PLAN FOR ENHANCING INTERNET SECURITY, STABILITY, AND RESILIENCY (FY 11)

September 2010

Table of Contents

Executive Summary 1
ICANN's Role 2
ICANN Security, Stability and Resiliency Programs 3
Plans to Enhance Security, Stability and Resiliency 3
1. Purpose and Overview 6
2. Challenge and Opportunity 7
3. ICANN Role 9
4. ICANN Contributors to Security, Stability and Resiliency Efforts 12
5. ICANN's Ongoing Programs Related to Security, Stability and Resiliency 15
5.1 Core DNS/Addressing Security, Stability and Resiliency 15
5.1.1 IANA Operations 15
5.1.2 DNS Operations 18
5.2 TLD Registries and Registrars Security, Stability and Resiliency 20
5.2.1 gTLD Registries 20
5.2.2 New gTLDs and IDNs 21
5.2.3 gTLD Registrars 22
5.2.4 Whois 23
5.2.5 Contractual Compliance 24
5.2.6 Protecting gTLD Registrants 25
5.2.7 ccTLDs 26
5.2.8 IANA Technical Requirements 26
5.2.9 Collaborative Response to Malicious Abuse of Domain Name System 26
5.2.10 Enabling Overall DNS Security and Resiliency 27
5.2.11 Validity, right of use, and uniqueness of Internet number resources. 28
5.3 Global Security Outreach (Engagement, Awareness) 29
5.3.1 Global Partners and Activities 29
5.3.2 Regional Partners and Activities 30
5.3.3 Working with Governments 31
5.4 Engaging with the Regional Internet Registries 32
5.5 ICANN Corporate Security and Continuity Operations 32
5.6 Activities of ICANN Supporting Organizations and Advisory Committees 33
6. ICANN FY11 Plans to Enhance Security, Stability and Resiliency 38
6.1 Core DNS/Addressing Functions 39
6.1.1 IANA Operations 39

6.1.2 DNS Operations 40
6.2 Relationships with TLD Registries and Registrars 40
6.2.1 gTLD Registries 41
6.2.2 New gTLDs 41
6.2.3 IDNs 41
6.2.4 ccTLDs 42
6.2.5 Registrars 42
6.2.6 Contractual Compliance 43
6.2.7 Collaborative Response to Malicious Abuse of Domain Name System 43
6.2.8 Enabling Overall DNS Security 44
6.3 Global Security Outreach 44
6.3.1 Extend Existing Partnerships 44
6.3.2 Commercial Enterprise 44
6.3.3 Participation in Global Cyber Security Dialogue 45
6.4 ICANN Corporate Security and Continuity Operations 45
6.5 ICANN Support Organizations and Advisory Committees 46
7. Conclusion 48
Appendix A–FY 11 SSR Resourcing 49
Appendix B – Glossary of SSR Plan Terms and Acronyms 59

Executive Summary

The Internet has thrived as an ecosystem engaging many stakeholders organizing through collaboration to foster communication, creativity and commerce in a global commons. The interoperability of the global commons depends on the operation and coordination of the Internet's unique identifier systems.[1] ICANN and the operators of these systems acknowledge that maintaining and enhancing the security, stability and resiliency of these systems is a core element of their collaborative relationship.

This document is an update to the ICANN Plan for Enhancing Internet Security, Stability and Resiliency published 16 May 2009 (here after referred to as the 2009 SSR Plan, http://www.icann.org/en/topics/ssr/ssr-draft-plan-16may09-en.pdf). For FY 11, the SSR Plan has been updated to reflect ICANN's Security activities from June 2010-July 2011. Updates from the 2009 SSR Plan will be noted in italics. The FY 11 SSR Plan is being published for comment from August to September 2010.

The ICANN 2010-2013 Strategic Plan (http://www.icann.org/en/strategic-plan/strategic-plan-2010-2013-19feb10-en.pdf) states "The stability and security of the Domain Name System (DNS) are important priorities for the ICANN community and for Internet users globally. They form the core elements of ICANN's mission. Misuse of and attacks against the DNS and other Internet infrastructure are steadily increasing. To ensure the security, stability and resiliency that are crucial to the DNS, ICANN must work in partnership with others involved in the broader aspects of these issues."

The Strategic Plan identifies DNS stability and security as one of ICANN's four key strategic focus areas. This aligns with the high importance given to SSR in the Affirmation of Commitments (http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm) executed on 30 September 2009 between ICANN and the U.S. National Telecommunications Information Administration (NTIA). The Strategic Plan separates the broad range of ICANN's security, stability and resiliency responsibilities into strategic objectives, community work, strategic projects and staff work.

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

The secure, stable and resilient operation of the Internet's unique identifier systems is a core part of ICANN's mission. As the frequency and sophistication of disruptive attacks and other malicious behaviour increases, ICANN and its community must continue to collaborate toward improving the resilience of the DNS and strengthen its capability to deal with these events. As the nature of attacks and malicious behaviour broadens, ICANN must work with other stakeholders in this arena to clarify ICANN's role and to find solutions to problems that are broader than the mission of any one entity.

Strategic objectives identified for DNS security and stability:

1. *100% DNS uptime.*
2. *Lower DNS abuse.*
3. *More secure top-level domain (TLD) operations.*
4. *Improved DNS resilience to attacks.*

On 12 February 2010, ICANN published the Proposed Strategic Initiatives for Improved DNS Security, Stability and Resiliency (SSR) (http://www.icann.org/en/topics/ssr/strategic-ssr-initiatives-09feb10-en.pdf). The paper describes the rationale, key features and projected costs of two strategic initiatives related to DNS security and stability.

Based on feedback received in two public comment periods, during the ICANN Nairobi meeting, and April 2010 DNS-CERT Operational Requirements and Collaboration Workshop, and the ICANN Brussels meeting, ICANN does not plan to operate a DNS-CERT, but instead ICANN continues to engage with stakeholders to define operational requirements for a DNS collaborative response capability and system-wide DNS risk assessment and threat analysis.

ICANN's Role

ICANN acts in accordance with its bylaws in conducting multi-stakeholder, consensus-based processes, policies and programs, including those related to security, stability and resiliency.

- ICANN's role must focus on its core missions related to the unique identifier systems.
- ICANN does not play a role in policing the Internet or operationally combating criminal behavior.
- ICANN does not have a role in the use of Internet related to cyber-espionage and cyber war.

- ICANN does not have a role in determining what constitutes illicit content on the Internet.
- ICANN's role includes participating in activities with the broader Internet community to combat abuse of the unique identifier systems. These activities will involve collaboration with governments combating malicious activity enabled by abuse of the systems to assist in protection of these systems.

ICANN Security, Stability and Resiliency Programs

- ICANN is responsible for Internet Assigned Numbers Authority (IANA) operations. Ensuring secure, stable and resilient operation of the DNS root zone function has been, and will remain, the highest priority.
- ICANN is an enabler for the Domain Name System (DNS) and addressing community efforts to strengthen the security, stability and resiliency foundations of the system. Such efforts will include supporting the development and deployment of protocols and supporting technologies to authenticate Internet names and numbers.
- ICANN is an enabler and facilitator of the security, stability and resilience activities conducted by DNS registries, registrars, and other members of the community.
- ICANN is responsible for the secure, stable and resilient operation of its own assets and services.
- ICANN is a participant in broader forums and activities related to the security, stability and resiliency of the Internet's unique identifier systems.

Plans to Enhance Security, Stability and Resiliency

During FY 11 operating year, ICANN plans to conduct the programs and initiatives outlined here. Appendix A details specific program and activity objectives, partners, deliverables, and resource commitments.

- ***IANA Operations*** – *On 16 July 2010, ICANN, VeriSign and NTIA implemented DNSSEC for the authoritative root zone. This was a significant milestone for improving the security and stability of the Internet. ICANN will continue working with the Internet community to remove obstacles to adoption of DNSSEC. Other initiatives include improving root zone management through automation; improved authentication of communications with TLD managers.*

- ***DNS Root Server Operations*** *– ICANN will continue efforts to conduct contingency planning and exercises with root operators, and improve L-Root resiliency and infrastructure.*
- ***gTLD Registries*** – Ensure applicant evaluation of new Generic top-level domain (gTLD) and Internationalized Domain Names (IDN) continues to provide for secure operations. *ICANN will continue to pursue implementation of measures to combat the potential for malicious conduct arising from the establishment of new gTLDs.* ICANN will mature the gTLD registry continuity plan and continue testing the data escrow system.
- ***ccTLD Registries*** *– As IDN ccTLDs are introduced through the Fast Track process, ICANN is continuing efforts to address variant management and security mitigation concerns.*

  ICANN will continue its collaboration with country code top-level domain (ccTLD) registries on through the joint Attack and Contingency Response Planning (ACRP) program and as the Registry Operations Course (ROC) in conjunction with the Country Code Names Supporting Organization (ccNSO), the regional top-level domain (TLD) associations and ISOC.
- ***Contractual Compliance*** – ICANN will continue to enhance the scope of contractual enforcement activities involving gTLDs to include initiating audits of contracted parties as part of implementing the 2009 Amendments to Registrar Accreditation Agreement (RAA) and identify potential involvement of contracted parties in malicious activity for compliance action. ICANN will also continue to facilitate policy consideration on enhanced compliance activities as part of potential amendments to the RAA in FY 11.
- ***Response to Malicious Abuse of DNS*** – ICANN will build on its collaborative efforts and facilitate information sharing to enable effective response related to malicious conduct enabled by the abuse of the DNS.
- ***ICANN Corporate Security and Continuity Operations –*** *ICANN will ensure its security programs are conducted within overall corporate risk management, crisis management, and business continuity programs. A major focus will be the establishment of a sound foundation of documented plans and supporting procedures. These programs include:*
  - ***Corporate Information Security Plan*** *– ICANN has developed a Corporate Information Security Plan benchmarked from ISO 27002 standards. The plan is being implemented in FY 11.*
  - ***Meetings Security Plan*** *– Building on efforts to support improved security planning for ICANN global meetings, a*

Meetings Security Plan has been developed and will be used in site selection and preparation for ICANN meetings in FY 11 and beyond.

