



Identifier Systems Security, Stability and Resiliency Framework – FY 15-16

ICANN is a not-for-profit public-benefit corporation with participants from all over the world dedicated to keeping the Internet secure, stable and interoperable.

15 September 2016

Table of Contents

Executive Summary 5

Part A – Foundational Section for ICANN’s Role 6

ICANN’s Mission & Core Values 6

ICANN’s SSR Role and Remit..... 6

Definitions for this Framework..... 7

Responsibilities that lie outside ICANN’s role in SSR 8

The Challenge 8

The Internet Ecosystem and ICANN Community..... 11

Relationships in SSR..... 14

Part B – FY 15-16 SSR Module16

SSR in the ICANN Strategic Plan..... 16

Affirmation of Commitments Review 17

ICANN IS-SSR Functional Areas..... 20

How Security, Stability & Resiliency Fits into ICANN’s Functional Areas..... 21

ICANN IS-SSR Team Members 21

Engagement Criteria..... 21

International Developments 24

FY 15-16 Activities 27

Appendices30

Appendix A – FY 15-16 Identifier Systems SSR Activity Reports 30

Appendix B - SSR RT Recommendations Tracking (as of 31 December 2015) 31

List of Figures and Tables

Figure 1 - ICANN's Technical Mission7
Figure 2 - Internet Ecosystem – Logical Layer of Digital Governance Infographic 12
Figure 3 - ICANN Infographic..... 13
Figure 4 – ICANN’s Strategic Objectives (2016-2020)..... 16
Table 1 – Security Criteria for Outreach and Engagement 18
Figure 5 - ICANN Security Functional Areas 20
Table 2 – Security Criteria for Outreach and Engagement 22
Figure 6 - Composite of IS-SSR Team Activities, FY15-16 (as of December 2015) 27

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 this 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 Identifier Systems Security, Stability and Resiliency (SSR) Framework. This 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 Framework is recognized in the Affirmation of Commitments², and has been analyzed favorably by the Security, Stability and Resiliency Review Team³ as part of the Affirmation of Commitments review process.

This document is divided into two parts. Part A explains the foundation for ICANN's role in security, stability and resiliency, the Internet ecosystem, and wider community. Part B describes ICANN's strategic objectives for SSR and planned activities in the FY 15 operational year (July 2014-June 2015) into the FY 16 operational year (July 2015-June 2016).

Major changes since publication of the FY 14 Framework include implementation of the SSR Review Team's October 2012 recommendations⁴, incorporation of Unique Identifier ecosystem goals defined in ICANN's Strategic Plan 2016-2020⁵, and changes in the composition and structure of the ICANN IS-SSR team. The ICANN IS-SSR Team now reports to the office of the CTO and works in coordination with the Identifier Research team to investigate Internet Health and provide data analysis relevant to ICANN's mission. Activities in FY 15 and FY 16 continue to focus on supporting a healthy, stable, and reliable Unique Identifier ecosystem, providing the foundation for a more secure and resilient Internet for the global community.

¹ According to the ICANN bylaws at the time of this writing, ICANN coordinates the allocation and assignment of the three sets of unique identifiers for the Internet: Domain Names (forming a system referred to as DNS); Internet Protocol (IP) addresses and Autonomous System (AS) numbers; and 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>.

⁵ Strategic Plan 2016-2020, 10 October 2014, <https://www.icann.org/en/system/files/files/strategic-plan-2016-2020-10oct14-en.pdf>

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^{6,7}

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 DNS⁸ – 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

The Affirmation of Commitments calls for periodic assessment by community review teams of ICANN's progress toward four key objectives, including security, resiliency, and stability of the DNS. In its 20 June 2012 report, the first SSR Review Team issued 28 recommendations (see Appendix B). Recommendation #1 suggests that ICANN “publish a single, clear and consistent statement of its SSR remit and limited technical mission.”

A statement of ICANN’s role and remit in security, stability and resiliency of the Internet’s unique identifiers was published in May 2012⁹ and revised to reflect public comment and discussion at ICANN meetings in Prague (June 2012) and Toronto (October 2012)¹⁰. An updated statement was then published in the FY14 Framework, finalized, and posted on ICANN’s website¹¹ in January 2015.

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

Using a global multistakeholder approach, 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.

⁶ Bylaws for Internet Corporation for Assigned Names and Numbers, as amended 30 July 2014, <http://www.icann.org/en/about/governance/bylaws#>

⁷ The CCWG-Accountability document contains edits to ICANN’s Mission, see: <https://community.icann.org/display/acctcrosscomm/Development+of+Final+Report?preview=/56989168/58723253/CCWGV4-Annex%205-FinalDraftV0.5-FinalLegalReview.pdf>

⁸ “DNS” is commonly used as an abbreviation for “domain name system.” However, within the Affirmation of Commitments, “DNS” refers specifically to “domain names; Internet protocol addresses and autonomous system numbers; protocol port and parameter numbers. ICANN coordinates these identifiers at the overall level, consistent with its mission.”

⁹ Draft Statement of ICANN's Role and Remit in Security, Stability and Resiliency of the Internet's Unique Identifier Systems, 12 May 2012, <http://www.icann.org/en/news/public-comment/draft-ssr-role-remit-17may12-en.htm>

¹⁰ Revised Draft Statement of ICANN’s Role and Remit in SSR, 4 October 2012, <http://toronto45.icann.org/meetings/toronto2012/presentation-draft-ssr-role-remit-04oct12-en.pdf>

¹¹ ICANN’s SSR Role and Remit, 19 January 2015, <https://www.icann.org/resources/pages/ssr-role-remit-2015-01-19-en>

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.



Figure 1 - ICANN's Technical Mission

Definitions for this Framework

Security – the capacity to protect Internet Identifier Systems and prevent misuse.

Stability – the capacity to ensure that Internet Identifier Systems operate as expected, and that users of these systems have confidence that the systems operate as expected or intended.

Resiliency – the capacity of Internet Identifier Systems to effectively withstand, tolerate, or survive malicious attacks and other disruptive events without interruption or cessation of service.

Note: The above definitions were originally published in the FY 12 Framework. They are refined slightly here to reflect changes in terminology and the evolving threat landscape.

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), a definition of **Unique Identifier Health** was included in the FY 14 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 behavior of its parts."¹²

Responsibilities that lie outside ICANN's role in SSR

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

- ICANN does not play a role in policing the Internet or operationally combatting criminal behavior;
- 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 a 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 legally authorized actions at their request. ICANN participates with the operational security community in studying, analyzing and identifying malicious use or abuse of the DNS, and participates in collaborative mitigation efforts, including Coordinated Vulnerability Disclosure.¹³

ICANN cannot unilaterally suspend or terminate domain names. ICANN is able to enforce its contracts with third parties, including domain name registry operators and registrars.

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

The security of the overall Internet Identifier Systems is challenged by attacks against global network operations and misuse of Identifier Systems (especially the DNS). Domain name,

¹² 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/>.

¹³ Coordinated Vulnerability Disclosure at ICANN, August 2013, <https://www.icann.org/en/system/files/files/vulnerability-disclosure-05aug13-en.pdf>

Internet address, and routing system attacks target a broad range of users, individuals, businesses, civil society and governments.

As the frequency and sophistication of disruptive events and other malicious behavior increases, ICANN and the global community increasingly collaborate to work towards ensuring a healthier ecosystem by aiming to improve the security, stability, and resiliency of Internet Identifier Systems and strengthen those Systems' capabilities.

The activities enabled by the Internet reflect 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 permissionless innovation, particularly 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 governments or the private sector, do not work. Neither governments nor private sector actors 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 global collaborative, multi-party endeavor.

All parties with a stake in cybersecurity must adopt a broad 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 for the future and is healthy, stable and resilient. We need to collectively concentrate on the ecosystem's "ability to maintain its structure and function over time in the face of external stress."¹⁴

Threats against the Internet's unique Identifier Systems continue to escalate. For example, between 2014 and 2015, the overall number of distributed denial of service (DDoS) incidents doubled, including significant growth in malware DoS attacks exploiting DNS services.¹⁵ Of special note are two incidents in late 2015 during which several DNS Root Servers were targeted by DDoS attacks involving 5 million queries per second per server. These attacks were unusually successful in saturating network connections near some Root Server instances, although other instances remained continuously reachable, thereby limiting or eliminating user-visible impacts.¹⁶

In 2015, numerous high-profile DNS brand hijacking incidents were also observed. For example, a Bangladeshi hijacker known by the handle Tiger-M@TE is alleged to be responsible for several very public website defacements via ccTLD domain name hijacking, including successful attacks against Google in Malaysia, Pitcairn, and Morocco, and similar attacks against Microsoft and Kaspersky.^{17,18,19} In another example, attackers broke into the ccTLD operator for Morocco

¹⁴ Costanza and Mageau, et al.

¹⁵ Verizon Data Breach Incident Report, <http://www.verizonenterprise.com/DBIR/2015>

¹⁶ <http://www.root-servers.org/news/events-of-20151130.txt>

¹⁷ Google Malaysia get Hacked, <http://www.deccanchronicle.com/150414/technology-science-and-trends/article/google-malaysia-gets-hacked-bangladeshi-hacker-tiger>

¹⁸ Google CO and PN Hacked by Tiger-M@TE, <https://www.informationlord.com/google-co-pn-hacked-by-tiger-mte-major-security-breach/>

where domain.ma, google.co.ma, google.ma, microsoft.ma and kaspersky.ma domains are hosted, defacing websites associated with these five domain names.

Botnet threats continue to evolve and grow. Starting with Conficker²⁰, ICANN and some of its contracted parties have participated in efforts to dismantle global botnets such as the GameOver ZeuS ransomware botnet.²¹ Botnet takedown activities have often involved thousands of domain names, delegated from numerous TLD registries, requiring cooperation and coordination between private sector actors, law enforcement, and justice communities worldwide.²²

Identifier system threats extend beyond the DNS. For example, the Border Gateway Protocol (BGP) is used to exchange routing and reachability information among autonomous systems on the Internet. From configuration errors and human mistakes to malicious attacks, 2015 saw several noteworthy BGP hijackings and service disruptions. In November 2015, BGP hijacks caused large scale Internet outages in Azerbaijan and India.^{23, 24} In June 2015, a massive BGP route leak allegedly caused by Telekom Malaysia significantly degraded global Internet routing for about two hours, resulting in a significant portion of global Internet traffic to be dropped and users worldwide to experience slow Internet service.²⁵

Government intervention saw users lose connectivity to the outside world, for example in reaction to widespread political protests in the Republic of Congo.²⁶ Government blocking of social media also continues to grow.²⁷ Earthquakes in Nepal and Vanuatu also significantly impacted Internet connectivity in those countries, showing the power of natural disasters on global networks.^{28,29}

While the DNSSEC adoption rate by browser and application developers and registrants remains low, the percentage of gTLDs supporting DNSSEC has grown significantly with the delegation of many new gTLDs.

Additional trends have been observed:

¹⁹ Google Microsoft and Kaspersky Morocco Hacked, <https://www.hackread.com/google-microsoft-kaspersky-morocco-hacked/>

²⁰ Conficker Summary and Review, ICANN, May 2010, <https://www.icann.org/en/system/files/files/conficker-summary-review-07may10-en.pdf>

²¹ U.S. Leads Multi-National Action Against “Gameover Zeus” Botnet and “Cryptolocker” Ransomware, June 2014, <http://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware>

²² Shadowserver Botnet Statistics, <https://www.shadowserver.org/wiki/pmwiki.php/Stats/BotnetCharts>

²³ Country-wide Outage in Azerbaijan, <http://www.bgpmon.net/country-wide-outage-in-azerbaijan>

²⁴ Large Scale BGP Hijack Out of India, <http://www.bgpmon.net/large-scale-bgp-hijack-out-of-india>

²⁵ Massive Route Leak Causes Internet Slowdown, <http://www.bgpmon.net/massive-route-leak-cause-internet-slowdown>

²⁶ Congo Government Allegedly Shuts Off Internet Service to Squash Protests, <http://motherboard.vice.com/read/congo-government-allegedly-shuts-off-internet-service-to-squash-protests>

²⁷ Six countries that block social media, <http://www.businessinsider.com/the-six-countries-that-block-social-media-2015-4>

²⁸ Earthquake rocks Internet in Nepal, <http://research.dyn.com/2015/04/earthquake-rocks-internet-in-nepal/>

²⁹ Earthquake hits off Vanatu, <http://www.news.com.au/national/major-73-earthquake-hits-off-vanuatu-no-tsunami-warning/news-story/83ea3d689a92c2dca8debe2a25734907>

- Continued growth in adoption of DNSSEC by TLD operators³⁰ and resolvers³¹, as well as increasing DNSSEC adoption in delegated domain names^{32,33}
- Expansion of root server instances worldwide³⁴
- Delegation of new ccTLDs – both Internationalized Domain Name and non-IDN ccTLDs – in a growing number of languages and character sets³⁵
- Launch of the new gTLD program in 2013, leading to delegation of hundreds of new gTLDs³⁶
- 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.^{37,38} The NetMundial Global Multistakeholder Statement (April 2014) recognized the Internet as a global resource that must be managed in the public interest.³⁹ “As a universal global resource, the Internet should be a secure, stable, resilient, reliable and trustworthy network. Effectiveness in addressing risks and threats to security and stability of the Internet depends on strong cooperation between different stakeholders.”

