to Caribbean ICT development and look forward to an ongoing partnership with ICANN in supporting Caribbean countries as they seek to leverage the power of ICT for social and economic development.

Sincerely,

Bernadette Lewis
SECRETARY GENERAL

Appendix E – Letter to ICANN from Caribbean Telecommunications Union



Europol Unclassified – Basic Protection Level

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

The Hague, 3 January 2013

Ref: 647233

Dr Stephen D. Crocker
Internet Corporation for Assigned Names
and Numbers (ICANN)
12025 Waterfront Drive, Suite 300
Los Angeles CA 90094-2536
USA

Dear Dr Crocker, Dear Steve!

Dave Piscitello of ICANN visited us in The Hague on 12 December. The purpose of this meeting was for Dave to be informed on the development of the new European Cybercrime Centre (EC3), ourselves to be aware of ICANN cooperation with law enforcement and all of us to see how this could specifically work between ICANN and the EC3.

We were all pleased by the constructive dialogue and positive outcomes of the meeting. There appear clear opportunities for the EC3 to play the role of facilitator with ICANN for MS law enforcement, both with respect to their views on internet governance and in training to improve investigative capabilities. We will be in contact with Dave over the specifics concerning this in the coming weeks.

The EC3 is very appreciative of this initiative between our two organisations and hope that you can lend your full support to it. Thank you very much.

Yours sincerely,

Troels Oerting
Assistant Director
Head of European Cybercrime Centre (EC3)

EDOC#647233

Eisenhowerlaan 73
2517 KK The Hague
The Netherlands

P.O. Box 908 50
2509 LW The Hague
The Netherlands

Phone: +31(0)70 302 50 00
Fax: +31(0)70 345 58 96
www.europol.europa.eu

Appendix F – Letter to ICANN from EC3