- ***Personnel and Physical Security Plan*** *– As part of efforts to improve security for personnel and facilities, these two plans are being implemented in FY 11.*
- ***Business Continuity and Incident Management Plan*** *– ICANN conducted an IANA Continuity Exercise in 2010, and efforts will continue in FY 11 with an ICANN crisis communications exercise and implementation of the ICANN Business Continuity and Incident Management Plan.*
- ***Enterprise Risk Management program*** *– ICANN implemented Enterprise Risk Management (ERM) Guidelines and established an ERM program in FY 10. ICANN will continue to enhance this program in FY 11 with a risk assessment and support to ICANN's Board Risk Committee.*

- ***Ensure Global Engagement and Cooperation*** – ICANN will continue to enhance partnerships with the Internet Engineering Task Force (IETF), Internet Society (ISOC), Regional internet Registries (RIRs), Network Operators Groups (NOGs), the DNS–Operations, Analysis and Response Center (DNS-OARC) *and the Forum for Incident Response Teams (FIRST).* ICANN will also engage in global dialogues to foster understanding of the security, stability, and resiliency challenges that face the Internet ecosystem and how to engage these challenges with multi-stakeholder approaches.

1. Purpose and Overview

The updated SSR Plan outlines to a wide range of stakeholders how ICANN will contribute to global efforts in addressing security, stability and resiliency as challenges for the Internet, focused on its mission related to the Internet's unique identifiers. The plan explains ICANN's roles and boundaries to how it engages in this area; overviews existing ICANN programs in this area; and details planned activities and dedicated resources through the next operational year. The plan is organized into seven sections and an appendix:

- Section 1: Purpose and Overview
- Section 2: Challenge and Opportunity
- Section 3: ICANN Role
- Section 4: ICANN Contributors to Security, Stability and Resiliency Efforts
- Section 5: ICANN's Ongoing Programs Related to Security, Stability and Resiliency
- Section 6: *ICANN FY11 Plans to Enhance Security, Stability and Resiliency*
- Section 7: Conclusion
- *Appendix A: ICANN FY 11 Security, Stability and Resiliency Program Objectives, Partners, Milestones/Deliverables and Resourcing*

As stated in the Executive Summary, this update builds upon the 2009 SSR Plan and the vision and objectives laid out in the ICANN 2010–2013 Strategic Plan. This version of the plan is intended to provide additional updates on the foundation for ICANN and its community regarding its role, and to enhance the framework for organizing its security, stability and resiliency efforts. The plan has been updated as part of the annual review in conjunction with the ICANN strategic and operational planning cycles.

2. Challenge and Opportunity

The vibrant Internet environment is threatened by growing levels of malicious activity conducted by a variety of actors including heavy involvement of criminal organizations in fraud, extortion, and other illicit on-line activity as well as a rise in Denial-of-Service (DoS) attacks and other disruptive activity conducted via the Internet. Increasingly, the activity on the Internet reflects the full range of human motivations and conduct. In part, such activity reflects the open nature of the Internet that has made it successful, enabled innovation at its edge, and allowed for communication, creativity and commerce in a global commons. But openness has also come with vulnerabilities. For example, activity that takes advantage of opportunities to "spoof" or "poison" DNS resolution to misdirect computer connections of unwitting users is growing. Similarly, the incidence of routing hijacks and address registration and Autonomous System Numbers (ASN) registration hijacks continues to grow. DoS attacks can disrupt users of all types. The full range of Internet stakeholders have expressed increasing concern over the past few years: users; enterprises; sovereign states; and organizations involved in discussions surrounding the Internet and the wider information society. Efforts to address these challenges must also address risks to security and stability that can stem from instituting new controls which can be misused by criminals, or network designs that make achieving stability more difficult.

ICANN will address risks to Internet security, stability and resiliency within the boundaries of its responsibilities. Article I of ICANN's bylaws states that ICANN's mission is "to coordinate, overall, the global Internet's system of unique identifiers, and to ensure stable and secure operation of the Internet's unique identifier systems." ICANN programs and activities in this area focus on achieving three main characteristics within the Internet's unique identifier systems: security, stability and resiliency. Security is the capacity to protect and prevent misuse of the Internet's unique identifier systems. Stability is the capacity to ensure that the system operates as expected, and that users of the unique identifier systems have confidence that the system operates as expected. Resiliency is the capacity of the unique identifier systems to effectively respond to, react to and recover from malicious attacks and other disruptive activity. ICANN works with responsible parties across the unique identifier systems to ensure accountability for proper implementation of its policies and contractual arrangements. As a multi-stakeholder driven organization, ICANN ensures that its efforts make the most effective use of available community resources in this area,

working closely with its core stakeholders, and explicitly identifying objectives and metrics for performance in its strategic, operational, and financial planning. This plan provides the community a roadmap as to how ICANN meets its responsibilities. *Appendix A of the plan provides details on planned FY 11 activities, milestones and associated resources. A major focus of the ICANN security staff's FY 11 objectives will be establishing metrics for broader programs seeking to improve the overall security, stability, and resiliency of the unique identifier systems.*

3. ICANN Role

ICANN acts in accordance with its bylaws in conducting multi-stakeholder, consensus-based processes, policies and programs to include those related to security, stability and resiliency. ICANN's core mission focuses on enabling a multi-stakeholder approach to the effective operation of the IANA functions; establishing global policies that ensure the coordination of the DNS, Internet Protocol (IP) addressing, and IP assignments; and promoting competition and choice within the gTLD environment through a system of contracts with gTLD Registries and ICANN-accredited registrars.

As part of its mission, ICANN has played a role over the past ten years in contributing to security and stability of the Internet's unique identifier systems. ICANN and the associated operators of the unique identifier systems have recognized and acknowledged that maintaining and enhancing the security and stability of services is a core element of their relationship. This principle is highlighted in the system of contracts and agreements between ICANN and the operators depending on the distinctive nature of the relationships, specific roles and mutual responsibilities. This collaborative effort and its implementation provide the essential confidence that unique identifiers and the organizations that provide them across the globe will ensure security, stability and resiliency through a coordinated, cooperative system.

ICANN plans to continue to contribute across a range of activities to enable the Internet names and addressing systems to be securable, stable and resilient in the face of evolving threats and risks. At the same time it will ensure its efforts focus on its core mission related to the Internet's unique identifier systems. It will not act as a police officer in operationally combating criminal behavior and engaging malicious actors. ICANN does not engage in activities related to the use of the Internet for cyber espionage and cyber war. Also, ICANN does not involve itself in activities related to what constitutes illicit content that resides on or transits the Internet. ICANN will continue to participate with the broader Internet security community in key forums concerning combating specific malicious activities (e.g., phishing and spread of malicious code) that use the Internet system of unique identifiers.

ICANN structures its security, stability and resiliency activities through consideration of its role: as directly responsible, as an enabler/facilitator, as a participant.

- ICANN is directly responsible for the IANA operations and collaborates in the compilation and distribution of the root zone with the US Department of Commerce and VeriSign. Ensuring secure, stable and resilient operation of the DNS root zone function has been, and will remain, the highest priority. Additionally, ICANN is a core enabler for the DNS and addressing community efforts to authenticate Internet names and numbers. ICANN advocates that an essential step in addressing DNS security is the implementation of Domain Name System Security Extensions (DNSSEC) (*ICANN, VeriSign and NTIA implemented DNSSEC in the root zone on 16 July 2010*). Other key efforts will focus on improving the system-wide understanding of risks, enabling the Single Trust Anchor (TA) implementation of the Resource Public Key Infrastructure (RPKI), and cooperating with partners to enhance the security and resiliency practices in the TLD community.
- ICANN serves as an enabler and facilitator of security, stability and resilience activities conducted by DNS registries and registrars. The nature of ICANN's roles and responsibilities depend on the specific characteristics of its relationships with these core operators. In addition to collaborative activities, ICANN maintains agreements with all gTLD registries and ICANN-accredited registrars. These agreements have increasingly become mechanisms for improving the security, stability and resiliency across the DNS. ICANN's efforts to ensure compliance and implement the provisions of these agreements are a major focus for its efforts going forward. With regard to ccTLD registries, ICANN and ccTLD operators have expressed a commitment to further enhance the security, stability and interoperability of the DNS for the benefit of the local and global Internet community on the basis of a peer relationship. Information sharing, mutual assistance and capability building will be a major focus of the activities going forward. ICANN will also focus on supporting collaborative response capabilities in the community to provide enhanced security for the DNS.
- ICANN participates in activities with the Numbering Resource Organization (NRO) and RIRs guided by an overarching understanding that RIRs and ICANN are to maintain and enhance the security, stability and resilience of the Internet for the benefit of local and global users of the Internet.
- ICANN is directly responsible for the secure, stable and resilient operation of its own assets and services as it conducts IANA and other coordinating functions, and as the operator of the DNS L-root server.

- ICANN supporting organizations, advisory committees and staff are key participants in broader forums and activities whose purposes range from improving resiliency in the face of disruptive attacks to collaborative efforts focused on combating malicious Internet activity such as the propagation of malware and phishing that use the Internet's unique identifier systems. Examples include the detailed sessions at recent ICANN meetings on DNS abuse and DNSSEC.
- ICANN has a mission of public trust regarding its role in coordinating the Internet's unique identifier systems and will play a leadership role regarding overcoming the challenges to achieving a secure, stable, resilient Internet ecosystem which must also remain a vibrant environment for global dialogue, commerce and innovation.