The Internet is also recognized as fundamental for supporting the world’s economy and sustainable development. According to the OECD, almost all businesses now rely on Information and Communication Technologies, with 76 percent of enterprises now having a web presence.⁴⁰ Furthermore, network connectivity contributes broadly to national economic health, as demonstrated by countries with greater openness on the Internet scoring better on the “Economic Impacts” pillar of the World Economic Forum’s Networked Readiness Index (NRI).⁴¹

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

³⁰ Daily TLD DNSSEC Report, http://stats.research.icann.org/dns/tld_report/

³¹ <http://stats.labs.apnic.net/dnssec>

³² Third Party DNS operator to Registrars/Registries Protocol , Internet Draft, January 2016,

<https://tools.ietf.org/html/draft-latour-dnsoperator-to-rrr-protocol-01>

³³ Announcing Universal DNSSEC: Secure DNS for Every Domain, CloudShare, November 2015,

<https://blog.cloudflare.com/introducing-universal-dnssec/>

³⁴ RootServers.org Website, <http://www.root-servers.org/>

³⁵ <http://icannwiki.com/CcTLD>

³⁶ <http://newgtlds.icann.org/en/>

³⁷ UNESCO Vancouver Declaration, September 2012,

http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/mow/unesco_abc_vancouver_declaration_en.pdf

³⁸ 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

³⁹ NetMundial Global Multistakeholder Statement, 24 April 2014, <http://netmundial.br/netmundial-multistakeholder-statement/>.

⁴⁰ OECD Digital Economy Outlook 2015,

<http://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm>

⁴¹ Open for Business, Dalberg, 2014, http://www.dalberg.com/documents/Open_for_Business_Dalberg.pdf

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.

As illustrated in the figure below, the Internet's logical infrastructure is what delivers “One Internet” for the world through Unique Identifiers (Names, Numbers, and Protocol Parameters). ICANN helps coordinate the administration of this logical layer of digital governance in partnership with other technical communities throughout the Internet Ecosystem to ensure the security, stability, resiliency, and integrity of the Internet.

THE LOGICAL LAYER OF DIGITAL GOVERNANCE

Layered on top of the Physical Infrastructure's thousands of networks and satellites, the Internet's Logical Layer is what delivers One Internet for the world through Unique Identifiers (Names, Numbers, and Protocol Parameters). ICANN coordinates the administration of this layer in partnership with other technical communities to ensure the security, stability, resiliency, and integrity of this critical layer.

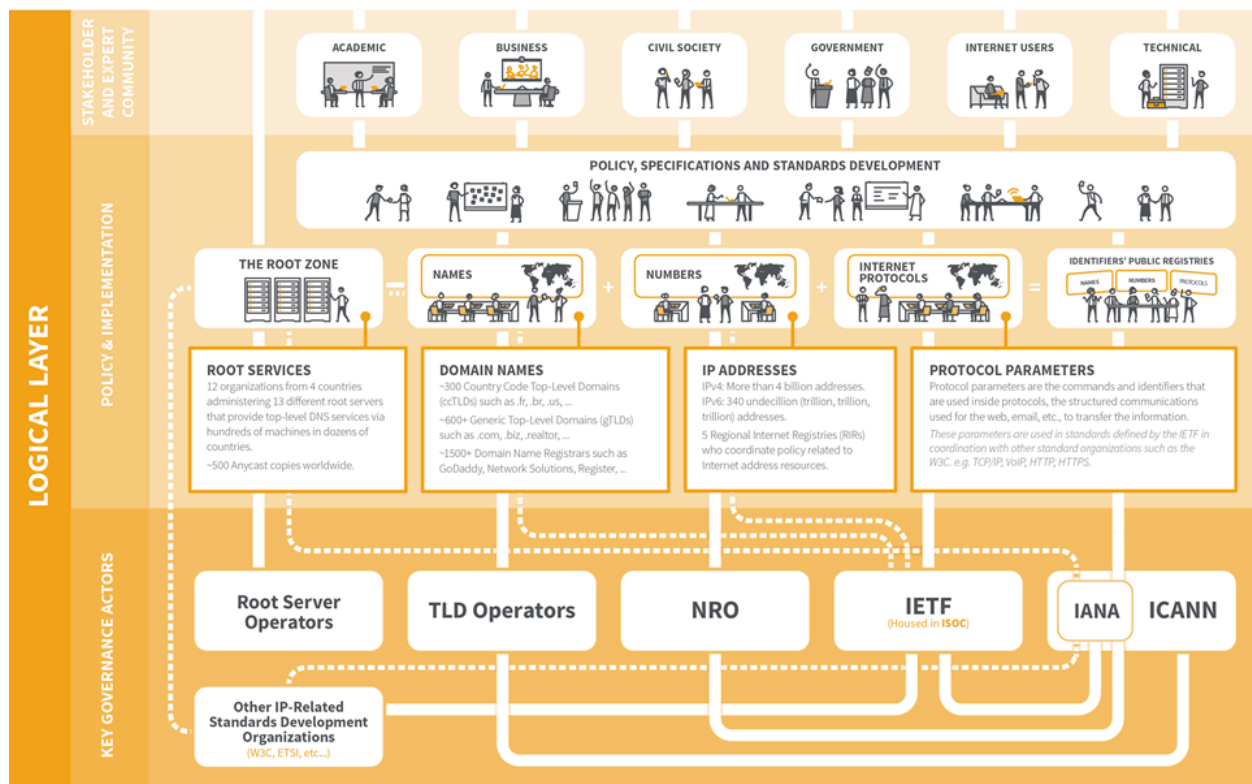


Figure 2 - Internet Ecosystem – Logical Layer of Digital Governance Infographic⁴²

⁴² Three Layers of Digital Governance, ICANN, August 2015, https://wiki.icann.org/download/attachments/31262295/Three_Layers_Digital_Governance_EN_print.pdf

From an ICANN perspective, the Internet Ecosystem can be viewed as:

- 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 Systems for the sharing of knowledge, commerce and innovation, but may not be aware of or participate in ICANN.

The ICANN community contains the 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 staff who support the greater ICANN community and multistakeholder coordination of the Internet's unique identifiers.

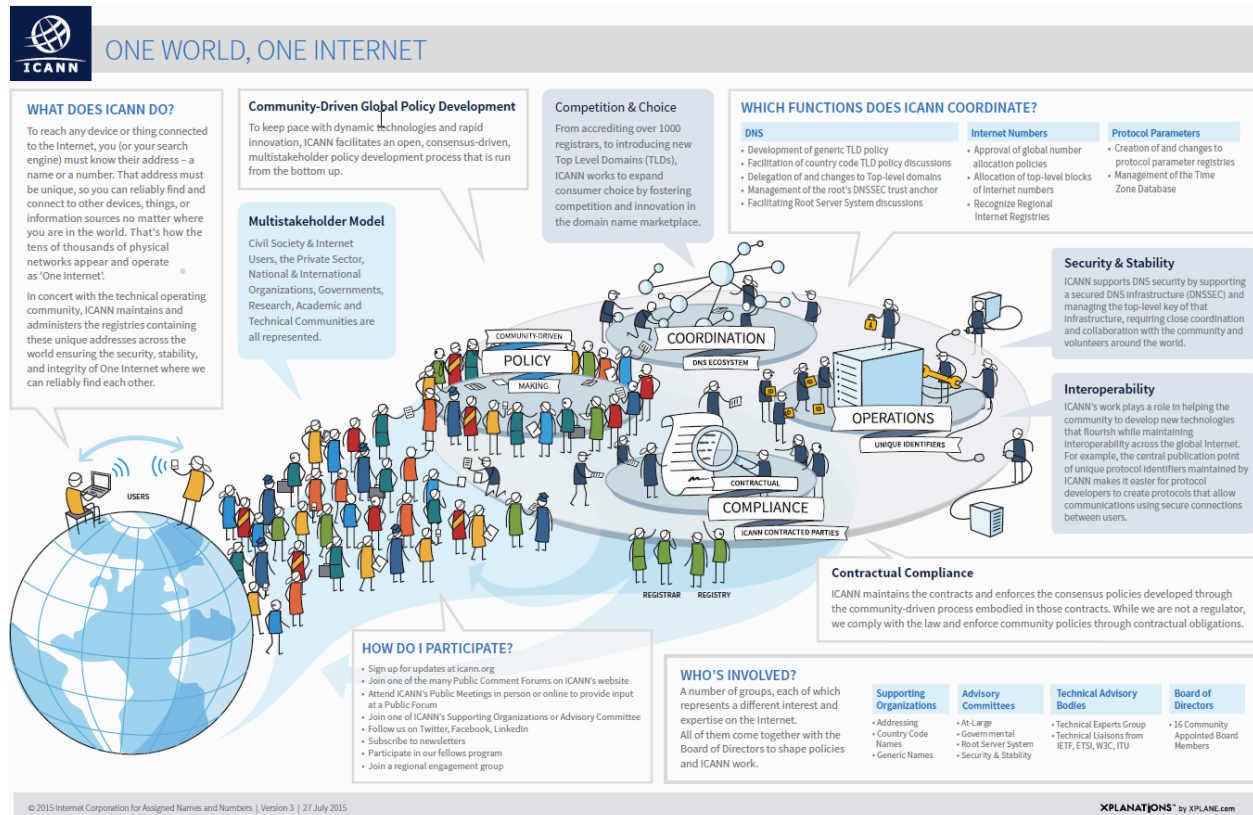


Figure 3 - ICANN Infographic⁴³

The community participates in ICANN in many ways, including Advisory Committees, and Supporting Organizations. Information on Advisory Committees (ACs) can be found on their pages below:

⁴³ What Does ICANN Do, Version 3, 27 July 2015, is available as full 11x17 infographic in 6 languages here: <https://community.icann.org/display/gsecomms/Speakers+Bureau+Handouts>

- At Large Advisory Committee (ALAC) - <http://www.atlarge.icann.org/alac>
- Governmental Advisory Committee (GAC) - <https://gacweb.icann.org/>, including the Public Safety Working Group (PSWG) recently created to advise on aspects of ICANN’s policies and procedures that implicate the safety of the public
- Root Server System Advisory Committee (RSSAC) - <http://www.icann.org/en/groups/rssac>
- Security and Stability Advisory Committee (SSAC)- <http://www.icann.org/en/groups/ssac>

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

Associated policy development derives from three Supporting Organizations (SOs):

- Address Supporting Organization (ASO) - <http://aso.icann.org/> (IP addresses)
- Country Code Names Supporting Organization (ccNSO) - <http://ccnso.icann.org/> (ccTLDs)
- Generic Names Supporting Organization (GNSO) – <http://gnsso.icann.org> (gTLDs)

Since ICANN’s formation in 1998, the DNS has grown from several hundred thousand domain names, distributed among seven generic top-level domains (gTLDs) and approximately 250 country-code TLDs (ccTLDs), into an increasingly large and complex ecosystem with approximately 299 million domain names⁴⁴ across more than 800 delegated gTLDs and 300 ccTLDs⁴⁵ used by over 3 billion Internet users.⁴⁶

Relationships in SSR

Parties involved in making decisions related to the global technical coordination of the Internet’s unique identifiers must work together to ensure that all such decisions are made in the public interest and are accountable and transparent.

ICANN maintains relationships with contracted parties (domain name registries and registrars, escrow providers and others), and partnerships, memoranda of understanding (MOU), 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. ICANN’s major agreements and related reports are published at this link: <https://www.icann.org/en/about/agreements>.

As part of implementing SSR Review Team Recommendation 4, ICANN has defined and publicized many of its SSR relationships within the ICANN community, and will update these periodically to keep pace with SSR activities. ICANN has also signed MOUs (posted on the agreements page mentioned previously) indicating roles and responsibilities for SSR. These steps help provide a single focal point for understanding the interdependencies between the various organizations and entities, within their respective roles. Further efforts are now

⁴⁴ Domain Name Industry Brief, 3Q15, http://www.verisign.com/en_US/innovation/dnib/index.xhtml

⁴⁵ Delegations as of December 2015; <http://www.iana.org/domains/root/db> and <https://newgtlds.icann.org/en/program-status/statistics>

⁴⁶ Internet Society Global Internet Report 2015, http://www.internetsociety.org/globalinternetreport/assets/download/IS_web.pdf

underway to provide more detail on formal relationships that ICANN has with key organizations, and to extract and catalogue SSR-related elements of MOUs.

As part of implementing SSR Review Team Recommendation 5, ICANN has also reported on its progress towards SSR-related Key Success Factors (KSFs) and Key Performance Indicators (KPIs) involving SSR relationships. As standard operating procedure, this progress is reflected in ICANN's regular project management reports, operating plans, SSR quarterly reports, and this Framework. These steps help ICANN to maintain effective working arrangements in support of ICANN's SSR goals and strategic objectives for the Unique Identifier ecosystem.

Part B – FY 15-16 SSR Module

This section of the Identifier Systems Security, Stability and Resiliency Framework centers on projected Identifier Systems SSR (IS-SSR) activities and initiatives for Fiscal Year 2015, covering the period from 1 July 2014 to 30 June 2015 and Fiscal Year 2016, covering the period from 1 July 2015 to 30 June 2016.