4. ICANN Contributors to Security, Stability and Resiliency Efforts

ICANN's engagement related to security, stability and resiliency involves activities across the organization's staff, supporting organizations and advisory committees. Key players include:

- ***IANA functions staff*** – Responsible for the conduct of the IANA functions to include the coordination of the DNS root zone, the operation of the .arpa registry, the allocation of IP address space, and the registration of protocol parameters. Specific activities related to security, stability and resiliency are outlined below.
- ***DNS Operations staff*** – Responsible for the operations of L-ROOT, one of the thirteen root name servers, DNSSEC Infrastructure for ICANN-managed domains and TLDs, DNSSEC Signing of the ROOT (KSK), KSK Facilities, Ceremonies, and ccTLD housing, authoritative DNS servers of ICANN and the domain portfolio of ICANN. The members of the DNS Operations team are regularly attending meetings such as NANOG, RIPE, MENOG, LACNOG, NZNOG, SANOG, AFNOG, among others to talk about various aspects regarding projects for ICANN's DNS Operations activities.
- ***Services/Contractual Compliance staff*** – Responsible for ensuring coordination and compliance with agreements by gTLD registries and ICANN accredited registrars. Specific activities related to security, stability and resiliency are outlined below.
- ***Policy staff*** – Responsible for assisting supporting organizations and advisory committees in the conduct of their activities related to policy formulation, including those of supporting organization-convened working groups. Specific activities related to security, stability and resiliency are outlined below.
- ***Global Partnerships staff*** – Responsible for engaging globally and regionally with ICANN stakeholders to ensure ICANN's full global engagement in operations and implementation. In this regard, ICANN activities relating to security, stability and resiliency are integrated into Global Partnerships' overall work for the organization.
- ***Corporate Communications staff*** – Responsible for ensuring effective communication of ICANN plans and programs, and representing the organization and its activities to the ICANN community. ICANN's activities related to security, stability and resiliency are integrated into its overall corporate communications program.

- ***Security staff*** – Responsible for day-to-day planning and execution of operational ICANN efforts related to security as directed by the ICANN Board and CEO in fulfillment of the ICANN strategic and operational plans. The team coordinates across the range of ICANN efforts to ensure effective engagement in topics relating to security, including cybersecurity and other forums related to security, stability and resiliency.
- ***Security and Stability Advisory Committee (SSAC)*** – An ICANN Advisory Committee, SSAC is responsible for identifying to the ICANN Board and community key issues and challenges that ICANN faces in ensuring the security and stability of the Internet's unique identifier systems. The Committee conducts studies on key issues as requested by the ICANN Board and as initiated as part of its mandate described below, as well as collaborating with other ICANN organizations such as the Generic Names Supporting Organization (GNSO).
- ***Root Server System Advisory Committee (RSSAC)*** – An ICANN advisory committee, RSSAC provides advice on the operational requirements of root name servers as well as examines and advises on the security aspects of the root name server system and the total system performance, robustness, and reliability.

More broadly, activities related to security, stability and resiliency occur throughout ICANN supporting organizations and other advisory committees as described below.

The ICANN security staff has overall responsibility for effective orchestration across ICANN activities and for establishing an integrated planning and tracking process for these activities while ensuring alignment and integration across departments and stakeholders. Figure 1 depicts the basic organizational relationship within the ICANN structure.

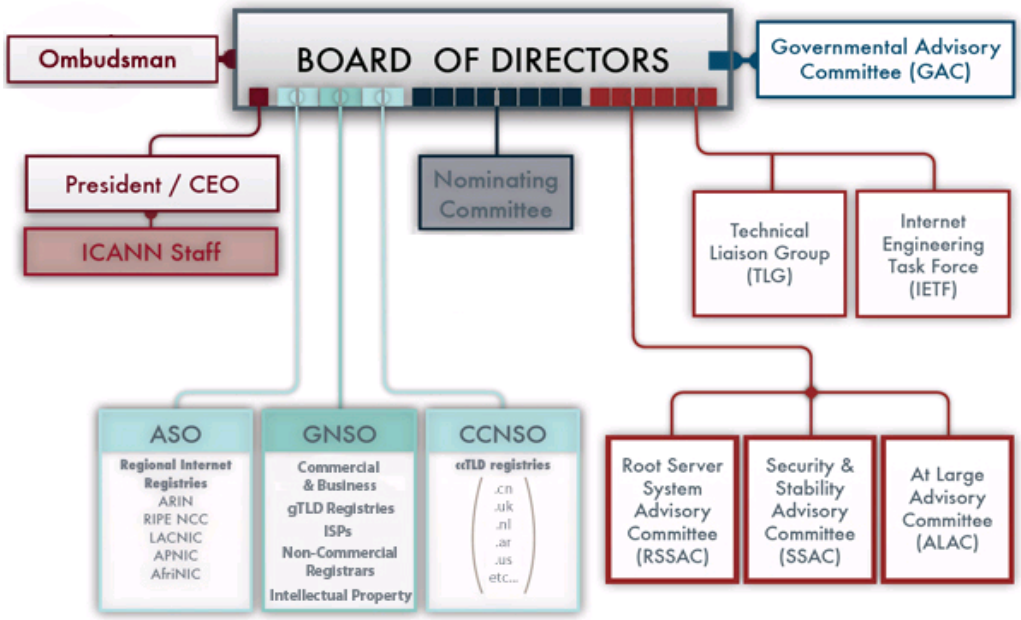


Figure 1 – ICANN organization

5. ICANN's Ongoing Programs Related to Security, Stability and Resiliency

This section describes the major programs and activities ICANN has conducted that contribute to the security, stability and the resiliency of the Internet's unique identifier systems, identifying key operational partners and providing background on existing efforts. The purpose of this section of the plan is to provide a baseline understanding of the wide range of ICANN activities that contribute to security, stability and resiliency of the unique identifier systems. For ICANN to effectively pursue its responsibilities in this area, most of the major staff elements as well as supporting organizations and advisory committees are involved. This section provides background and explanation of how the programs and activities fit into the ICANN structure as well as how they intersect with outside organizations.

The section is organized around the framework established in Section 3, beginning with core DNS/addressing functions; working with the TLD registry and the registrar communities; engaging with the Regional Internet Registries (RIRs) through the ASO; corporate security and continuity programs; activities of the supporting organizations and advisory committees, and participation in global and regional Internet security, stability and resiliency activities.

5.1 Core DNS/Addressing Security, Stability and Resiliency

5.1.1 IANA Operations

ICANN operates the IANA functions in coordination with the US Department of Commerce, VeriSign, the Internet Engineering Task Force (IETF), the Regional Internet Registries (RIRs) and the Top Level Domain (TLD) operators as described below. Effective conduct of these activities is the fundamental contribution made by ICANN to the Internet's stability and resiliency. Through the conduct of the IANA functions, ICANN coordinates and manages the registries of the key identifiers enabling a global, interoperable Internet.

While the Internet is renowned for being a worldwide network free from central coordination, key unique identifier system operations must be globally coordinated—and this coordination role is undertaken by ICANN. Specifically, through the IANA

functions, ICANN allocates and maintains unique codes and numbering systems that are used in the technical standards (protocols) that drive the Internet. The IANA functions' various activities can be broadly grouped into three categories:

- ***Domain Names*** – Through the IANA functions, ICANN manages the root zone, the .int and .arpa domains, and an Internationalized Domain Name (IDN) practices resource. Management practices ensure that each change to these zones is assessed for its impact on stability and security for the specific Top-Level Domain, and for the root zone overall. The operation of the IANA functions also allows ICANN to play a role in enabling security of the DNS and IP address systems by deploying and maintaining trust anchors at the root of the DNS and addressing systems that can greatly enhance the integrity of unique identifier data as well as the integrity of responses within the DNS system.
- ***Addresses and AS Numbers*** – IANA administers and manages the global pool of IP addresses (IPv4 and IPv6) and ASNs. IANA allocates these number resources to the RIRs in accordance with global number resource policies that are developed by the RIR communities through their policy development processes and coordinated globally by the ASO. This participatory policy process allows for global consensus by the ultimate recipients of the resources that IANA is acting in a fair, predictable and stable manner. *ICANN is working with RIRs (through the ASO) and the IETF on the development of RPKI technology to introduce the certification of number resources.*
- ***Protocol Assignments*** – Internet protocol and parameter registries are managed by ICANN, through the IANA functions, in conjunction with the IETF. ICANN implements and maintains the more than 700 protocol and parameter registries according to standards developed through the long-standing consensus process of Request for Comments (RFC) publication. Working closely with the IETF and authors of the RFCs, the IANA functions staff ensures that the registries are established using consistent processes, and are maintained so that they are accurate and available. The relationships between the IANA functions staff and the IETF are documented in RFC 2860 and in a Service Level Agreement.

The IANA functions staff worked with the TLD community to track the overall mitigation implementation within the TLD system in response to the DNS cache poisoning vulnerability discovered in the summer of 2008 (see "2008 DNS Cache Poisoning Vulnerability" presentation at http://www.iana.org/about/

presentations/davies-cairo-vulnerability-081103.pdf). ICANN will ensure its programs and activities enhance secure, stable and resilient processes for root zone changes/additions and the operation of trusted anchors for queries within the DNS as detailed below.

ICANN annually provides the US Department of Commerce an information security plan related to the conduct of the IANA functions in compliance with the IANA functions contract ICANN has with the Department of Commerce and as part of its own corporate security and contingency planning. *In January 2010, ICANN conducted a successful IANA Continuity Exercise, see the After Action Report located at http://www.icann.org/en/security/iana-business-continuity-exercise-aar-23feb10-en.pdf.*

ICANN expects to make the last allocations of IPv4 unicast space to the Regional Internet Registries (RIRs) during the calendar year 2011. The allocations will be made according to the Global Policy for the Allocation of the Remaining IPv4 Address Space[2], which was developed by the RIR communities and ratified by the ICANN board in March 2009.

Although this allocation will empty the pool of address space managed by ICANN's IANA Department, the RIRs will still have address pools from which they can allocate and assign addresses to ISPs and other network operators. The RIRs have been working on establishing policies that will ensure access to small blocks of IPv4 address space for new market entrants[3] during the period after the last five /8s have been allocated and before IPv6 is adopted by the majority of Internet connected networks.

The RIRs have also established policies allowing IPv4 address space to be transferred from one network operator to another network operator[4]. These policies are designed to allow networks to move addresses where they provide most value, allowing continued network growth.

[2] http://www.icann.org/en/general/allocation-remaining-ipv4-space.htm

[3] http://www.nro.net/documents/comp-pol-201006.html#2-6

[4] http://www.nro.net/documents/comp-pol-201006.html#1-3-2

The ICANN Board Risk Committee is working on assessing the risks ICANN might face as a consequence of reduced availability of IPv4 address space.

The long-term solution is the widespread adoption of IPv6. While considerable progress has been made and ISPs, such as XS4all in the Netherlands, are starting to offer IPv6 as a standard service to all their customers, there is still some way to go. ICANN has run a number of awareness-raising sessions at ICANN meetings, while the RIRs operate IPv6 training and awareness training programs[5][6][7][8][9].

The key thing to remember is that the existing Internet will continue to operate, even after the RIRs have allocated their IPv4 reserves. There will be a period where some networks will be accessible over IPv6 and some will not but IPv6 will allow operators to continue to grow their networks beyond the limits imposed by IPv4.

5.1.2 DNS Operations

ICANN has advocated for the need to implement DNSSEC at the root-level. *Since the initial SSR Plan, ICANN, VeriSign and NTIA have progressed toward implementation of DNSSEC through a scaled introduction leading toward overall root signing in July 2010. The first Key Signing Key (KSK) ceremony for DNSSEC was conducted in Culpeper, Virginia on 16 June 2010 (see http://www.icann.org/en/announcements/announcement-4-16jun10-en.htm), and a second KSK ceremony was conducted on 12 July 2010 in Los Angeles, California to enable the signing of the root zone. The deployment of DNSSEC in the root zone provides benefits for those who publish information in the DNS, permits Internet community and end users to locate cryptographic key material "trust anchors" in the root zone and protect DNS resolvers from cache poisoning.*

[5] http://www.afrinic.net/training/ipv6training.htm

[6] http://www.apnic.net/services/services-apnic-provides/training/courses/ipv6-essentials

[7] https://www.arin.net/knowledge/v4-v6.html

[8] http://lacnic.net/en/eventos/ipv6/

[9] http://www.ripe.net/training/ipv6/outline.html

ICANN has begun to sign .arpa and many of ICANN's own organizational domains. Preparations have included implementation of a DNSSEC test bed since June 2007, collaboration with TLD and other DNS operators regarding efforts to implement DNSSEC, gaining technical proficiency in implementing cryptologic approaches in compliance with relevant standards, and ensuring implementation of DNSSEC efforts are part of operating plans and budgets. ICANN has established a dedicated staff group responsible for operating and securing its DNSSEC implementations, including the signing of icann.org and iana.org. Finally, in order to further general DNSSEC implementation, ICANN has established the IANA Trust Anchor Repository for Top Level Domains (ITAR) as a way of ensuring DNSSEC keys for TLDs that have implemented DNSSEC are available to those deploying DNSSEC at this time.

ICANN collaborates with the operators of root name servers with respect to the secure and stable coordination of the root zone, to ensure appropriate contingency planning and to maintain clear processes in root zone changes. ICANN will continue to collaborate with the operators of root name servers and others with respect to the secure and stable coordination of the root server system. The RSSAC has been a key advisor in the way that protocol changes, such as the addition of IPv6 records to the root, affect that system.

Additionally, ICANN operates the root name server designated *l.root-servers.net.* Through this operational role, ICANN staff also interacts at the operational level with the other root server operators. As the operator of L-root, ICANN is also active within the DNS community including contributing to community efforts such as the Domain Name System–Operations, Analysis and Research Center (DNS–OARC) and The Cooperative Association for Internet Data Analysis (CAIDA)'s "Day in the Life of the Internet" research project. ICANN is committed to using its operations to promote diversity and understanding of best practices and seeks to learn and disseminate lessons. *The DNS Operations team has also supported study of L-Root Scaling, http://www.icann.org/en/announcements/announcement-17sep09-en.htm.*

In 2009, ICANN improved L Root resiliency with instances in Prague, Czech Republic and Istanbul, Turkey. Additional enhancements are planned in 2010 and into FY 11.

5.2 TLD Registries and Registrars Security, Stability and Resiliency

A fundamental, direct responsibility of ICANN related to the overall security, stability and resiliency of the Internet is the management of agreements with gTLD registries and ICANN-accredited registrars and the framework agreement structure used to manage relationships with the ccTLD registries. ICANN has contracts with 16 gTLD registries and more than 900 accredited registrars who are responsible for coordinating the registration of domain names and ensuring they resolve in the DNS. The responsibilities of these contracted parties are delineated through Registry Agreements (RA) and Registrar Accreditation Agreements (RAAs). ICANN seeks to protect registrants and to contribute to maintaining the security, stability and resiliency of the DNS and the broader Internet through the provisions in these agreements. Over the past decade, ICANN has sought to strengthen these agreements to include provisions that improve stability and resiliency as described below.

5.2.1 gTLD Registries

ICANN collaborates with gTLD operators with respect to the secure and stable coordination of these TLDs. All gTLD registries maintain agreements with ICANN. While some elements of these agreements may differ, provisions related to security, stability and resiliency are consistent. These agreements contain a provision requiring registry operators to implement temporary specifications or policies established by ICANN and consensus policies developed by the Generic Names Supporting Organization (GNSO) and adopted and approved by ICANN. Other provisions of the agreements that contribute to a secure and stable registry operation include the requirement for third-party data escrow and service level agreements for DNS services, the shared registration system, and name server operations. ICANN-gTLD contracts specify availability, performance levels and data center requirements. In 2007 ICANN initiated the gTLD registry continuity planning effort that has resulted in the establishment of a working plan as well as commitment to a series of annual exercises of the plan to improve the ability of the gTLD registry community to respond to problems or failures within the registry/registrar system.

In 2006, ICANN introduced the Registry Services Evaluation Process (RSEP) as a means to facilitate a timely and predictable process for the introduction of new registry services. A key component of the RSEP is a determination of whether the proposed service has the potential to pose a security or stability

issue. If it is determined that the proposed service could pose a security or stability issue, the proposal is referred to an independent panel of technical experts known as the Registry Services Technical Evaluation Panel (RSTEP). The RSTEP conducts reviews of the proposed service and makes a recommendation to the ICANN Board about whether to approve or deny the service.

The Expedited Registry Security Request (ERSR) process was introduced in October 2009 (see http://www.icann.org/en/registries/ersr/). The ERSR was developed to provide a process for gTLD registries to inform ICANN of a present or imminent security incident to their TLD and/or the DNS to request a contractual waiver for actions it might take or has taken to mitigate or eliminate an Incident. A contractual waiver is an exemption from compliance with a specific provision of the Registry Agreement for the time period necessary to respond to the Incident. The ERSR has been designed to allow operational security to be maintained around an Incident while keeping relevant parties (e.g., ICANN, other affected providers, etc.) informed as appropriate.

5.2.2 New gTLDs and IDNs

Through FY 10 and into FY 11, ICANN has been working with the community to enhance approaches to mitigating malicious conduct in new TLDs [See Mitigating Malicious Conduct Explanatory Memorandum 28 May 2010, http://www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-memo-update-28may10-en.pdf].

With the launch of the IDN ccTLD Fast Track in November 2009 and preparations for the new gTLD process to include IDNs, ICANN recognizes the need to undertake efforts to ensure the secure, stable and resilient operations of new entrants in the DNS and the system as a whole. The new gTLD application and review process includes a technical assessment of the applicant's ability to operate a registry as well as the strings conformance to technical requirements outlined in RFCs, per the Internationalizing Domain Names in Applications (IDNA) protocol and IDN Guidelines.

ICANN launched the IDN ccTLD Fast Track process on 16 November 2009 (see http://www.icann.org/en/topics/idn/fast-track/). The program has received 34 requests in 22 different languages since its launch (see http://www.icann.org/en/topics/idn/fast-track/string-evaluation-completion-en.htm). These strings are currently moving through the IANA delegation step, and the first IDN ccTLD strings were entered into the root zone in May 2010 for

Egypt, Saudi Arabia, United Arab Emirates and the Russian Federation. The ICANN Board approved delegation of strings to China, Hong Kong and Taiwan at the ICANN meeting in Brussels in June 2010, and strings for Sri Lanka, Thailand, Occupied Palestinian Territory, Jordan and Tunisia were approved in August 2010.

The initial introduction of IDN ccTLDs in the Fast Track is limited to non-contentious strings that represent countries and territory names corresponding to the existing ccTLDs.

In the Fast Track process, an independent team of experts, the DNS Stability Panel, conducts an evaluation of the proposed IDN ccTLD string for confusability and potential conflicts with security and stability requirements for IDN strings. The new gTLD process is expected to have similar expert panels available to conduct the technical evaluation of applicants and their proposed TLDs. Additionally, the new gTLD process provides for an upfront Registry Services Evaluation Process (RSEP) to assess potential security or stability issues of new registry services that are proposed in the gTLD application.

Furthermore, all applicants will be required to pass a pre-delegation technical check to verify they have met their technical requirements to operate a registry.

ICANN intends to launch a review of the IDN ccTLD Fast Track implementation in FY 11.