SSR in the ICANN Strategic Plan

In October 2014, ICANN published a new Strategic Plan for fiscal years 2016-2020.⁴⁷ As illustrated below, the ICANN Strategic Plan identifies a healthy, stable, and resilient Unique Identifier ecosystem as one of five strategic objectives for the organization. This aligns with the high importance given to SSR in the Affirmation of Commitments and shows support for the technical engagement provided by ICANN’s IS-SSR Team.

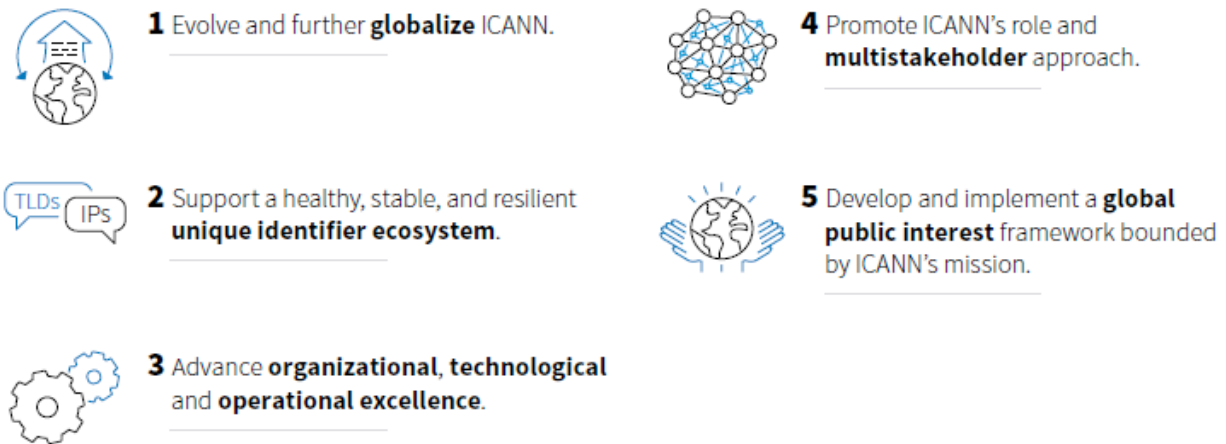


Figure 4 – ICANN’s Strategic Objectives (2016-2020)

As described by the 2016-2020 Strategic Plan, the ecosystem of cooperating parties faces immense change while seeking to define itself, evolve, and contend with increased misuse or abuse of Internet’s unique Identifier Systems. The activity on the Internet reflects the full range of human motivations, conduct, conflict, and misconduct. The open nature of the Internet has made it successful, enabled innovation at its edge, and allowed for the sharing of knowledge, creativity and commerce in a global commons. However, this openness has also created opportunities for the Internet to be exploited for a wide range of abuses and unintended uses.

By the end of 2013, there were more mobile devices than people on the planet. By the end of 2020, it is estimated there will be as many as one trillion “things” connected to the Internet, many using the DNS and IP addresses as a platform for a range of services for the world’s users. This will expand the very nature of the Internet from an on-demand human service to an always on, near continuous use service for sensors and machines.

⁴⁷ Strategic Plan 2016-2020, 10 October 2014, <https://www.icann.org/en/system/files/files/strategic-plan-2016-2020-10oct14-en.pdf>

New use of domain names, including new TLDs, are driving change and expansion – inspiring new Internet applications, but also creating the possibility of consumer confusion and introducing new challenges in security and stability at all levels of the hierarchical system. A challenge will be to concentrate on the ecosystem’s resilience and ability to maintain its structure and function over time in the face of external stress.

By contrast, the rise of apps for mobile devices (having reached 45 billion downloads in 2013 and expected to reach 350 billion by 2018) is putting the future and even relevance of domain names in question⁴⁸, while heightening the importance of IP addresses in the background as unique identifiers to connect users to their intended destination in a global interoperable Internet. The exhaustion of IPv4, and either the gradual migration to IPv6 or the increased use of address sharing techniques, will result in changes to the addressing ecosystem that will affect how addresses are used and managed.

The growing and evolving unique Identifier Systems ecosystem is operating within that changing landscape. In accordance with the Strategic Plan, ICANN will engage stakeholders to help support and plan for the industry’s evolution and empower a global and responsible industry that fosters growth and innovation.

To advance this strategic objective, ICANN’s 2016-2020 Strategic Plan seeks to:

1. Foster and coordinate a healthy, secure, stable, and resilient identifier ecosystem
2. Proactively plan for changes in the use of unique identifiers and develop technology roadmaps to help guide ICANN activities
3. Support the evolution of domain name marketplace to be robust, stable and trusted

Each of these activities is associated with key success factors (outcomes) and strategic risks, further detailed in the Strategic Plan 2016-2020.

Affirmation of Commitments Review

The Affirmation of Commitments, signed by ICANN and the US Department of Commerce on 30 September 2009,⁴⁹ 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.” The SSR Review Team’s findings and recommendations

⁴⁸ Mobile applications “embed” the serving endpoint’s identification, while shortened URLs obscure underlying domain names. These trends, combined with greater user interface emphasis on icons and voice activation, are diminishing the value of imprinting brands within domain names.

⁴⁹ Affirmation of Commitments, 30 September 2009, <http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm>

are documents in the team’s Final Report.⁵⁰ The ICANN Board of Directors approved the final report and recommendations in October 2012.⁵¹

The SSR Review Team’s 28 recommendations, listed below, are aligned with ICANN’s Management Delivery structure, as follows:

- ICANN Remit and Mission [Recommendations 1, 2, 18, 24]
- Internationalization [Recommendations 3, 4, 5, 14, 16]
- Multistakeholder Model Evolution [Recommendations 6, 12, 13, 23]
- Operations Excellence [Recommendations 7, 8, 9, 10, 11, 22, 15, 19, 25, 26, 27, 28, 17, 20, 21, 23]

ICANN continues to move forward with implementation of these SSR Review Team recommendations. As of 31 December 2015,⁵² implementation has been completed for 16 of the Review Team’s 28 recommendations.

Table 1 – Security Criteria for Outreach and Engagement

Rec #	Description
1	ICANN should publish a single, clear and consistent statement of its SSR remote and limited technical mission.
2	ICANN’s definition and implementation of its SSR remit and limited technical missions should be reviewed in order to maintain consensus and elicit feedback from the Community.
3	Once ICANN issues a consensus-based statement of its SSR remit and limited technical missions, ICANN should utilize consistent terminology and descriptions of this statement in all materials.
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.
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.
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.
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.
8	ICANN should continue to refine its Strategic Plan objectives, particularly the goal of maintaining and driving DNS availability, with clear alignment of Framework and Strategic Plan.
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.

⁵⁰ SSR RT Final Report, June 2012, available in 5 languages at <https://www.icann.org/resources/pages/documents-88-2012-05-31-en>

⁵¹ ICANN Board Resolution, 18 October 2012, <http://www.icann.org/en/groups/board/documents/resolutions-18oct12-en.htm#1.e>

⁵² SSR Review Implementation Reports, posted quarterly at <https://community.icann.org/display/SSR/SSR+Review+Implementation+Home>

-
- 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 compliance issues and investigations.
-
- 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.
-
- 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.
-
- 13 ICANN should encourage all Supporting Organizations to develop and publish SSR-related best practices for their members.
-
- 14 ICANN should ensure that its SSR-related outreach activities continuously evolve to remain relevant, timely and appropriate.
-
- 15 ICANN should act as a facilitator in the responsible disclosure and dissemination of DNS security threats and mitigation techniques.
-
- 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.
-
- 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.
-
- 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.
-
- 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 execution of its SSR responsibilities.
-
- 20 ICANN should increase the transparency of information about organization and budget related to implementing the SSR Framework and performing SSR-related functions.
-
- 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.
-
- 22 ICANN should public, monitor and update documentation on the organization and budget resources needed to manage SSR issues in conjunction with introduction of new gTLDs.
-
- 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.
-
- 24 ICANN must clearly define the charter, roles and responsibilities of the Chief Security Office Team.
-
- 25 ICANN should put into place mechanisms for identifying both near and longer-term risks and strategic factors in its Risk Management Framework.
-
- 26 ICANN should prioritize the timely completion of a Risk Management Framework.
-
- 27 ICANN's Risk Management Framework should be comprehensive within the scope of its SSR remit and limited missions.
-
- 28 ICANN should continue to actively engage in threat detection and mitigation, and participate in efforts to distribute threat and incident information.
-

For the remainder of FY 15 through FY 16 and the start of the next SSR Review process, ICANN will track its implementation of these recommendations, along with the other Affirmation of Commitments reviews, in accordance with Accountability Mechanisms.⁵³

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>.

ICANN IS-SSR Functional Areas

As part of explaining ICANN’s role and remit, the following graphic identifies and expands upon the four functional areas addressed by ICANN IS-SSR to enable the security, stability, and resiliency of the Unique Identifier ecosystem.

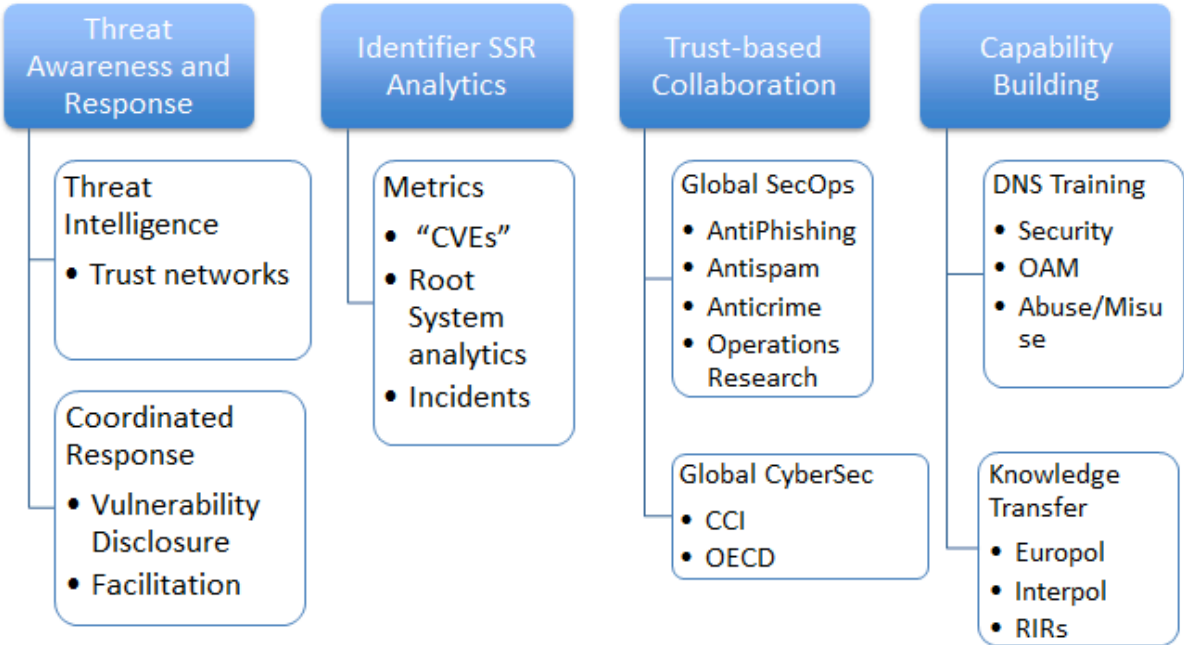


Figure 5 - ICANN Security Functional Areas

This graphic shows the primary functional areas addressed by ICANN IS-SSR:

- Facilitate awareness of and preparedness for responding to threats against the Internet’s unique identifiers;
- In cooperation with the ICANN Research Team and under the direction of the Chief Technology Officer, develop SSR-related metrics and analytics for unique Identifier Systems, such as root system measurements and analysis of DNS or registration abuse and misuse;
- Maintain Trust-based Collaboration and coordination with Global Cybersecurity partners through ICANN Global Stakeholder engagement, daily interaction with DNS operators, first responders, governments and law enforcement, and academia and research communities; and

⁵³ ICANN Accountability Mechanisms, <http://www.icann.org/en/news/in-focus/accountability>

- Enable DNS security capability building by providing subject matter expertise in technical engagement, including training and knowledge transfer.

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

SSR at ICANN can be viewed as

- A Core Value for ICANN, in the Affirmation of Commitments
- One of the Five Strategic Objectives identified by ICANN's Strategic Plan
- An overall thematic area, cutting across the organization
- A department within ICANN
- An essential element in ICANN projects and activities

ICANN IS-SSR is a distributed team, with global reach and expertise in technical and technology policy issues impacting the Internet's unique Identifier Systems. The IS-SSR 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. The team serves as a bridge between DNS operators, the technical community, law enforcement, the operational security community, and stakeholder groups.

ICANN IS-SSR Team Members

As of publication of this document, the IS-SSR Team includes:

- [John Crain](#), Chief Security, Stability and Resiliency Officer: Team Lead & Member of ICANN Executive Team; Lead on Threat Awareness & Monitoring and Root Server representative on the DNS-OARC Board; reporting to David Conrad, Chief Technology Officer
- [Geoff Bickers](#), Director of Security Operations: Corporate Security Programs, Meetings Security, liaison with the ICANN Information Technology Department; reporting to CISO
- [Dave Piscitello](#), Vice President of Security & Information and Communications Technology (ICT) Coordination: Technical Engagement, training & thought leadership; Lead with law enforcement & operational security community; member of Executive Management Group for the Commonwealth Cybercrime Initiative; member of Anti-Phishing Working Group (APWG) Steering Committee, Associate Fellow at the Geneva Center for Security Policy
- [Richard Lamb](#), Senior Manager, DNSSEC Programs: Technical Engagement in DNSSEC adoption & training; collaboration with community on DNSSEC; Policy Management and Practices for DNSSEC deployment
- [Carlos Alvarez, CFE](#), Senior Manager, Security Engagement: Technical Engagement with law enforcement on cybercrime, training, collaboration with operational security community
- [Steve Conte](#), Training Coordination, Senior Manager: Coordinates ICANN SSR training across the globe

Engagement Criteria

In February 2012, the IS-SSR team formalized its criteria for outreach and engagement. The criteria have been influential in other parts of ICANN and is intended to provide guidance to

ICANN’s IS-SSR team and Executive Management on the types of collaborative and community activities supported by the IS-SSR team.

Table 2 – Security Criteria for Outreach and Engagement

Types of Events	Examples
ICANN Public Meetings	ICANN Los Angeles, Singapore, Buenos Aires, Dublin, Marrakech
ICANN Internal Meetings	Executive Meeting, IS-SSR Team, Board Workshop, Staff Training, Budget, Other
Meetings relevant to operational aspects of ICANN/IANA/L-root/DNSSEC, etc Meetings where ICANN collaborates on global threats/mitigation	IETF, DNS-OARC, RIPE NCC, NOGs, SSAC, RSSAC, LACNIC, LACTLD, BlackHat, InterOp, RSA, others APWG, MAAWG, cyber exercises, OAS, INTERPOL Global Cybercrime Expert Group (IGCEG), Europol, US FBI InfraGuard, APT-CST, APAC-FCACP, OSCE
Technical Engagement – Trainings & Capability Building	Attack & Contingency Response training (ACRP), Secure Registry Ops, DNSSEC, Law Enforcement & Govt, Commonwealth Cybercrime Initiative, Stop. Think.Connect Program, Secure The Human Project, ICANN Train-the-Trainers Program
Symposia, Invited SME conferences, continuing education	South School on Internet Governance, Dominios Latinoamerica, Security Analysts Summit Latin America, Mesa de Gobernanza de Internet
Engagement in Ecosystem, Multistakeholder model	IGF & regional IGFs, regional and national CERTs, European Commission, Organization for the Security and Cooperation in Europe, OECD
Engagement Criteria ✓	
Does the event support ICANN’s SSR strategic objective?	<ol style="list-style-type: none"> 1. Foster and coordinate a healthy, secure, stable, and resilient identifier ecosystem 2. Proactively plan for changes in the use of unique identifiers and develop technology roadmaps to help guide ICANN activities 3. Support the evolution of domain name marketplace to be robust, stable and trusted
Does the event fit within one of the following functional areas:	<ol style="list-style-type: none"> 1. Threat Awareness and Response 2. Identifier SSR Analytics 3. Trust-based Collaboration 4. Capability Building
Is the event in support of a partnership, MOU or stakeholder relationship?	
Does the event 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?

As part of ICANN’s matrix structure, the IS-SSR 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 IS-SSR team appear below:

- IETF Meetings
- CIS Registries Meeting in Budva, Montenegro
- DNS training with the National Crime Agency and Office of Fair Trading in London, UK
- DNS abuse training to police cybercrime units in Chile, Peru, Costa Rica, Colombia and Argentina
- DNSSEC training in various events worldwide
- DNS capability building training with LACTLD in St. Maarten & Paraguay
- MENOG in Dubai
- LACNIC/LACNOG in Uruguay and Colombia
- DNS training with Europol
- MAAWG, APWG, RIPE NCC and DNS-OARC
- OAS CICTE & World Economic Forum on Principles for Cyber Resilience
- APNIC, APTLD & APRICOT
- Providing talks via remote presentation, such as Georgetown University’s Center for Intercultural Education and Development Cyber Security Program, OAS/CITEL, LACRALO, and the Universidad de los Andes

A key part of the technical engagement provided by the IS-SSR 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
- Identifier Systems Fundamentals for government or ministerial level stakeholders

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

The IS-SSR Team engaged in significant international activity during FY 15-16, as follows.

Capability Building. ICANN’s IS-SSR Team delivers half-, full, or multi-day training programs with live demonstrations of techniques and hands-on learning opportunities. In 2H 2014 and 2015, the team provided 104 training programs in numerous regions (NA, SA, LAC, EU, AF, ME/IN, AP). The DNS abuse/misuse program – now more advanced, spanning multiple days - continues to be the most popular training session. Requests for DNSSEC training also remained strong. In 1H15, the IS-SSR Team partnered with RIPE NCC and LACNIC to deliver multi-day Identifier System Abuse training.

Training Trainers. Numerous requests from South America and Asia Pacific Regions were able to be satisfied as a result of previous “Train-the-Trainer” efforts in those regions. In 1H15, the IS-SSR Team, cooperating with partners at Network Startup Resource Center (NSRC), conducted a pilot Train-the-Trainer course on DNS Operations in Dubai, UAE, teaching ten individuals from the Middle East and African regions. In 2H15, we conducted a Train-the-Trainer course for the Centre for Development of Advanced Computing (C-DAC), teaching twenty individuals from various institutions in India. The intent of these efforts is to seed regions with subject matter expertise and eventually have these partners deliver training in local languages. Based on these initial successes, another Train-the-Trainer course will be held for the Asia/Pacific region in 2H16. In January 2016, the IS-SSR Team also began DNS investigations training at CERT-UK, shadowed by CERT-UK trainer candidates.

Zone Signing by ccTLDs. DNSSEC zone signing continues to grow, supported in part by IS-SSR DNSSEC training sessions across the globe. In 2014, .ad, .au, .aw, .es, .gd, .hr, .id, .ie, .ke, .no, .pe, .sj, .tn, and .vu signed their zones. The IS-SSR Team also supports a DNSSEC Status Page, as well as a Resource Page that offers public root key rollover testing.

Strengthening Relationships with Security Communities. During FY 15-16, the IS-SSR Team took advantage of its membership in M3AAWG, the Messaging, Malware and Mobile Anti-Abuse Working Group, to work more closely with global email and Internet service providers. ICANN greatly benefitted from these relationships when the company fell victim to a series of phishing attacks: the generous offers for assistance to mitigate and investigate these attacks illustrates that trust-based collaboration benefits organizations in many ways.

The team also helped to update ‘Operation Safety Net: Best Practices to Address Online, Mobile and Telephony Threats,’ a document prepared by M3AAWG and the London Action Plan.⁵⁴ ICANN’s continued participation in M3AAWG has led to IS-SSR Team members joining M3AAWG’s Public Policy and Technical committees and exploring further opportunities to contribute to Identifier Systems security, stability, and resilience. We now have steering committee responsibilities for both the APWG and APWG EU and established new working relationships with the Geneva Centre for Security Policy (GCSP), complementing our sustained relationships illustrated in Table 1.

⁵⁴ Operation Safety Net: Best Practices to Address Online, Mobile and Telephony Threats, https://www.m3aawg.org/Operation_Safety-Net

Grow Threat Intelligence Reporting. During FY 15-16, the IS-SSR Team continued to assist with or facilitate introductions among appropriate parties on a wide set of awareness reporting and response activities, including inquiries related to alleged 2013 RAA violations, advice in preparing court orders and Expedited Registry Security Request (ERSR) waivers, or where the public safety community seeks assistance in communicating the gravity of a malicious activity to a registrar so that the registrar may take appropriate voluntary action. In fact, the number of inquiries or requests for IS-SSR Team assistance doubled in 1H 2015, illustrating how dramatically cyber incidents spiked in 2015. Threats ranged from malicious registration, domain hijacking, and Identifier System DDoS to assistance with policy matters and registration issues. For example, following multi-party investigations of attacks against ccTLD authoritative name servers (ICANN, NSRC, MarkMonitor), the IS-SSR Team gathered input from investigating parties and published a Top Level Domain Incident Response “Recovery Checklist” and presented this during the ICANN Dublin CCNSO Tech Day.⁵⁵

Reinforcing ICANN Community Relationships. IS-SSR Team staff continue to use the persistent interest in cybersecurity as a segue to promote ICANN and multistakeholder approaches to governance when they present or train at engagements arranged by GSE and through relationships with cybercrime initiatives, network operations groups, ccTLDs, and RIRs. In 2H 2014 and 1H 2015, the team satisfied 106 engagement requests. Many of these engagements were collaborations with governance, ministerial, policy, or cybersecurity communities. Many others were coordinated or jointly attended with GSE staff. Noteworthy among these activities were:

- Invited participation at the Munich Security Conference (Germany)
- Invited presentations at the NASK Internet Policy Conference (Poland)
- Invited presentations at the American University of Science and Technology in Beirut and the Lebanese Internet Center (Lebanon)
- Invited presentations at the International Security and Diplomacy in Cyberspace (Colombia)
- DNS abuse training, co-organized with the Organization of American States and Interpol in Buenos Aires, attended by law enforcement cybercrime unit representatives from 18 countries from Latin America and the Caribbean
- iLAC Roadshow (Bolivia)
- DNS Forum (Turkey)
- National Conference on Cybersecurity (Sri Lanka)
- Cybersecurity Event, meetings with Bulgarian Deputy Ministers of Communications, Interior (Bulgaria)
- Meetings with vice ministers of ICT and the telecommunications regulatory authorities from Bolivia and Costa Rica
- PACNOG Conference (New Zealand)
- APriIGF, APRIGF (India)
- Indonesia Stakeholder Engagements (Indonesia)
- TAG DNSSEC Workshop
- LACTLD Technical Training (Brazil)

⁵⁵ Top Level Domain Incident Response “Recovery Checklist”,
<https://www.icann.org/en/system/files/files/tld-ir-checklist-01sep15-en.pdf>

- Diplo Summer School Program (Serbia)
- Investigating DNS Workshop (Romania, Colombia, Chile, Argentina, Bolivia, Costa Rica)
- An Identifier Systems and Cybercrime Workshop for European Commission Directorates General (Belgium)
- Multi-day training open to all branches of UK law enforcement at ICDDF (UK)
- Cyber Secure Pakistan Workshops for cybercrime investigators, technical and academic communities, and the Pakistan Telecommunications Authority (ME)
- Presentations and workshops at DEFTcon, La Sapienza University, and for Italian law enforcement (Italy)
- South School on Internet Governance and Dominios Latinoamérica (Costa Rica)
- A joint IS-SSR Team and GSE collaboration and training exercise with law enforcement in Tonga, Kiribati, and Fiji (APAC)
- Workshop to Government of India Security Advisors, Investigators, and Law Enforcement (India)
- Workshops for CERT, ISP, and law enforcement in Cairo (Egypt)
- National ICT Conference (Montenegro)
- Direct engineering assistance to .TR, .CR and .AR (Argentina)
- Network Security Workshop in collaboration with WorldBank & APNIC (MM)
- APCERT Conference (MY)
- Security Analysts Summit Latin America (Chile)

Program for GSE/IS-SSR Engagement Tracking. With the deployment of our engagement tracking software, the IS-SSR Team has been able to work with GSE (Global Stakeholder Engagements) to facilitate relevant training and engagement with sufficient lead time to provide proper planning and cost-efficient travel. This program also increased our ability to engage in “events of opportunity” where ICANN Regional VPs can help the IS-SSR Team engage with other individuals, events, or governments while team members are on the ground in a given country or region. Careful planning has also allowed the IS-SSR Team to maximize the benefit of international travel, increasing engagements with ICANN communities or stakeholders at reduced travel time and expense.

Remote Delivery. During FY 15-16, the IS-SSR Team delivered 9 webinars as part of its experiment with remote delivery, along with a remote broadcast of a live training session. While interest in remote delivery is high, so too are the technical challenges. The IS-SSR Team is continuing to investigate the viability of offering remote training as one piece of its overall international engagement puzzle.

Security and Technology Awareness Raising Activities. In 2H15, the IS-SSR Team began a series of monthly blog posts intended to de-mystify Internet and cybersecurity terminology for readers across the globe. As part of the Office of the CTO’s (OCTO) mission to increase technical expertise and awareness in the ICANN community, the OCTO Team, of which the IS-SSR Team is a part, rolled out a series of “How it Works” tutorials to increase the technical foundation of knowledge for those who attend ICANN meetings. To date, tutorials have covered the Internet Engineering Task Force (IETF), Internet routing basics, protocols used when operating a DNS registry, and a history and overview of the Root Server Operating System provided by root server operators. The IS-SSR team also continued periodic training for ICANN staff and delivered

phishing awareness and Identifier Systems basics training to staff in the US and Brussels, with Istanbul and Singapore offices scheduled for early 2016.