5.2.3 gTLD Registrars

ICANN collaborates with the registrars on issues related to security, stability and resiliency. Contractually, a standard Registrar Accreditation Agreement (RAA) governs ICANN's relationship with registrars. The RAA sets certain standards for data collection, retention, and escrow. The RAA also incorporates, by reference, consensus policies developed by the ICANN community, such as the Inter-Registrar Transfer Policy, Whois Data Reminder Policy, and Restored Names Accuracy Policy, among others, which in various ways support the security, stability, and resiliency of the DNS. *An enhanced RAA was introduced in 2009, and over 95% of gTLD registrations are now covered under the 2009 RAA through voluntary registrar adoption. ICANN has also published a Non-Lawyer's Guide to the 2009 RAA, in response to the At-Large Advisory Committee's request for a guide (http://www.icann.org/en/registrars/non-lawyers-guide-to-ra-agreement-15feb10-en.htm).*

ICANN's Registrar Liaison staff acts as a first-line in monitoring registrar compliance with RAA requirements on a daily basis through informal resolution of registrant complaints and inter-registrar disputes, and through periodic accreditation reviews (e.g., upon renewal of a registrar's RAA).

In supporting a more stable domain name system, ICANN has developed programs and procedures to address potential registrar failure. For example, ICANN has implemented its Registrar Data Escrow program, which requires registrars to deposit backup registration data into escrow on a daily or weekly basis. The De-Accredited Registrar Transition Procedure facilitates the timely transfer of registrations from one de-accredited registrar to an ICANN-accredited registrar. Additionally, ICANN staff uses several internal operating processes that are intended to help maintain a healthy domain registration environment and prevent disruption to registrants and Internet users in the event of registrar failure.

5.2.4 Whois

Whois services provide public access to data on registered domain names, which currently includes contact information for registered name holders. ICANN plays a role in administering community-developed rules for the Whois system within the gTLDs. The extent of registration data collected at the time of registration of a domain name, and the ways such data can be accessed, are specified in agreements established by ICANN for domain names registered in gTLDs. For example, ICANN requires accredited registrars to collect and provide free public access to the name of the registered domain and its nameservers and registrar, the date the domain was created and when its registration expires, and the contact information for the registered name holder, the technical contact and the administrative contact.

Whois is used by different communities for a number of purposes including to facilitate technical coordination and to help provide information about organizations and individuals that may be involved in the potential abuse of DNS. ICANN activities focus on ensuring compliance of the gTLD registries and ICANN-accredited registrars with their contractual obligations. In considering policy changes related to Whois, the ICANN community does recognize the legitimate use of the Whois system in helping those combating DNS abuse, while seeking to balance the broad range of stakeholder interests in how the Whois system operates. ICANN recognizes the privacy and security concerns that individuals have

expressed about making their information available via Whois. ICANN continues efforts to address these concerns. Recognizing that the current Whois service might decrease in reliability and usefulness over time and at the direction of the GNSO, ICANN staff has compiled a comprehensive set of requirements for WHOIS that includes known deficiencies in the current service and possible requirements that may be needed to support future policy initiatives. [Reference: ICANN Generic Names Supporting Organization (GNSO) Council Resolutions May 2009. Marina Del Rey, CA: ICANN. Retrieved October 25, 2009, from http://gnso.icann.org/resolutions/#200905]. The report attempts to identify technical requirements that would be necessary to implement to correct deficiencies and implement future Whois policies. A number of features in this inventory have their origins in SSAC recommendations to the GNSO, demonstrating that ICANN, through cross-SO/AC consideration of measures to improve WHOIS, is committed to finding solutions that maintain the utility of WHOIS while also considering the privacy and security of WHOIS information.

5.2.5 Contractual Compliance

The Contractual Compliance Department ensures that both ICANN and its contracted parties fulfill the requirements set forth in the agreements between the parties. Its activities include managing ICANN's complaint intake system, which allows the public to register domain name related complaints that may relate to security, stability and resiliency issues. See website at http://reports.internic.net/cgi/registrars/problem-report.cgi. Contractual compliance staff investigates complaints regarding possible RAA violations and compliance action is taken when contract violations are discovered. Although most complaints received through this system concern matters outside ICANN's authority (e.g., spam, website content, registrar customer service), ICANN forwards these complaints to registrars for handling.

The Contractual Compliance Department also manages the Whois Data Problem Report System (WDPRS), which can be accessed at http://wdprs.internic.net/. The WDPRS is designed to assist registrars in complying with their obligation to investigate alleged Whois data inaccuracies. This system, developed in 2002, allows the public to register Whois data inaccuracy claims and those claims are transmitted to registrars for appropriate action. In consultation with the community, the WDPRS was redesigned in 2008 to address concerns on functionality, limited capacity and

the lack of compliance follow-up. The redesigned WDPRS was launched in December 2008, and the Compliance team is continuing to improve this system with the objective of increasing Whois data accuracy.

ICANN commissioned the National Opinion Research Center at the University of Chicago to conduct a study on Whois data accuracy. A draft report was published on 15 February 2010, http://www.icann.org/en/announcements/announcement-3-15feb10-en.htm.

5.2.6 Protecting gTLD Registrants

ICANN also endeavors to ensure registrants have confidence in the security, stability and resiliency of the DNS in a variety of ways. These protections include provisions in ICANN contracts, agreements and enforcement programs. ICANN provides information to registrants about registrar obligations under the RAA and a means for complaints through the InterNIC web site http://www.internic.net/. ICANN has also conducted outreach with the registrar community, encouraging IPv6 support for domain registrants.

Additionally, the work of ICANN supporting organizations and advisory committees has focused on registrant security, stability and resiliency concerns. Past SSAC advisories have identified practices registrars should consider to protect domain names and domain registration accounts against unauthorized access, and to protect DNS configuration information from misuse.[10] SSAC projects in 2010 include a complementary report that identifies practices registrants can implement directly to proactively monitor and protect domain registration accounts and DNS configuration information against misuse. Other SSAC activities include papers on prohibition of redirection by TLDs [SAC041], DNSSEC deployment, documented abuse contacts [SAC038] and treatment of orphan DNS records.

The At-Large Advisory Committee (ALAC) has raised several issues concerning protecting registrants. The ALAC first raised the issue of domain tasting which led to GNSO Council and Board approval of a new consensus policy aimed at eliminating abuse of the add grace period for domain tasting. *More recently, the ALAC addressed the GNSO Council concerns about post-expiration recovery of domain names by registrants (PEDNR) and domain name registration accountability and transparency*

[10] See SAC 40, Measures to Protect Domain Registration Services Against Exploitation or Misuse, 19 August 2009 (http://www.icann.org/en/committees/security/sac040.pdf).

[http://www.atlarge.icann.org/announcements/announcement-19jul10-en.htm]. The GNSO is undertaking a number of additional initiatives that have the potential to result in better protection for registrants such as Inter-Registrar Transfer Policy enhancements which includes consideration of the need for electronic authentication and policy developments in the areas of fast flux hosting and registration abuse policies.

5.2.7 ccTLDs

ICANN's interaction with ccTLD registries is guided by the overarching understanding that ccTLD registries and ICANN are to maintain and enhance the security, stability and resilience of the DNS for the benefit of local and global users of the Internet. This is reflected in the accountability framework program that forms the basis to document the relationship between individual ccTLD registries and ICANN. ICANN's principal focus in fostering enhanced security, stability and resiliency with regard to ccTLDs is, through teaming with ccTLDs and others, to provide a platform for information sharing and common action, awareness-raising technical training and capacity building on attack and contingency response planning. ICANN staff work closely with the TLD operators to apprise them of security issues through the IANA functions, the Attack and Contingency Response Planning (ACRP) program and the efforts of the Global Partnerships regional liaisons. ICANN has developed a trust relationship with the TLD operators through improved performance and outreach to the TLD operator community, which assists in enabling collaborative response in situations requiring global coordination related to the DNS.

5.2.8 IANA Technical Requirements

ICANN, through management of the IANA functions, also helps ensure that TLDs meet the technical requirements to support stable and secure operations. Specific nameserver requirements ensure DNS availability of domains, and IANA functions staff work closely with TLD managers to resolve any problems they may have in maintaining those technical standards. ICANN does not involve itself in the operations of the ccTLDs, but stands ready to assist in situations where changes to their root zone data must be made quickly and reliably. ICANN's overarching goal is to ensure stability and security of the TLD's zone and the root zone.

5.2.9 Collaborative Response to Malicious Abuse of Domain Name System

ICANN cooperates with a range of organizations in endeavoring to ensure stakeholders can analyze activity that may involve abuse of

the DNS. Since late 2008, a major increase in activity involving malware that leverages the DNS has occurred. One of the more noteworthy of such incidents was the Conficker Worm [Conficker Summary and Review, http://www.icann.org/en/security/conficker-summary-review-07may10-en.pdf]. ICANN participated in a global, collaborative response to contain Conficker in concert with the security, TLD registry operators, and law enforcement communities. ICANN published a report, Conficker Summary and Review, that documents the chronology of events related to Conficker containment, discusses lessons learned, and suggests ways to improve future collaborative efforts (for example, ICANN's ERSR process). ICANN continues to work with registries and registrars to ensure awareness and to facilitate dissemination of information when security incidents of a global scale involving DNS occur. ICANN's mandate is limited in this area and therefore has participated as a peer in discussions about how to enable effective responses when specific operational situations arise.

To facilitate greater collaboration in this area, ICANN staff has supported efforts within the ccNSO on incident response for ccTLDs. In February 2010, ICANN published a Global Business Case for a DNS-CERT (http://www.icann.org/en/topics/ssr/dns-cert-business-case-19mar10-en.pdf) function in the Internet community. The business case contains a description of the requirements and possible costs, including the option that other members of the community operate such a DNS-CERT function. Since the publication of the DNS-CERT Business Case, consideration of public comment (http://www.icann.org/en/public-comment/summary-analysis-strategic-ssr-initiatives-and-dns-cert-business-case-24may10-en.pdf) and discussions at ICANN meetings in Nairobi and Brussels, ICANN is working with interested stakeholders to identify approaches to a DNS collaborative response capability not operated by ICANN but developed in collaboration with the community.

5.2.10 Enabling Overall DNS Security and Resiliency

While no single entity has overarching responsibility, ICANN staff, supporting organizations and advisory committees play an enabling role in improving the overall stability, security and resiliency of the DNS. Since its establishment, the SSAC has provided analysis and recommendations to the DNS community. The SSAC Advisory 004, *Securing the Edge*, provides a foundational analysis related to security challenges to the unique

identifier systems.[11] Key efforts have included analysis and recommendations related to DDoS attacks, DNSSEC implementation, adding IPv6 records to the DNS root, domain name front running, fast flux hosting and domain name hijacking. Additionally, SSAC members participate in the Anti-Phishing working group (APWG)'s Internet Policy Committee and have co-authored whitepapers on how phishers exploit sub-domain names, how organizations should respond to a web site attack, and are collaborating with the IPC to study commonly exploited web site vulnerabilities.

ICANN will continue its facilitating role going forward, in seeking to identify community-wide opportunities for collaboration, and in identifying and mitigating risks to the systems. ICANN initiated efforts to improve understanding of and mitigation of DNS-wide risks during its February 2009 Global DNS Security, Stability and Resiliency Symposium held in partnership with Georgia Tech Information Security Center (GTISC). The symposium focused on understanding DNS-related risks in large enterprises, challenges of secure, stable, resilient DNS operations in resource constrained environments, and addressing the misuse of the DNS for malicious activity. The report is available at http://www.gtisc.gatech.edu/icann09. *A second DNS Security, Stability and Resiliency Symposium was conducted in Kyoto, Japan in February 2010, see http://dns-srr.e-side.co.jp/, and the report published in April 2010 at http://www.icann.org/en/announcements/announcement-26apr10-en.htm.*

Additionally, ICANN staff, supporting organizations and advisory committees have initiated increasing collaboration with a range of multi-stakeholder efforts in order to improve ICANN's ability to conduct effective policy formulation, contractual enforcement and other initiatives in a manner that addresses security and resiliency challenges posed to and by the DNS.

5.2.11 Validity, right of use, and uniqueness of Internet number resources.

ICANN, through management of the IANA functions, acquires the strategy and the responsibility of the stability, security and resiliency of the Internet number allocation system and ultimately, through the application of Resource Public Key Infrastructure (RPKI), the global Internet routing system. This responsibility manifests in the need to implement a technically

[11] SAC 004, Securing the Edge, 17 October 2002, http://www.icann.org/en/committees/security/sac004.pdf.

ideal application of the RPKI Single Trust Anchor, as noted by the IAB[12] and NRO[13], and results in ability to fully certify the validity, right of use, and uniqueness of Internet number resources. ICANN and ICANN Staff have made substantial efforts in working with the IETF and other focus groups by engaging in the standards process, communicating with stakeholders, and deploying a (now retired) trial RPKI implementation.

ICANN is committed to working with all RPKI stakeholders and ICANN Staff has initiated processes in a manner that ensures the most sensible technical implementation is deployed and available to the Internet community as appropriate timelines and consideration demand.

5.3 Global Security Outreach (Engagement, Awareness)

5.3.1 Global Partners and Activities

The core of ICANN's global engagement strategy in relation to security, stability and resiliency is to build upon effective partnerships with a range of organizations. Many of these efforts are lead by the ICANN staff Global Partnerships team. ICANN has been an active participant in a wide range of global Internet related forums, including several that address Internet security, stability and resiliency issues. The range of partners and activities listed below is not comprehensive and ICANN will seek to engage others as opportunities arise. Key global partners include:

- ***Internet Engineering Task Force (IETF)/Internet Architecture Board (IAB)*** – Leads efforts to establish technological approaches to advance Internet security focused on the development of stronger protocols and operational practices. ICANN works with the IETF to establish the protocols related to naming and addressing, and endeavors to ensure their deployment within the core of the Internet to help secure the overall environment. In particular, ICANN will participate in efforts to establish protocols that provide a more securable foundation for the Internet focused on efforts such as DNSSEC and RPKI.
- ***Internet Society (ISOC)*** – Promotes awareness of cybersecurity concerns and the need to establish trust in the Internet for the global user base, particularly in the

[12] http://www.ietf.org/mail-archive/web/ietf-announce/current/msg07028.html

[13] http://www.nro.net/news/nro-declaration-rpki.html

developing world; in collaboration with others, provides for technical training to improve the security and resiliency of the Internet. ICANN works with ISOC to help ensure awareness and improved capabilities for security, stability and resiliency. ICANN plans to collaborate in maturing the ongoing joint ISOC/ICANN program to provide training to TLD operators to include technical training in how to improve security and mitigate cyber attacks and disruptions.

- ***Internet Governance Forum (IGF)*** – The IGF sponsors multi-stakeholder dialogues on cybersecurity and trust. Additionally, the IGF has developed a focus on managing critical Internet resources and cybercrime. ICANN will continue to participate in the IGF including providing awareness of its role in security, stability and resiliency in relation to the Internet's unique identifier system, and will contribute to the global dialogue in this Forum.
- ***DNS–Operations, Analysis and Response Center (DNS–OARC)*** – ICANN will continue as a supporting sponsor and active participant across the full range of DNS-OARC activities.

5.3.2 Regional Partners and Activities

ICANN has established regional ties through a variety of partners and activities. Key aspects of ICANN's regional activities are highlighted below:

- ***Regional ccTLD Associations*** – In addition to collaboration on the ACRP program as specified below, ICANN will continue to provide assistance and expertise for activities sponsored by these organizations.
- ***Regional Network Information Centers (NICs)/Network Operations Groups (NOGs)*** – ICANN will continue to participate in these forums to ensure its activities best enable secure and resilient network operations, including the coordination of the IANA functions.
- ***Asia*** – ICANN initiated the ccTLD security and resiliency training program as part of efforts to support DNS Capacity Building in collaboration with the Asia-Pacific TLD Association (APTLD) in May 2008 in Kuala Lumpur and has continued to receive strong support for the activity in that region. ICANN will continue to participate in regional forums such as the Internet Resource Management Essentials to provide operational advice and training related to DNS security and resiliency as opportunities arise.
- ***Europe*** – ICANN will continue participation in European Network and Information Security Agency (ENISA) efforts related to DNSSEC and improving DNS resiliency as part of the

larger European Commission effort in the critical infrastructure protection area. ICANN will collaborate with the Council of European National Top-Level Domain Registries (CENTR) to conduct ccTLD security and resiliency training sessions initiated in conjunction with the May 2009 RIPE 58 meeting in Amsterdam. ICANN will continue its partnership with Moscow State University Institute for Information Security Issues (IISI) in fostering the global dialogue on cybersecurity. Specifically, ICANN and IISI held joint workshops in Garmisch, Germany in 2008-2010 with the support of the German/American Marshall Center for Strategic Studies and both plan to continue collaboration in 2011.

- ***Africa and Latin America*** – ICANN will pursue activities related to cybersecurity jointly with regional organizations of ISOC as well as in other appropriate forums. ICANN provided ccTLD security and resiliency training in conjunction with the LACTLD Association in 2009 and 2010. ICANN has also provided ccTLD training in conjunction with the African Top Level Domains Association (AfTLD) and ISOC-Africa, and with APTLD in Asia.

5.3.3 Working with Governments

ICANN collaborates with governments across the globe in pursuing security, stability and resiliency of the Internet's unique identifier systems. ICANN will continue to provide its technical and operational perspective as to improving the security, stability and resiliency of the Internet's unique identifier systems. ICANN understands these systems must be treated as critical infrastructures. Within the ICANN structure, the Governmental Advisory Committee (GAC) will receive regular updates on ICANN security, stability and resiliency efforts and provide inputs to these programs as part of the strategic planning process. ICANN will remain active in defining its role in global discussions surrounding security and the implications for managing security and resiliency related to the unique identifier systems. ICANN will engage with UN, International, Intergovernmental and Regional Organizations targeting its efforts on enabling regional activities designed to improve security and resiliency in the DNS. These activities will build upon the memorandums of understanding that ICANN has with a range of these organizations. For example, ICANN will continue to participate in forums related to cybersecurity such as the ongoing OECD efforts to combat malware. ICANN will also continue to engage the associated APEC and other organizations efforts in this area.

The GAC also provides guidance to ICANN in the form of Communiques at ICANN International public meetings.

5.4 Engaging with the Regional Internet Registries

ICANN's engages with the ASO by interacting with the Number Resource Organization (NRO). Through this interaction ICANN works with the RIRs enabling ICANN and the RIRs to maintain and enhance the security, stability and resilience of the Internet for the benefit of local and global users of the Internet. ICANN participates in a number of activities with these organizations related to Internet security, stability and resiliency. Specifically, ICANN has been working with these organizations to DNSSEC sign subdomains within .arpa including ip6.arpa and in-addr.arpa. The RIRs are developing the means to enable the certification of IP addresses and AS numbers through the RPKI effort. RIRs are also responsible for ASN assignments and ICANN should seek to partner with RIRs on the integrity of those assignments. In the near term, this effort will provide a validated correlation between the number resource holder and the number resource. This hierarchical certification system can serve as the basis for the development of a means to validate Border Gateway Protocol routes. ICANN will continue to seek to be a partner on these efforts.

5.5 ICANN Corporate Security and Continuity Operations

ICANN ensures its own operations are secure, stable and resilient in the conduct of IANA and other core functions it performs, as part of the DNS and addressing systems, and to meet its corporate responsibilities and as a community contributor to the overall security, stability and resiliency of the Internet's unique identifier systems. ICANN will have the capacity to effectively respond and work with appropriate authorities if its own assets are subject to malicious activity.

ICANN is committed to an ongoing security program aimed at managing risks to the organization's information, personnel and physical assets. In the fall of 2008, ICANN hired a Director of Security Operations responsible for these programs. ICANN provides information assets, services and technology in support of IANA and other critical operations. Recent efforts have focused on re-assessing, documenting and deploying more robust security processes and policies. *The ICANN Information Security Plan is benchmarked from ISO 27002 standards and improvements to supporting procedures and processes are ongoing. The ICANN*

Information Security Plan also includes providing the US Department of Commerce the IANA Information Security Plan and managing the conduct of outside audits of its program. ICANN Personnel and Physical security planning focuses on protecting ICANN personnel and facilities required to conduct ICANN's set of global activities, to include ensuring security at ICANN Global Meetings. ICANN has established a planning process to manage security related risks to the overall enterprise and leverages its own internal security team as well as support from security consultants.