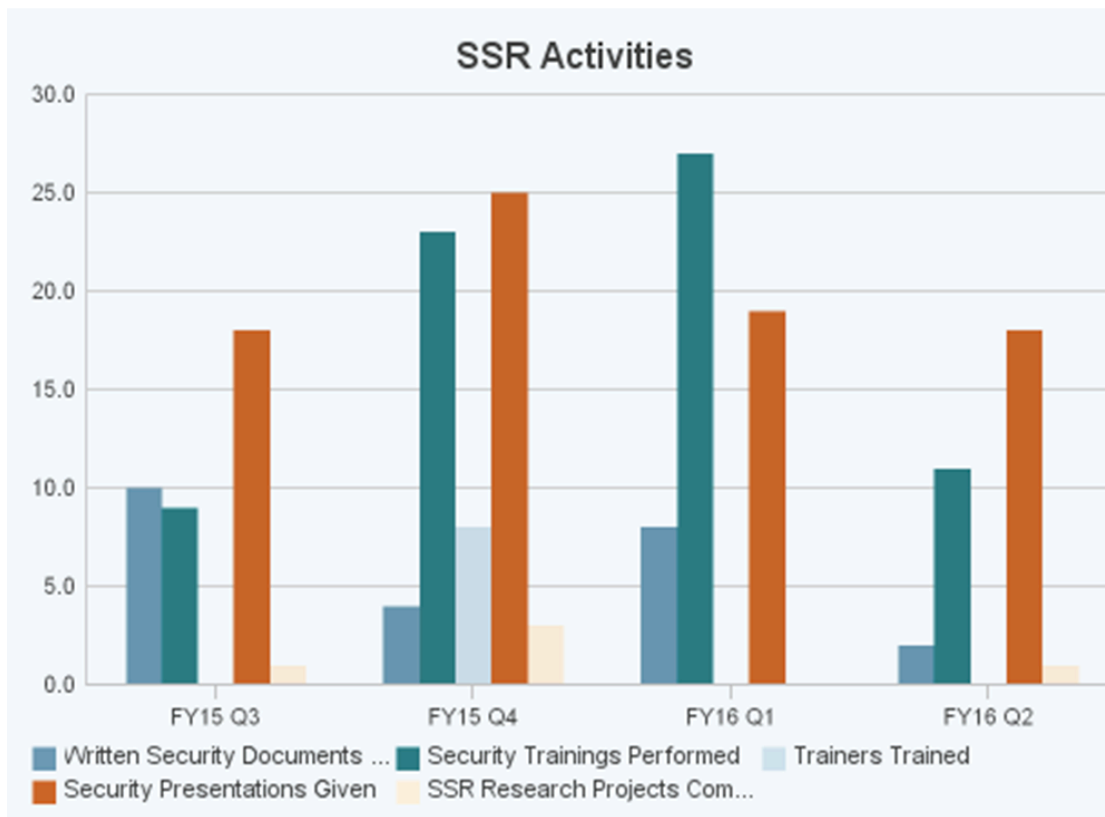


Figure 6 - Composite of IS-SSR Team Activities, FY15-16 (as of December 2015)

FY 15-16 Activities

For FY 15-16, ICANN’s activities supporting a secure, stable and resilient Unique Identifier ecosystem centered on the:

- Support Operational Excellence in activities led by IANA, IT, DNS Ops, and Global Domains Division
- Support ICANN’s research team’s Identifier Technologies Health Indicators development
- Develop proof of concept data analytics for tracking, measuring, or reporting domain name and registration service misuse or abuse
- Provide Technical Engagement (through subject matter expertise and thought leadership, community engagement, conducting Identifier Systems training and capability building activities where requested)
- Develop “force multiplier” relationships with CERT or other stakeholders to expand the pool of experienced and qualified trainers of capability building programs created by the IS-SSR Team
- Encourage adoption and awareness of DNSSEC by enterprises, users and operators

- Review and implement SSR Review Team recommendations
- Support further L-root capacity, publication of data and measurement by ICANN's DNS Operations team
- Support ICANN hub office locations in Singapore and Istanbul and expand the IS-SSR Team's capabilities in those locations to better serve the community
- Serve as a resource for the Global Stakeholder Engagement team in Internet governance and cybersecurity discussions, representing ICANN in conferences and meetings
- Facilitate and encourage broader participation from the law enforcement and operational security community in ICANN; in particular, through the Public Safety Working Group (PSWG) of the Government Advisory Committee (GAC).
- Engage 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)
- Strengthen ICANN's internal networks, IT processes and information security
- Raise ICANN staff security awareness through training, make security awareness resources available to the ICANN community
- Collaborate with the technical community, root server operators, application and browser developers on Identifier Systems issues
- Draft mitigation plans for some of the risks included in ICANN's DNS Risk Matrix
- Support ICANN's Policy and Stakeholder Relations teams where needed (SSAC, RSSAC, and SSR issues when discussed in SOs and ACs)
- Support ICANN meetings in Los Angeles, Singapore, Buenos Aires, Dublin, and Marrakech by providing DNS, technical and security subject matter expertise for Newcomer, Fellowship, Public Safety, and How It Works programs. Participate in Supporting Organization (GNSO, ccNSO) and Advisory Committee (GAC, ALAC, SSAC, RRSAC) activities, where invited.

In order to deliver on these initiatives, ICANN evolved its IS-SSR Team in FY 15 with additional expertise and skills.

The vision of the IS-SSR Team is to be a trusted partner in multi-stakeholder, collaborative efforts to ensure the security, stability, and resiliency of the Internet's unique Identifier Systems.

The mission of the IS-SSR Team is to preserve the security, stability and resiliency of the Internet's system of unique identifiers that ICANN helps coordinate, to promote user confidence and trust in these systems, and to strengthen these systems through capability building among the communities ICANN serves.

The IS-SSR Team contributes to achieving the overall mission of the Office of the CTO (OCTO): to constantly improve knowledge about the identifiers ICANN helps coordinate; to disseminate this information to the Internet community; and to improve the technical operation of the Internet's system of unique identifiers in order to improve ICANN's technical stature. To do so, the IS-SSR Team collaborates with OCTO Research Team, which is responsible for researching

issues related to the Internet's system of unique identifiers, improving the security, stability, and resiliency of those identifiers, and providing internal and external Internet Technology Resources.

Appendices

Appendix A – FY 15-16 Identifier Systems SSR Activity Reports

As part of ICANN's continuing commitment to transparency and accountability, ICANN's IS-SSR Department publishes periodic reports, describing the activities performed by the IS-SSR Team to maintain the security, stability, and resiliency of the Internet's unique Identifier Systems. These activities include collaboration with ICANN, security and operations, and public safety communities.

The 2H 2014 activities report highlights IS-SSR Team collaboration and stakeholder activities from July 1 through December 31, 2014:

<https://www.icann.org/en/system/files/files/is-ssr-update-s2-2014-21jan15-en.pdf>

The 1H 2015 activities report covers the period January 1 through June 30, 2015.

<https://www.icann.org/en/system/files/files/is-ssr-update-1h-2015-20jun15-en.pdf>

The 2H 2015 activities report covers the period July 1 through December 31, 2015.

<https://www.icann.org/en/system/files/files/is-ssr-update-2h-2015-26feb16-en.pdf>

Appendix B - SSR RT Recommendations Tracking


Below are the most recent quarterly implementation reports for the SSR RT recommendations.

SSR RT Implementation Reports, including this one, are posted quarterly at <https://community.icann.org/display/SSR/SSR1+Review+Implementation+Home>

SSR Recommendation 1 Implementation

ICANN's SSR Remit and Limited Technical Mission
30 June 2015

Implementation 1 Timeline



Publish remit


Status of Deliverables

	Responsible	Due Date
Post public comment	Staff	✓
Incorporate into SSR Framework	Staff	✓
Publish SSR remit	Staff	✓

Complete
 Planned/in Process
 Behind schedule, expected to recover within original plan
 Behind schedule, original plan to be adjusted

Recommendation 1 Implementation Description

ICANN should publish a single, clear and consistent statement of its SSR remit and limited technical mission.



1

SSR Recommendation 1 Implementation

ICANN's SSR Remit and Limited Technical Mission
30 June 2015


Project Status

Public comment was taken on a [draft statement between May-Sept 2012](#); it was subsequently [revised in Oct 2012](#).

The updated [statement](#) was published on ICANN's website and incorporated in the [FY 14 SSR Framework](#) and is part of SSR SOP in which SSR Framework and statement is periodically reviewed and updated as needed. This statement also has been incorporated into other ICANN documentation.

Implementation Notes

This recommendation is complete.



2

SSR Recommendation 2 Implementation

ICANN's SSR Remit and Limited Technical Mission
30 June 2015

Implementation 2 Timeline



Recommendation 2 Implementation Description

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.

Status of Deliverables

	Responsible	Due Date
Reflect ICANN's strategic SSR objectives, goals and key success factors (KSFs) in the Strategic Plan for FY2016–2020	Staff	✓
Include SSR key performance indicators (KPI's), dependencies, five-year phasing and portfolios in the Five-Year Operating Plan	Staff	✓
Include details on proposed SSR activities and expenditures in the Annual Operating Plan & Budget	Staff	✓
Periodically review SSR Framework, including the SSR role and remit statement	Staff	✓

- Complete
- Planned/In Process
- Behind schedule, expected to recover within original plan
- Behind schedule, original plan to be adjusted

1



SSR Recommendation 2 Implementation

ICANN's SSR Remit and Limited Technical Mission
30 June 2015

Project Status

The [statement](#) (and [SSR Framework](#)) informed ICANN's new [Strategic Plan for FY2016–2020](#), which reflects strategic SSR objectives, goals and key success factors (KSFs) for the next five years and was result of input and review by the ICANN community, Staff and Board. SSR elements are highlighted [here](#).

This, in turn, informed the new [Five-Year Operating Plan](#), which also was developed with community input and includes SSR key performance indicators (KPIs), dependencies, five-year phasing, and portfolios. SSR elements are highlighted [here](#).

The Annual Operating Plan & Budget, which is derived from the Five-Year Operating Plan and from community input, is being developed for FY16 and will include details on proposed SSR activities and expenditures. More information is posted [here](#).

Periodic review of the SSR Framework, including the SSR role and remit statement, are part of the SSR SOP, and also will be reviewed by the next SSR RT in 2015.

This is a recurring component as ICANN continues to refine the scope of its SSR activities (within its mission) to meet changing demands. The new structure of the Identifier System Security, Stability and Resiliency Team (ISSSR, previously the ICANN Security team) and ICANN's new Chief Technology Officer help ensure ICANN's SSR remit and scope continually evolves.

Implementation Notes

This recommendation is complete.

2



SSR Recommendation 3 Implementation

ICANN's SSR Remit and Limited Technical Mission
30 June 2015

Implementation 3 Timeline



Consistent terminology and descriptions

Recommendation 3 Implementation Description

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.

Status of Deliverables

	Responsible	Due Date
Publicize consistent terminology and descriptions related to ICANN's SSR role and remit	Staff	✓
Add key terms to ICANN's public glossary on an ongoing basis as part of SOP; as SSR activities evolve, terminology and descriptions will be updated as part of SOP.	Staff	✓

Complete
 Planned/In Process
 Behind schedule, expected to recover within original plan
 Behind schedule, original plan to be adjusted



1

SSR Recommendation 3 Implementation

ICANN's SSR Remit and Limited Technical Mission
30 June 2015

Project Status

Consistent [terminology and descriptions](#) related to ICANN's SSR role and remit have been publicized and are encouraged in all ICANN material.

Key terms are added to ICANN's public [glossary](#) on an ongoing basis as part of SOP. As SSR activities evolve, terminology and descriptions will be updated as part of SOP.

Implementation Notes

This recommendation is complete.



2

SSR Recommendation 4 Implementation

ICANN's SSR-Related Roles and Responsibilities
30 June 2016

Implementation 4 Timeline



Recommendation 4 Implementation Description

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.

Status of Deliverables

	Responsible	Due Date
Update ISSR Team SOP work based on SSR activities	Staff	✓
(Phase I) Post Memorandums of Understanding that indicate roles and responsibilities relevant to SSR	Staff	✓
(Phase II) Provide additional detail on formal relationships ICANN has with key organizations	Staff	✓
(Phase II) Extract and catalogue SSR-related elements of MOUs	Staff	Sept 2016

Complete
 Planned/In Process
 Behind schedule, expected to recover within original plan
 Behind schedule, original plan to be adjusted



1

SSR Recommendation 4 Implementation

ICANN's SSR-Related Roles and Responsibilities
30 June 2016

Project Status

- (Phase I) Many of ICANN's SSR relationships have been [defined and publicized](#). As part of ISSR Team SOP, this work will be [updated periodically](#) to keep pace with SSR activities.
- (Phase I) Memorandums of Understanding that indicate roles and responsibilities relevant to SSR have been signed with numerous entities; the list is posted [here](#) and will be updated as part of SOP, as needed.
- (Phase II) Extract and catalogue SSR-related elements of MOUs; Target completion date: September 2016.
 - Work is underway to capture and publish all the SSR-related MOUs and publish the information on the IS-SSR web site once the inventory has been completed
- (Phase II) In development stage – building on above, provide additional detail on formal relationships ICANN has with key organizations. This includes: 1) defining "relationship," covering informal and formal arrangements; 2) documenting that some relationships are sensitive (not disclosed) and noting the industry best practices and conventions that are used to address this lack of disclosure. Target completion date for phase II details: September 2016.
- [ICANN Security Awareness Resource Locator Developed](#) - All stakeholders should learn how to protect themselves, their families, or their organizations against online threats. The resources on this page can help consumers, business or IT professionals avoid online threats or harm and make informed choices regarding (personal) data disclosure or protection.