ICANN's security programs fit within an overall corporate risk management program overseen by the ICANN Board, as well as mutually supporting corporate business continuity programs. ICANN has matured its risk management processes with the establishment of Risk Management Guidelines for the organization, a Risk Oversight Management Team and by conducting regular risk assessments on key organizational risks and risk management reporting in core ICANN initiatives.

As ICANN grows, the corporation's asset base is growing along with its global activity and public profile. ICANN continues to stress sound risk management, business continuity and security as fundamental parts of its corporate processes.

5.6 Activities of ICANN Supporting Organizations and Advisory Committees

The broader ICANN community also plays an essential role in enabling the security, stability and resiliency of the unique identifier systems through a bottom-up policy process. ICANN's three supporting organizations—the Generic Names Supporting Organization (GNSO), the Country Code Names Supporting Organization (ccNSO), and the Address Supporting Organization (ASO)—are responsible for policy development that include matters related to security and stability. Specifics regarding each supporting organization and its processes can be found at http://gnso.icann.org, http://ccnso.icann.org/, and http://aso.icann.org/. These organizations make recommendations that must be approved by the ICANN Board in order to be implemented through a variety of contracts, agreements, Memorandums of Understanding (MoUs), and staff activities. Key areas under the purview of the GNSO include policy related to gTLD registry and registrar agreements to include consideration of any policy changes to gTLD Whois, the examination of issues raised by fast flux hosting, domain name

expiration issues, inter-registrar transfers of domain names and registration abuse policies among others.

ICANN is currently working with the community to revise the existing gTLD policy development process (PDP) to make it more effective and responsive to ICANN's policy development needs. Among the many revisions to the current PDP that are envisioned are changes geared at bringing greater technical expertise and research and fact-finding into the process early on to help define and target difficult policy challenges in a more informed and knowledgeable way; and developing better ways of assessing the effectiveness of new policies.

The ccNSO facilitates ICANN's collaboration with ccTLDs to include information sharing related to security, stability and resiliency.

The ASO coordinates the development of policy related to allocation by the IANA of IP addresses and AS numbers to the RIRs. The separate RIR communities develop these global policies. It is the function of the ASO to take these regionally developed policies and coordinate them into a single global policy, which is then transmitted to the ICANN Board for ratification.

Additionally, ICANN has four advisory committees that provide advice to the Board and ICANN community: the At-Large Advisory Committee (ALAC), the Governmental Advisory Committee (GAC), the Root Server System Advisory Committee (RSSAC), and the Security and Stability Advisory Committee (SSAC). Specifics related to the functions, processes, and activities of these committees can be found at http://www.icann.org/en/committees/. These advisory committees often collaborate across the supporting organization/advisory committee structure on efforts, particularly with the SSAC. The committees are supported by ICANN policy staff in conducting studies, undertaking deliberations, and in making recommendations.

The SSAC advises the ICANN community and Board on matters relating to the security and stability of the Internet's naming and address allocation systems. This includes matters pertaining to the correct and reliable operation of the root name system, address allocation and Internet number assignment, and gTLD registry and registrar services such as Whois. SSAC engages in an ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. Details of SSAC activities can be found at www.icann.org/en/committees/security.

Beyond those mentioned earlier, other ongoing activities occurring within the supporting organizations and advisory committees include joint discussions between these groups at ICANN meetings where they discuss issues of common interest in relation to security and stability, the organization of workshops and briefings on security and stability related issues, and communication of policy related activities to the community through the monthly Policy Update (http://www.icann.org/en/topics/policy/).

Relevant GNSO policy work includes the following:

Fast Flux: A GNSO Policy Development Process (PDP) on Fast Flux Hosting was completed in September 2009. The WG report explored who benefits from fast flux, and who is harmed, how Internet users are affected by fast flux hosting, and whether technical and policy changes to DNS reduce the negative effects of fast flux hosting. The GNSO Council adopted a motion in September 2009 to create a drafting team to develop a work plan to implement the recommendations proposed by the working group.

Transfers:

The GNSO Council has a working group focusing on the third of six planned policy development efforts addressing various aspects of inter-registrar transfers. This Working Group, IRTP Part B, is addressing five issues focusing on issues related to domain name hijacking, the urgent return of an inappropriately transferred name and the use of 'lock states'. The IRTP Part B WG published its Initial Report on 29 May (http://www.icann.org/en/announcements/announcement-05jul10-en.htm). The report includes, amongst others, a proposal for an Expedited Transfer Reversal Policy and the proposal to request an Issues Report on the requirement for a thick Whois for all gTLDs. Following the closing of the public comment period on 8 August, the WG will review the public comments received and start working on finalizing their report for GNSO Council consideration.

Registration Abuse:

The Registration Abuse Policies Working Group, which was launched in February 2009, was tasked to take a closer look at registration abuse policies. The RAP WG considered issues such as defining the difference between registration abuse and domain

name use abuse, defining existing abuses, identifying possible benefits or drawbacks from having a more uniform approach in contracts, and which areas, if any, are suitable for GNSO policy development to address abuse. The RAP WG delivered its final report to the GNSO Council on 29 May 2010 [http://www.icann.org/en/announcements/announcement-29may10-en.htm]. The Report includes concrete recommendations to address domain name registration abuse in gTLDs. Included are recommendations related to:

- *Cybersquatting: recommending the initiation of a Policy Development Process to investigate the current state of the UDRP.*
- *WHOIS access problems: seeking ways to ensure that WHOIS data is accessible in an appropriately reliable, enforceable, and consistent fashion; and requesting that the ICANN Compliance Department publish data about WHOIS accessibility.*
- *Malicious use of domain names: recommending the creation of best practices to help registrars and registries address the illicit use of domain names.*
- *Fake renewal notices: recommending possible enforcement actions by ICANN Compliance*
- *Cross-TLD registration scam: recommending to monitor and co-ordinate research with the community*
- *Uniformity of contracts: recommending the creation of an Issues Report to evaluate whether a minimum baseline of registration abuse provisions should be created for all in-scope ICANN agreements.*
- *GNSO-wide practices for the collection and dissemination of best*
  practices, and for uniformity of reporting.
- *Front running*
- *Domain kiting*
- *Deceptive and/or offensive domain names*

In considering the recommendations, the GNSO Council has decided to form a drafting team to draft a proposed approach with regard to the recommendations contained in the report, which could include the timing of forming groups to consider some of the recommendations in the final report as well as how to deal with those recommendations that did not achieve unanimous consensus.

Post expiration domain name recovery: The GNSO Council initiated a PDP on Post-Expiration Domain Name Recovery in May 2009. This Working Group is addressing questions regarding the extent to which registrants should be able to reclaim their domain names after they expire. At issue is whether the current policies of registrars on the renewal, transfer and deletion of expired domain names are adequate.

Improvements to the RAA: The ICANN Board approved a revised Registrar Accreditation Agreement (RAA) in May 2009 (http://www.icann.org/en/topics/raa/). The new RAA includes increased due diligence on registrars and their affiliates, identification of registrars that may be involved in cybersquatting and other malicious conduct, enhanced WHOIS requirements and obligations for privacy/proxy providers, and requirements to identify abuse point of contacts to report instances of malicious conduct involving the DNS. *Law enforcement representatives, ALAC and other stakeholder groups are engaged in seeking further enhancements to the RAA (see http://www.icann.org/en/announcements/announcement-28may10-en.htm), and presented suggested modifications at the ICANN meeting in Brussels in June 2010.*

Internationalized Registration Data: Currently, no standards or guidelines define how internationalized domain registration data should be composed and displayed. A joint SSAC-GNSO Working Group was convened by the ICANN Board to study the feasibility and suitability of introducing display specifications to deal with the internationalization of registration data. The group will be soliciting input from interested constituencies including ccTLD operators, the CCNSO, the ASO, ALAC, and the GAC during its discussions to ensure broad community input. The initial set of goals of the IRD-WG are to gain an understanding of, and achieve consensus on, the types, kinds, and encodings of registration data that contracted parties would collect, display and maintain.

6. ICANN FY11 Plans to Enhance Security, Stability and Resiliency

Strategic and operational planning processes guide ICANN activities relating to enhancing security, stability and resiliency, and the resources allocated to these efforts. In FY 11, ICANN activities will include a number of key initiatives, such as:

- ***IANA Operations*** – Advocate, educate and complete DNSSEC implementation at the root level as called for in the ICANN 2010-2013 Strategic Plan as well as improving root zone management through automation; improved authentication of communications with TLD managers.
- ***DNS Root Server Operations –*** Continuing to seek mutual recognition of roles and responsibilities and initiate a voluntary effort to conduct contingency planning and exercises.
- ***gTLD Registries –*** Ensure applicant evaluation of new gTLD and IDN applicants continues to provide for secure operations. ICANN will mature the gTLD registry continuity plan and test the data escrow system.
- ***ccTLD Registries –*** ICANN will enhance its collaboration on maturing the DNS Capacity Building program, including the joint Attack and Contingency Response Planning (ACRP) and Registry Operations Curriculum program that has been established in conjunction with the ccNSO and the regional TLD associations.
- ***Contractual Compliance –*** ICANN will continue to enhance the scope of contractual enforcement activities involving gTLDs to include initiating audits of contracted parties as part of implementing the 2009 RAA and identify potential involvement of contracted parties in malicious activity for compliance action.
- ***Response to Malicious Abuse of Domain Name System –*** ICANN will build on its collaborative efforts related to malicious conduct enabled by the use of the DNS and facilitate information sharing to enable effective response.
- ***Internal ICANN Security and Continuity Operations*** – ICANN will ensure its security programs are conducted within overall corporate risk management, crisis management, and business continuity programs. A major focus will be the implementation of documented plans and supporting procedures.
- ***Ensure Global Engagement and Cooperation*** – ICANN will enhance partnerships to include the Internet Engineering

Task Force (IETF), Internet Society (ISOC), regional internet registries and network operators groups, the DNS–Operations, Analysis and Response Center (DNS–OARC) and the Forum for Incident Response Team (FIRST). ICANN will also engage in global dialogues to foster understanding of the security, stability, and resiliency challenges that face the Internet ecosystem and how to engage these challenges with multi-stakeholder approaches.