Implementation Notes

This recommendation is in progress with Phase II estimated delivery expected by September 2016 to complete this recommendation.



2

SSR Recommendation 5 Implementation

ICANN's SSR-Related Roles and Responsibilities
30 June 2016

Implementation 5 Timeline



Status of Deliverables

	Responsible	Due Date
(Phase I) Report on ICANN's progress toward SSR-related KSFs and KPIs involving SSR relationships	Staff	✓
(Phase II) Include information on how key relationships noted in Recommendation 4 are used to achieve SSR goals (as part of SOP) in next SSR Framework/report on SSR activities	Staff	Dec 2015

Recommendation 5 Implementation Description

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.

- Complete
- Planned in Process
- Behind schedule, expected to recover within original plan
- Behind schedule, original plan to be adjusted



1

SSR Recommendation 5 Implementation

ICANN's SSR-Related Roles and Responsibilities
30 June 2016

Project Status

- (Phase I) Reporting on ICANN's progress toward SSR-related KSFs and KPIs involving SSR relationships is SOP, and can be found in ICANN's regular project management reporting, operating plans, [SSR Framework](#), and SSR quarterly reports.
- (Phase II) Next SSR Framework/report on SSR activities will include information on how key relationships noted in Recommendation 4 are used to achieve SSR goals (as part of SOP). Revised target completion date: September 2016.
 - SSR Framework for 2015 under development with expected publication date September 2016.

Implementation Notes

This recommendation is in progress with Phase II estimated delivery expected by September 2016 to complete this recommendation.



2

SSR Recommendation 6 Implementation

ICANN's SSR-Related Roles and Responsibilities
30 June 2015

Implementation 6 Timeline



SSR Roles and Responsibilities

Recommendation 6 Implementation Description

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. ICANN should seek consensus for this across both groups, recognizing the history and circumstances of the formation of each. ICANN should consider appropriate resourcing for both groups, consistent with the demands placed upon them.

Status of Deliverables

	Responsible	Due Date
Reflect roles and responsibilities of SSAC in ICANN's Bylaws and defined in SSAC's Operating Procedures	Staff	✓
Reflect roles and responsibilities for RSSAC in an updated charter contained in ICANN's Bylaws	Staff	✓
Reflect SSAC and RSSAC roles and responsibilities in a brief explanatory text for icann.org (linking to respective charters), and text as agreed to by the AC's chairs	Staff	✓

Complete
 Planned in Process
 Behind schedule, expected to recover within original plan
 Behind schedule, original plan to be adjusted



1

SSR Recommendation 6 Implementation

ICANN's SSR-Related Roles and Responsibilities
30 June 2015

Project Status

- Roles and Responsibilities of SSAC are reflected in ICANN's Bylaws and defined in SSAC's [Operating Procedures](#).
- Roles and Responsibilities for RSSAC are reflected in an updated charter contained in [ICANN's Bylaws](#).
- SSAC and RSSAC have been asked to reflect their roles and responsibilities in a brief explanatory text for [icann.org](#) (linking to respective charters), and [text](#) as agreed to by the AC's chairs. April 2015

Implementation Notes

This recommendation is complete.



2

SSR Recommendation 7 Implementation

ICANN's SSR Framework and Strategic Plan
30 June 2016

Implementation 7 Timeline



Clear SSR objectives and priorities

Recommendation 7 Implementation Description

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.

Status of Deliverables

	Responsible	Due Date
Incorporate SSR Framework and reflect SSR priorities, objectives and activities into standard operating procedures for development of ICANN plans and budgets	Staff	✓
Report on SSR-related priorities, objectives and activities on regular basis as part of SOP, including in ICANN's regular portfolio management reporting and SSR quarterly reports	Staff	✓
Improve and publish process for establishing updated SSR priorities and objectives	Staff	✓
Publish Annual SSR Framework Report	Staff	Target Feb. 2016 for 2015 Report

Complete
 Planned/In Process
 Behind schedule, expected to recover within original plan
 Behind schedule, original plan to be adjusted



1

SSR Recommendation 7 Implementation

ICANN's SSR Framework and Strategic Plan
30 June 2016

Project Status

[Note: Recommendation was made before ICANN's current planning, budgeting and portfolio/project management and reporting processes were instituted].

- The Strategic and Operating Plans (see Recommendation 2) were informed by SSR Framework and reflect SSR priorities, objectives and activities. This is SOP for development of ICANN plans and budgets.
- SSR-related priorities, objectives and activities are reported on regularly as part of SOP, including in ICANN's regular [portfolio management reporting](#) and SSR [quarterly reports](#).
- Revamped process for establishing updated SSR priorities and objectives. The ICANN Security, Stability and Resiliency department documented its [Mission, Approach, Tasks](#) in its August 2015 blog.
- Release of 2015 [SSR Annual Framework report](#), target February 2016, current estimate for release of report is August 2016.

Implementation Notes

This recommendation is in progress with Report expected to be announced and published August 2016



2

SSR Recommendation 8 Implementation

ICANN's SSR Framework and Strategic Plan
30 June 2015

Implementation 8 Timeline



Status of Deliverables

	Responsible	Due Date
Incorporate SSR Framework and reflect SSR priorities, objectives and activities into standard operating procedures for development of ICANN plans and budgets	Staff	✓
Report on SSR-related priorities, objectives and activities on regular basis as part of standard operating procedures, including in ICANN's regular portfolio management reporting and SSR quarterly reports	Staff	✓

Recommendation 8 Implementation Description

ICANN should continue to refine its Strategic Plan objectives, particularly the goal of maintaining and driving DNS availability. Clear alignment of Framework & Strategic Plan.

- Complete
- Planned/In Process
- Behind schedule, expected to recover within original plan
- Behind schedule, original plan to be adjusted



1

SSR Recommendation 8 Implementation

ICANN's SSR Framework and Strategic Plan
30 June 2015

Project Status

The Strategic and Operating Plans (see Recommendation 2) were informed by SSR Framework and reflect SSR priorities, objectives and activities. This is SOP for development of ICANN plans and budgets, in which SSR alignment is reviewed as annual plans/budgets are developed.

Progress on SSR-related priorities, objectives and activities are reported on regularly as part of SOP, including in ICANN's regular [portfolio management reporting](#) and SSR [quarterly reports](#)

Implementation Notes

This recommendation is complete.



2

SSR Recommendation 9 Implementation

ICANN Operational Responsibilities
30 September 2015

Implementation 9 Timeline



Status of Deliverables

	Responsible	Due Date
Implement DNSSEC in the root	Staff	✓
Incorporate SSR-related certification into EFQM program	Staff	✓

Recommendation 9 Implementation Description

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.

- ✓ Complete
- Planned in Process
- Behind schedule, expected to recover within original plan
- Behind schedule, original plan to be adjusted



1

SSR Recommendation 9 Implementation

ICANN Operational Responsibilities
30 September 2015

Project Status

ICANN's implementation of DNSSEC in the root has [achieved SysTrust certification](#).

Staff certification options initially focused on ITIL certification of DNS engineering staff. SSR-related certification effort subsequently incorporated into EFQM program in April 2015. Closure date TBD as part of EFQM RADAR evaluation schedule (FY15).

ICANN launched its [EFQM web page](#) where the focus is on continuous improvement. The EFQM Excellence Model provides mechanisms for the holistic assessment of an organization. These assessments help improve the way ICANN works, so that it can deliver better results.

Implementation Notes

This recommendation is complete.



2

SSR Recommendation 10 Implementation

ICANN Operational Responsibilities
30 June 2015

Implementation 10 Timeline



Status of Deliverables

	Responsible	Due Date
Report compliance activities as part of standard operating procedures	Staff	✓
<ul style="list-style-type: none"> Migrate complaints icann.org and automated Launch bulk complaint tool Implement Pulse Survey Launch WHOIS inaccuracy qualities check Create complaints submission processes & FAQs to address new 2013 RAA requirements Launch compliance auditing and outreach programs Create new positions to ensure fulfillment of goals and objectives in this area 	Staff	✓

Recommendation 10 Implementation Description

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 compliance issues and investigations.

- Complete
- Planned/In Process
- Behind schedule, expected to recover within original plan
- Behind schedule, original plan to be adjusted



1

SSR Recommendation 10 Implementation

ICANN Operational Responsibilities
30 June 2015

Project Status

[Note: As Review Team noted, this Recommendation is more fully addressed in the WHOIS Review]

Regular public reporting of compliance activities are part of SOP; detailed information is available [here](#).

Complaints migrated to icann.org and automated; bulk complaint tool launched; Pulse Survey implemented; WHOIS inaccuracy qualities check launched; complaints submission processes & FAQs to address new 2013 RAA requirements completed; compliance auditing and outreach programs in place; new positions created to ensure fulfillment of goals and objectives in this area.

Implementation Notes

This recommendation is complete.



2

SSR Recommendation 11 Implementation

ICANN Operational Responsibilities
30 June 2016

Implementation 11 Timeline



Recommendation 11 Implementation Description

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.

Status of Deliverables

	Responsible	Due Date
Identify and implement measures of success for new gTLDs and IDN fast track that expressly address SSR-related program objectives	Staff	Oct 2015
Include operations that support SSR objectives in new gTLDs as part of standard operating procedures, including: <ul style="list-style-type: none"> Service Level Agreements and monitoring Emergency back-end registry operators and data escrow Trademark Clearinghouse Root zone scaling management DNSSEC-related activities Compliance Department activities 	Staff	✓
Organize two panels for security and stability review for all applied-for labels	Staff	✓
Incorporate security and stability evaluation mechanisms for applied-for IDN labels across the new gTLD and IDN ccTLD Fast Track Programs	Staff	✓

Complete
 Planned/In Process
 Behind schedule, expected to recover within original plan
 Behind schedule, original plan to be adjusted



1

SSR Recommendation 11 Implementation

ICANN Operational Responsibilities
30 June 2016

Project Status

Effort has been underway to identify and implement measures of success for new gTLDs and IDN fast track that expressly address SSR-related program objectives. Examples of key activities that are being factored in are included below. Target completion date for implementation schedule: Closure date estimated March 2016.

- Operations that support SSR objectives in new gTLDs are part of ICANN's SOP, including Service Level Agreements and monitoring, emergency back-end registry operators and data escrow, Trademark Clearinghouse, root zone scaling management, DNSSEC-related activities, and Compliance Dept. activities.
- Implementation is underway for (IAG-CC) metrics on the impact of the New gTLD Program on competition, consumer trust, and consumer choice, which has SSR-related elements; this supports the upcoming CCT Review. ICANN commissioned [third-party research](#) that supports the IAG-CC work.
- Specification 11 of the Registry Agreement signed by all new gTLD registries requires technical analysis and reporting on security threats, and a framework is under development. The targeted schedule of deliverables for the [Framework Drafting Team](#) is as follows:
 - 29 Jan. 2016 - Release of Framework revised with input received during public comment period.
- For the new gTLD Program [Application Guide Book](#), two separate panels were organized for security and stability review for all applied-for labels, focused on: (i) security and stability evaluation of the strings, and (ii) string similarity review against existing, reserved and applied-for labels.
- Security and stability evaluation mechanisms for applied-for IDN labels across the new gTLD and IDN ccTLD Fast Track Programs are in place. As defined in the [Final Implementation Plan](#), the IDN ccTLD Fast Track Program includes a two-panel mechanism for technical string evaluations, including the DNS Stability Panel.
- For both IDN gTLDs & ccTLDs, the [Label Generation Rule set \(LGR\)](#) for the root zone is developed to have a conservative mechanism to define IDN TLD labels, focused on DNS stability and security. [Guidelines for Designing Script-Specific Label Generation Rules \(LGR\) for the Root Zone](#)
- The IDN ccTLD Fast Track Process is reviewed annually and includes SSR components.
- [Coordinated Vulnerability Disclosure Reporting at ICANN](#)

As part of addressing recommendation and its implementation a report is under development to inventory numerous activities within multiple ICANN departments that have the potential to support to-be-defined SSR objectives for new gTLD and IDN fast track programs.

- ICANN 55 [Root Stability Study Workshop](#)

A review of the New gTLD Program for security and stability impact is a previous commitment based on advice from the GAC and other discussions. The vendor contracted to conduct this study presented their methodology for conducting this review and invited feedback from interested stakeholders.

Implementation Notes

This recommendation is in progress, work has been divided into two phases and both reports are expected to be published by September 2016



2

SSR Recommendation 12 Implementation

ICANN Areas of Influence as a Coordinator, Collaborator and Facilitator
30 June 2016

Implementation 12 Timeline



Recommendation 12 Implementation Description

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.

Status of Deliverables

	Responsible	Due Date
Identify and/or establish "best practices," and integrate those best practices into agreements into which ICANN enters	Staff	Oct 2015
Maintain resource locator page to support ICANN community member security awareness	Staff	✓
Inform SOS/ACs of best-practices and invite these groups to identify additional, targeted best-practices for their constituents.	Staff	✓
Address SSR-related practices in MOUs with numerous international entities	Staff	✓
Emphasize SSR responsibilities and best practices in Regional Engagement Strategies	Staff	✓
Work with Anti-Phishing Working Group (APWG) Internet Policy Committee to publish recommendations for web application protection and development of resources for security awareness	Staff	✓
Include additional SSR best practices language in revised new gTLD registry agreement	Staff	✓

- ✓ Complete
- Planned in Process
- Behind schedule, expected to recover within original plan
- Behind schedule, original plan to be adjusted



Date



SSR
ICANN
30 Jun
Imple

Recommendation 13 Implementation Description

Engage in a variety of ongoing activities to encourage global use of SSR best practices

Staff



ICANN
Orga
best

SSR Recommendation 12 Implementation

ICANN Areas of Influence as a Coordinator, Collaborator and Facilitator
30 June 2016

Project Status

Staff has been working with a number of SSR-related bodies in the wider Internet community (described below) to identify and/or establish "best practices," and have been working to integrate those best practices into agreements into which ICANN enters.

○ Staff is assessing the range of activities underway that advance identification and communication of SSR-related best practices, and will institute an updated and holistic approach to identifying and supporting the implementation of best practices. This information will be captured in a report. Target completion date currently March 2016, report is currently slated for release the end of May 2016

ICANN staff has a resource locator [page](#) that the Security Team maintains to support ICANN community member security awareness. The page identifies web sites, organizations, and government resources, in some cases in multiple languages, that have developed security awareness education, training, and best practices or guidelines for individuals and members of collaborative communities. Additional information related to best practices is linked [here](#) and [here](#).

ICANN Staff periodically informs SOS/ACs of best-practices and invites these groups to identify additional, targeted best-practices for their constituents. As part of SOP this will be done annually and publicly documented.

[MOUs](#) with numerous international entities address SSR-related best practices.

Several [Regional Engagement Strategies](#) include SSR best practices; in particular, strategies for Africa, Latin America and Middle East regions emphasize SSR responsibilities.

ICANN staff works with the Anti-Phishing Working Group (APWG) Internet Policy Committee to publish recommendations for web application protection, has engaged in development of resources for security awareness (through SANS Secrethuman.org activities and with NCA Stop.Think.Connect). Organization of American States (OAS) has released a 2014 Latin American & Caribbean Cybersecurity Report which includes best practices recommendations for countries in the region and includes a section contributed by ICANN. ICANN Staff also is participating through the Commonwealth Cybercrime Initiative.

The [revised new gTLD registry agreement](#) contains additional language on SSR best practices.

Implementation Notes

This recommendation is in progress; report is expected to be published September 2016



SSR Recommendation 13 Implementation

ICANN Areas of Influence as a Coordinator, Collaborator and Facilitator
30 June 2015

Implementation 13 Timeline



Status of Deliverables

	Responsible	Due Date
Contact SO and AC Chairs to encourage identification and publication of a best practices repository page that is responsive to their constituencies	Staff	✓
Engage in a variety of ongoing activities to encourage global use of SSR best practices	Staff	✓
Develop standard operating procedures to support activity in this area	Staff	✓

Recommendation 13 Implementation Description

ICANN should encourage all Supporting Organizations to develop and publish SSR-related best practices for their members.

- Complete
- Planned/In Process
- Behind schedule, expected to recover within original plan
- Behind schedule, original plan to be adjusted



1

SSR Recommendation 13 Implementation

ICANN Areas of Influence as a Coordinator, Collaborator and Facilitator
30 June 2015

Project Status

As part of SOP, ICANN staff contacts all SOs and ACs (via chairs) to encourage identification and publication of a best practices repository page that is responsive to their constituencies. The ccNSO currently publishes SSR-related best practices [information](#) for their members.

ICANN staff engages in a variety of ongoing activities to encourage global use of SSR best practices, as part of SOP (see Recommendation 12).

Activity in this area is ongoing as part of SOP and ICANN builds on its activities annually. In 2015, for example, ICANN anticipates the creation [of a set of resources of best practices](#) for securing collaborative community assets. These resources will help SOs and ACs make informed decisions regarding identity management and data protection. From these, SOs and ACs could set requirements for how community assets should be made secure, stable and resilient.

Implementation Notes

This recommendation is complete.



2

SSR Recommendation 14 Implementation

ICANN Engagement with Others in the Global Internet Ecosystem
30 June 2015

Implementation 14 Timeline



Recommendation 14 Implementation Description

ICANN should ensure that its SSR-related outreach activities continuously evolve to remain relevant, timely and appropriate

Status of Deliverables

	Responsible	Due Date
Outreach activities have been expanded and are reviewed annually as part of SOP. 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. A new Engagement Interface allows the community to see upcoming SSR and related outreach and engagement activities. This is an on-going obligation.	Staff	✓

- Complete
- Planned/in Process
- Behind schedule, expected to recover within original plan
- Behind schedule, original plan to be adjusted



1

SSR Recommendation 14 Implementation

ICANN Engagement with Others in the Global Internet Ecosystem
30 June 2015

Project Status

Outreach activities have been expanded and are reviewed annually as part of SOP. 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. A [new Engagement Interface](#) allows the community to see upcoming SSR and related outreach and engagement activities. This is an on-going obligation.

Implementation Notes

This recommendation is completed.



2

SSR Recommendation 15 Implementation

ICANN Engagement with Others in the Global Internet Ecosystem
30 June 2015

Implementation 15 Timeline



Recommendation 15 Implementation Description

ICANN should act as a facilitator in the responsible disclosure and dissemination of DNS security threats and mitigation techniques.

Status of Deliverables

	Responsible	Due Date
Publish Coordinated Vulnerability Disclosure document	Staff	✓
Collaborate with operators and trusted security community entities on DNS security threats and mitigation techniques	Staff	✓

1

Complete
 Planned/in Process
 Behind schedule, expected to recover within original plan
 Behind schedule, original plan to be adjusted



SSR Recommendation 15 Implementation

ICANN Engagement with Others in the Global Internet Ecosystem
30 June 2015

Project Status

ICANN published a [Coordinated Vulnerability Disclosure document](#) in 2013. While the framework and SOP is in place, staff notes that because facilitation of responsible disclosure is an on-going obligation the work in this area is ongoing.

Staff collaborates with operators and trusted security community entities on DNS security threats and mitigation techniques. This is related to Recommendation 28.

Implementation Notes

This recommendation is complete.

2



SSR Recommendation 16 Implementation

Maintaining Clear Processes for SSR Issues

30 June 2015

Implementation 16 Timeline



Status of Deliverables

	Responsible	Due Date
Expand Outreach activities and processes to solicit input on the SSR Framework	Staff	✓
Include SSR best practices and SSR topics in several Regional Engagement Strategies	Staff	✓
Support a variety of capability-building initiatives by the Security Team	Staff	✓

Recommendation 16 Implementation Description

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.

- Complete
- Planned/In Process
- Behind schedule, expected to recover within original plan
- Behind schedule, original plan to be adjusted



1

SSR Recommendation 16 Implementation

Maintaining Clear Processes for SSR Issues

30 June 2015

Project Status

[Outreach activities](#) and processes solicit input on the SSR Framework have been expanded and are part of ICANN's SSR SOP; activities are ongoing and are reviewed annually. For example: the Security team's ongoing work with security communities including the Anti Phishing Working (APWG), the Messaging, Malware and the Mobile Anti-Abuse Working Group (MAAWG) has resulted in participation by members of those communities in SSAC; through engagement with the International Criminal Law Network (ICLN) and Commonwealth Cybercrime Initiative (CCI), the Security team emphasizes the value of multistakeholder approaches to cybersecurity issues.

Several [Regional Engagement Strategies](#) include SSR best practices and SSR topics are addressed by ICANN across all global regions.

This is related to Recommendations 4, 5 and 14.

At the request of stakeholders, the Security team supports a variety of capability-building initiatives, such as DNSSEC training, ccTLD attack and contingency response training, law enforcement training, outreach at Network Operator Group meetings such as Caribbean Network Operators Group (CaribNOG), Middle East Network Operators Group (MENOG), among others.

Implementation Notes

This recommendation is complete.



2

SSR Recommendation 17 Implementation

Maintaining Clear Processes for SSR Issues
30 June 2015

Implementation 17 Timeline



Status of Deliverables

	Responsible	Due Date
See Recommendation 2 for information on how activities and initiatives relate to SSR priorities, objectives and goals and are integrated into ICANN's planning, budgeting and project reporting efforts.	Staff	✓

Recommendation 17 Implementation Description

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

- Complete
- Planned/in Process
- Behind schedule, expected to recover within original plan
- Behind schedule, original plan to be adjusted



1

SSR Recommendation 17 Implementation

Maintaining Clear Processes for SSR Issues
30 June 2015

Project Status

See Recommendation 2 for information on how activities and initiatives relate to SSR priorities, objectives and goals and are integrated into ICANN's planning, budgeting and project reporting efforts.

Implementation Notes

This recommendation is complete.



2

SSR Recommendation 18 Implementation

Maintaining Clear Processes for SSR Issues
30 June 2015

Implementation 18 Timeline



Status of Deliverables

	Responsible	Due Date
Implement SSR Framework and update annually	Staff	✓
Publish previous status of SSR Review Team implementation	Staff	✓
Reflect SSR Framework in the Strategic and Operating Plans and budgets, with the status/progress being reviewed and reported annually for public input prior to the issuance of the following-year's Ops Plan and budget	Staff	✓
Integrate SSR objectives and goals into ICANN's Organizational (structural) reviews	Staff	✓

Recommendation 18 Implementation Description

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

- Complete
- Planned/In Process
- Behind schedule, expected to recover within original plan
- Behind schedule, original plan to be adjusted



1

SSR Recommendation 18 Implementation

Maintaining Clear Processes for SSR Issues
30 June 2015

Project Status

Implemented as part of the [FY 13 & FY 14 SSR Frameworks](#) and will be repeated annually.

The previous status of SSR RT implementation was published in [Appendix C of the ATRT2 Report](#)

Elements of the SSR Framework are reflected in the Strategic and Operating Plans and budgets, with the status/progress being reviewed and reported annually for public input prior to the issuance of the following-year's Ops Plan and budget. Information is posted [here](#).

SSR objectives and goals are integrated into ICANN's [Organizational \(structural\) reviews](#), as appropriate; these are scheduled every five years.

Implementation Notes

This recommendation is complete.



2

SSR Recommendation 19 Implementation

Maintaining Clear Processes for SSR Issues
30 June 2015

Implementation 19 Timeline



SSR Framework

Status of Deliverables

	Responsible	Due Date
Publish annual SSR Framework and track progress against activities committed to in the previous year's Framework	Staff	✓

Recommendation 19 Implementation Description

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 execution of its SSR responsibilities.

- Complete
- Planned/in Process
- Behind schedule, expected to recover within original plan
- Behind schedule, original plan to be adjusted



1

SSR Recommendation 19 Implementation

Maintaining Clear Processes for SSR Issues
30 June 2015

Project Status

The publication of the [annual SSR Framework](#) tracks progress against the activities committed to in the previous year's Framework. This tracking mechanism, along with ICANN's regular project management reporting, and operating plans and budgets, provide more details on SSR (see Recommendation 2 for more information) and are all part of ICANN's SOP.

Implementation Notes

This recommendation is complete.



2

SSR Recommendation 20 Implementation

ICANN's SSR-Related Budget and Staff
30 June 2016

Implementation 20 Timeline



Recommendation 20 Implementation Description

ICANN should increase the transparency of information about organization and budget related to implementing the SSR Framework and performing SSR-related functions.

Status of Deliverables

	Responsible	Due Date
(Phase I) Integrate SSR Framework and reports on SSR activities and expenditures into planning framework and process to provide public information about SSR-related plans, budgets and activities	Staff	✓
(Phase II) Identify mechanisms that provide more detailed public information on SSR-related budgets and expenditures across multiple ICANN departments	Staff	Nov 2015
(Phase II) Explore after-event-reports (for relevant threats) that include budget and resource impacts related to managing the event	Staff	✓

Complete
 Planned/In Process
 Behind schedule, expected to recover within original plan
 Behind schedule, original plan to be adjusted



1

SSR Recommendation 20 Implementation

ICANN's SSR-Related Budget and Staff
30 June 2016

Project Status

[Note: Recommendations 20, 21, 22 are addressed by the framework and related processes that ICANN has in place.]

(Phase I) A [planning framework and process](#) is in place to provide public information about SSR-related plans, budgets and activities (as outlined in Recommendation 2). This is integrated with ICANN's SSR Framework and reports on SSR activities and expenditures. Periodic SSR activity [reporting](#) augments this public information.

(Phase II) Exploration is underway to identify mechanisms that provide more detailed public information on SSR-related budgets and expenditures across multiple ICANN departments. Target completion date: Nov 2015.

- November 2015 – Information gathered for SSR-related budget and expenses support from ICANN's various departments and is being reviewed before it is posted.
- February 2016 – posting of data collected for ICANN SSR-related budget and expenses, anticipated date now end of September 2016

(Phase II) Staff also is exploring after-event-reports (for relevant threats) that include budget and resource impacts related to managing the event; producing a public version of these reports is under consideration. Revised target completion date: September 2016.

Implementation Notes

This recommendation is in progress.



2

SSR Recommendation 21 Implementation

ICANN's SSR-Related Budget and Staff
30 June 2016

Implementation 21 Timeline



Recommendation 21 Implementation Description

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

Status of Deliverables

	Responsible	Due Date
(Phase I) Integrate SSR Framework and reports on SSR activities and expenditures into planning framework and process to provide public information about SSR-related plans, budgets and activities	Staff	✓
(Phase II) Identify mechanisms that provides more detailed public information on SSR-related budgets and expenditures across multiple ICANN departments	Staff	Nov 2015
(Phase II) Explore after-event-reports (for relevant threats) that include budget and resource impacts related to managing the event	Staff	✓

Complete
 Planned/In Process
 Behind schedule, expected to recover within original plan
 Behind schedule, original plan to be adjusted



1

SSR Recommendation 21 Implementation

ICANN's SSR-Related Budget and Staff
30 June 2016

Project Status

[Note: Recommendations 20, 21, 22 are addressed by the framework and related processes that ICANN has in place.]

(Phase I) A [planning framework and process](#) is in place to provide public information about SSR-related plans, budgets and activities (as outlined in Recommendation 2). This is integrated with ICANN's SSR Framework and reports on SSR activities and expenditures. Periodic SSR activity [reporting](#) augments this public information.

(Phase II) Exploration is underway to identify mechanisms that provide more detailed public information on SSR-related budgets and expenditures across multiple ICANN departments. Target completion date: Nov 2015.

- November 2015 – Information gathered for SSR-related budget and expenses support from ICANN's various departments and is being reviewed before it is posted.
- February 2016 – posting of data collected for ICANN SSR-related budget and expenses, anticipated date now end of September 2016

(Phase II) Staff also is exploring after-event-reports (for relevant threats) that include budget and resource impacts related to managing the event; producing a public version of these reports is under consideration. Revised target completion date: September 2016.

Implementation Notes

This recommendation is in progress.



2

SSR Recommendation 22 Implementation

ICANN's SSR-Related Budget and Staff
30 June 2016

Implementation 22 Timeline



SSR Resources
for new gTLDs

Recommendation 22 Implementation Description

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.

Status of Deliverables

	Responsible	Due Date
(Phase I) Integrate SSR Framework and reports on SSR activities and expenditures into planning framework and process to provide public information about SSR-related plans, budgets and activities	Staff	✓
(Phase II) Identify mechanisms that provides more detailed public information on SSR-related budgets and expenditures across multiple ICANN departments	Staff	Nov 2015
(Phase II) Explore after-event-reports (for relevant threats) that include budget and resource impacts related to managing the event	Staff	✓

- ✓ Complete
- Planned/In Process
- Behind schedule, expected to recover within original plan
- Behind schedule, original plan to be adjusted



SSR Recommendation 22 Implementation

ICANN's SSR-Related Budget and Staff
30 June 2016

Project Status

[Note: Recommendations 20, 21, 22 are addressed by the framework and related processes that ICANN has in place.]

(Phase I) A [planning framework and process](#) is in place to provide public information about SSR-related plans, budgets and activities (as outlined in Recommendation 2). This is integrated with ICANN's SSR Framework and reports on SSR activities and expenditures. Periodic SSR activity [reporting](#) augments this public information.

(Phase II) Exploration is underway to identify mechanisms that provide more detailed public information on SSR-related budgets and expenditures across multiple ICANN departments. Target completion date: Nov 2015.

- November 2015 – Information gathered for SSR-related budget and expenses support from ICANN's various departments and is being reviewed before it is posted.

- February 2016 – posting of data collected for ICANN SSR-related budget and expenses, anticipated date now end of September 2016

(Phase II) Staff also is exploring after-event-reports (for relevant threats) that include budget and resource impacts related to managing the event; producing a public version of these reports is under consideration. Revised target completion date: September 2016.

Implementation Notes

This recommendation is in progress.



SSR Recommendation 23 Implementation

Immediate and Near-Term Future Risk
30 June 2015

Implementation 23 Timeline



Appropriate Resources
and Support

Recommendation 23 Implementation Description

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.

Status of Deliverables

	Responsible	Due Date
Maintain adequate independent funding to allow SSAC and RSSAC to conduct work	Staff	✓
Establish processes and procedures for Working Groups and ACs to support their decisions being reached in an objective manner that is free from external or internal pressure	Staff	✓
Document budget process for SO/AC input on the budget	Staff	✓

- Complete
- Planned/In Process
- Behind schedule, expected to recover within original plan
- Behind schedule, original plan to be adjusted



1

SSR Recommendation 23 Implementation

Immediate and Near-Term Future Risk
30 June 2015

Project Status

ICANN has in place [funding allocated to allow SSAC and RSSAC](#) to conduct work. The support funding has never been linked to, or conditioned by, any performance/output/content evaluation, thus maintaining adequate independence.

Established processes and procedures for WGs and ACs also support their decisions being reached in an objective manner that is free from external or internal pressure.

A publicly documented budget process for SO/AC input on the budget is SOP; for example, these requests have been [published for FY 15](#).

Implementation Notes

This recommendation is complete.



2

SSR Recommendation 24 Implementation

Longer-Term Future Risk
30 June 2015

Implementation 24 Timeline



Chief Security
Office Role

Recommendation 24 Implementation Description

ICANN must clearly define the charter, roles and responsibilities of the Chief Security Office Team.

Status of Deliverables

	Responsible	Due Date
Address range of internal and external SSR responsibilities with Identifier Systems Security, Stability & Resiliency (ISSR) Team, CTO (and staff), and CIO (and staff); ISSR team to focus on current externally focused ISSR, the CIO and team to focus on current internally focused ISSR and the CTO and team looking towards future ISSR risks and opportunities	Staff	✓

- ✓ Complete
- Planned/In Process
- Behind schedule, expected to recover within original plan
- Behind schedule, original plan to be adjusted



1

SSR Recommendation 24 Implementation

Longer-Term Future Risk
30 June 2015

Project Status

The Identifier Systems Security, Stability & Resiliency (ISSR) Team, CTO (and staff), and CIO (and staff) closely coordinate to address the range of ICANN's internal and external SSR responsibilities, enumerated in this document, with ISSR team focused on current externally focused ISSR, the CIO and team focused on current internally focused ISSR and the CTO and team looking towards future ISSR risks and opportunities. As the SSR environment associated with the Internet's system of unique identifiers evolves, so too will ICANN staffing. Updates will be published in appropriate places on the icann.org website.

Implementation Notes

This recommendation is complete.



2

SSR Recommendation 25 Implementation

Longer-Term Future Risk
31 March 2016

Implementation 25 Timeline



Risk Management

Status of Deliverables

	Responsible	Due Date
The DNS Risk Management Framework was approved by the Board in Nov. 2013.	Staff	✓
The DNS Risk Assessment and DNS Resilience Model was published in May 2014.	Staff	✓
ICANN is now in the ongoing DNS Risk Mitigation Phase, which is part of our SOP; risk mitigation collaboration (such as this session), have been held to engage the community to participate in mitigation of the identified risks.	Staff	✓
ICANN also has published a Report on Mitigating Risk of Name Collisions , and has been using the Name Collision Risk Management Framework to manage name collision issues.	Staff	✓
Periodic review and update of the DNS Risk Management Framework is part of ICANN's SOP.	Staff	✓
Community collaboration on, and updating of, ERM continues. Recommendations 25 – 28 will reach closure upon completion and Board Risk Committee approval of ERM update.	Staff	✓

Recommendation 25 Implementation Description

ICANN should put into place mechanisms for identifying both near and longer-term risks and strategic factors in its Risk Management Framework.

Complete
 Planned/In Process
 Behind schedule, expected to recover within original plan
 Behind schedule, original plan to be adjusted



1

SSR Recommendation 25 Implementation

Longer-Term Future Risk
31 March 2016

Project Status

[Note: ICANN's enterprise risk management work—including the ongoing efforts to identify and remediate enterprise risk and apply ERM best practices, under guidance of the Board Risk Committee—incorporates SSR-related risk management and threat mitigation addressed in Recommendations 25 – 28]

- The [DNS Risk Management Framework](#) was approved by the Board in Nov. 2013.
- A [DNS Risk Assessment and DNS Resilience Model](#) was published in May 2014.
- ICANN is now in the ongoing DNS Risk Mitigation Phase, which is part of our SOP; risk mitigation collaboration (such as this [session](#)), have been held to engage the community to participate in mitigation of the identified risks. ICANN will continue to collaboratively engage and leverage the Enterprise Risk Model to identify the key asset owners and resources needed to address the risks that have been shared and identified with the community.
- ICANN also has published a [Report on Mitigating Risk of Name Collisions](#), and has been using the Name Collision Risk Management Framework to manage name collision issues.
- Periodic review and update of the [DNS Risk Management Framework](#) is part of ICANN's SOP.
- Also part of ICANN's ERM SOP, are ongoing root zone coordination and monitoring, I Root operations, threat detection and mitigation related to ICANN's DNS Operations.
- [Community collaboration](#) on, and updating of, ERM continues. Recommendations 25 – 28 will reach closure upon completion and [Board Risk Committee](#) approval of ERM update.
- [Risk Committee of the ICANN Board](#) is engaged in reviewing [the ERM framework](#).

Implementation Notes

This recommendation is complete.

The [Risk Committee of the Board](#) has agreed on the ERM strategy that the organization should pursue, and that this strategy includes at the minimum annual updates on risk assessments, mitigation plans assessment and risk governance.



2

SSR Recommendation 26 Implementation

ICANN's Risk Management Process
31 March 2016

Implementation 26 Timeline



Status of Deliverables

	Responsible	Due Date
See Recommendation 25	Staff	✓

Recommendation 26 Implementation Description

ICANN should prioritize the timely completion of a Risk Management Framework.

- ✓ Complete
- Planned in Process
- Behind schedule, expected to recover within original plan
- Behind schedule, original plan to be adjusted



1

SSR Recommendation 26 Implementation

ICANN's Risk Management Process
31 March 2016

Project Status

See Recommendation 25

Implementation Notes

This recommendation is completed.

The [Risk Committee of the Board](#) has agreed on the ERM strategy that the organization should pursue, and that this strategy includes at the minimum annual updates on risk assessments, mitigation plans assessment and risk governance.



2

SSR Recommendation 27 Implementation

Risk Management Framework
31 March 2016

Implementation 27 Timeline



Status of Deliverables

	Responsible	Due Date
See Recommendation 25	Staff	✓

Recommendation 27 Implementation Description

ICANN's Risk Management Framework should be comprehensive within the scope of its SSR remit and limited missions

- Complete
- Planned/In Process
- Behind schedule, expected to recover within original plan
- Behind schedule, original plan to be adjusted



1

SSR Recommendation 27 Implementation

Risk Management Framework
31 March 2016

Project Status

See Recommendation 25

Implementation Notes

This recommendation is completed.

[The Risk Committee of the Board](#) has agreed on the ERM strategy that the organization should pursue, and that this strategy includes at the minimum annual updates on risk assessments, mitigation plans assessment and risk governance.



2

SSR Recommendation 28 Implementation

Incidence Response and Notification
31 March 2016

Implementation 28 Timeline



Publish remit

Status of Deliverables

	Responsible	Due Date
See Recommendation 25 for status of Enterprise Risk Management Framework	Staff	✓
Identifier Systems SSR Activities Reporting	Staff	✓
Coordinated Vulnerability Disclosure Reporting	Staff	✓

Recommendation 28 Implementation Description

ICANN should continue to actively engage in threat detection and mitigation, and participate in efforts to distribute threat and incident information

- Complete
- Planned/In Process
- Behind schedule, expected to recover within original plan
- Behind schedule, original plan to be adjusted



31

1

[Identifier Systems SSR Activities Reporting](#)

As part of our continuing commitment to transparency and accountability, the Identifier Systems SSR department publishes an activities report. The report describes the activities ICANN performs to maintain the security, stability, and resiliency of the Internet's global identifier systems. These activities include collaboration with ICANN, security and operations, and public safety communities, where our staff serves several roles.

SSR Recommendation 28 Implementation

Incidence Response and Notification
31 March 2016

Project Status

[Identifier Systems SSR Activities Reporting](#)

As part of our continuing commitment to transparency and accountability, the Identifier Systems SSR department publishes an activities report. The report describes the activities ICANN performs to maintain the security, stability, and resiliency of the Internet's global identifier systems. These activities include collaboration with ICANN, security and operations, and public safety communities, where our staff serves several roles.

- The 1H 2015 activities report highlights ICANN's collaboration and stakeholder activities from January 1 through June 15, 2014. It summarizes activities performed as part of the identifier system SSR threat awareness and preparedness remit. It also provides progress reports on analytics or productivity improvement projects as well.

[Coordinated Vulnerability Disclosure Reporting at ICANN](#)

Posted the following Blogs:

- [Threats, Vulnerabilities and Exploits – oh my! 10 August 2015](#)
- [What is ICANN IIS-SSR? 4 August 2015](#)
- [Is This a Hack or an Attack? 15 September 2015](#)
- [Top Level Domain Incident Response Resource Now Available 28 September 2015](#)

See Recommendation 25 for additional details on ICANN's risk management work.

Implementation Notes

This recommendation is completed.

The [Risk Committee of the Board](#) has agreed on the ERM strategy that the organization should pursue, and that this strategy includes at the minimum annual updates on risk assessments, mitigation plans assessment and risk governance



2

2