The full range of activities is explained further below. Appendix A provides details on specific objectives, partners, deliverables, and resource commitments planned during FY 11.

6.1 Core DNS/Addressing Functions

6.1.1 IANA Operations

ICANN will continue conducting IANA functions and working to improve the operational excellence of these operations in collaboration with the US Department of Commerce, VeriSign, the RIRs and TLD operators.

Specific IANA functions improvement initiatives include:

- Improving root zone management through automation (eIANA/RZM software); improved authentication of communications with TLD managers; and reviews of processes and practices for security and optimization considerations.
- Supporting the development and implementation of certified IP address allocations and assignments through RPKI or other mechanisms adopted by the RIRs and the Internet routing community to include continued support of the IETF Secure Inter-Domain (SIDR) working group.
- Working with the technical and operational communities to identify, analyze, and potentially implement additional technical requirements or standards to improve DNS security, stability and resiliency.

As part of overall resiliency improvements, ICANN conducted an IANA Continuity Exercise in January 2010, testing the failover of IANA services from Marina del Rey, California to Reston, Virginia. The test exercise demonstrated IANA failover capabilities and communications mechanisms to ensure the availability of IANA services. ICANN will enhance resiliency of IANA services in 2010-2011.

6.1.2 DNS Operations

ICANN, the US Department of Commerce and VeriSign achieved a significant milestone in 2010 with the implementation of DNSSEC in the root zone. Per the priority laid out in the 2010–2013 strategic plan, ICANN will continue efforts to support the introduction of DNSSEC by TLD operators and others in FY 11.

ICANN will also pursue a range of activities to enable broader DNSSEC implementation throughout the DNS globally, collaborating with DNS experts and experienced operators. ICANN will ensure that its programs including inter-registrar transfers and escrow account for such implementations and continue stakeholder discussions on implementations. ICANN will continue maintaining the IANA Trust Anchor Repository for Top Level Domains (ITAR) until the root zone is signed. ICANN will continue to seek authorization to sign the .int and .arpa zones. ICANN will support the implementation of DNSSEC by signing ICANN managed zones (including icann.org and iana.org), and facilitating lessons learned effort among those involved in DNSSEC implementation.

ICANN seeks to enable the establishment of more robust mechanisms for coordination as part of the root operator community regarding measures that would contribute to security, stability and resiliency. ICANN, in its role as L-operator, plans to collaborate with other root operators in initiating a voluntary effort to conduct planning and exercises to improve the resiliency of the root server systems against a range of stressing contingencies.

ICANN plans to continue enhancements to the operation of L-root. Additionally, ICANN has contracted the DNS-OARC to study the impact of changes including the implementation of new gTLDs and IDNs, implementing IPv6, and possible implementation of DNSSEC signing of the root zone on the operation of a single root-server operation based on the L-root model. More broadly, the RSSAC and SSAC are conducting a joint study of root server security and stability in light of projected changes detailed in Section 6.6.

6.2 Relationships with TLD Registries and Registrars

6.2.1 gTLD Registries

ICANN will continue contractual coordination related to gTLD operations to include vetting applications for new services via RSEP. Once the new gTLD process is operational, ICANN expects reviews to include proposals that require activation of the RSTEP to evaluate security, stability and resiliency concerns. ICANN will continue its efforts to encourage community collaboration and use of best practices related to security, stability and resiliency through the conduct of ICANN regional registry/registrar workshops, participation in a range of community forums, and sharing of information on its own web site. In 2010, ICANN introduced enhanced reporting of data on gTLD registries on its Dashboard for community use (http://www.icann.org/idashboard/public/).

6.2.2 New gTLDs

The potential implementation of processes related to establishing new gTLDs will provide the primary security, stability and resiliency focus in the upcoming year. In February 2009, the ICANN Board tasked the RSSAC and SSAC to jointly study the potential security, stability and resiliency implications for the root server system as a whole, with regard to a series of potential changes within the DNS including the implementation of new gTLDs and IDNs, along with possible implementation of DNSSEC signing of the root zone. Their reports are expected in 2010. As part of the new gTLD process, ICANN will also establish the provisions for the evaluation of applicants to ensure they can implement operations that are technically secure, are compliant with Whois provisions, can provide for sound contingency planning, and ensure the protection of registrants. ICANN will continue to mature the gTLD registry continuity plan and exercise program. ICANN will also ensure that the automated TLD Applicant System is established and operated in a secure fashion.

6.2.3 IDNs

In a similar vein, ICANN's effort to enable the implementation of IDN TLDs (ccTLDs and gTLDs) will ensure these new domain names represented by local language characters will be secure, stable, and resilient. ICANN is supporting work to update the IDN Guidelines to be followed by the operators of IDN TLDs and operation of second-level IDNs. ICANN will continue to facilitate registries' efforts in working with vendors to ensure that IDN tables are established which limit as much as possible string conflicts and confusions, and reduce opportunities for misuse of the system for malicious purposes. An IDN focused support

function will be made available for those parties interested in becoming an IDN TLD operator and in need of assistance and expertise in the field.

ICANN is also engaged with experts to ensure the stable introduction of IDN TLDs for countries and territories that have more than one appropriate language or script and need to have a synchronized implementation. This also includes collaborating with stakeholders such as browser and application developers, IDN registry operators and others to support the introduction of IDNs.

6.2.4 ccTLDs

ICANN will continue its efforts related to enhancing ccTLD security, stability and resiliency through collaboration with ccTLD operators. In the upcoming year these activities will focus on maturing DNS Capacity Building program, which includes the joint Attack and Contingency Response Planning (ACRP) workshop program that has been established in conjunction with the ccNSO and the regional TLD associations. The DNS Capacity Building program focuses on improved security and resiliency through proactive planning and strong response capabilities against a full range of disruptive threats and risks. The program will expand in the upcoming year to include technical training to improve security and resiliency in response to advancing threats and to provide assistance in the development of exercise and evaluation programs for ccTLD security and contingency planning.

6.2.5 Registrars

The community is preceding with further consideration of enhancements to registrar accreditation and data escrow requirements through improvements to the RAA. In addition to supporting these efforts, ICANN staff will continue to develop procedures and processes within the existing contractual and policy frameworks to protect registrants and ultimately enhance the security, stability, and resiliency of the DNS. In particular, work is under way to tighten accreditation application procedures, establish heightened RAA eligibility requirements and disqualification rules, and develop procedures to allow registrars to exit the registrar marketplace in a responsible manner. Previous work in developing data escrow and registrar termination procedures will also strengthen ICANN's ongoing and future compliance enforcement efforts, allowing for termination of registrar accreditation in cases where registrar actions threaten the security and stability of the DNS. ICANN will continue to build a strong registrar community through outreach events that permit sharing of industry best practices, and will begin implementing

new channels of communication to assist registrars in timely reporting and responding to critical security threats.

6.2.6 Contractual Compliance

ICANN will continue to increase the scope of contractual enforcement activities. Activity will include audits of contracted parties as part of implementing the 2009 RAA. Additionally, Contractual Compliance staff will work collaboratively with ICANN's Security team to identify contracted parties who may be engaged in malicious activity. In those cases where contracted parties have engaged in malicious activity, contract enforcement action may be taken. In all other cases, law enforcement or other appropriate agencies will be notified for proper handling of such matters.

The Contractual Compliance Department has conducted to assess Whois data contact information accuracy within the gTLD system and to assess the extent to which registrants are using privacy and proxy services to shield their identity. In an effort to encourage contract compliance and to provide public confidence, the Contractual Compliance Department is developing a system to publically identify compliant parties. This system is in the early stages of development, and consultation with the registrar and registry communities will be sought before it is implemented.

6.2.7 Collaborative Response to Malicious Abuse of Domain Name System

ICANN staff will also continue to build on collaborative efforts that have emerged in response to recent events involving the Domain Name System since late 2008 such as activities surrounding the Szirbi botnet and Conficker worm in late 2008/early 2009. ICANN envisions such collaboration to involve DNS registries and registrars, the security research community and software and anti-virus vendors. Specifically, ICANN plans to work with registry and registrar communities to enhance collaborative approaches to combat the spread of malware, worms and botnets that use the DNS for propagation and control. ICANN will seek to delineate procedures for communication and validation of registry and registrar activities as well as how it will participate in information sharing with security researchers, technology vendors and law enforcement as appropriate. ICANN will provide for public comment on its procedures for conducting collaborative response activities. These procedures will be submitted to the Board for approval. These approaches will ensure ICANN can be responsive to the full range of global stakeholders that may seek its engagement and collaboration.

6.2.8 Enabling Overall DNS Security

ICANN staff will seek to build on the February 2009 and February 2010 DNS Security, Stability, and Resiliency Symposiums by assisting key collaborative efforts related to mitigating operational risks to the operators and users of the DNS. Plans include convening an annual symposium to review DNS-wide risks and enhancing collaborative opportunities with an ongoing focus of meeting the challenges of ensuring DNS security and stability in the developing world. ICANN also plans to collaborate with DNS-OARC and the Forum of Incident Response and Security Teams (FIRST) with a focus of how to orchestrate effective responses to significant contingencies and events within the DNS community. Additionally, ICANN staff will continue to track the evolution of plans for establishing an Object Naming System (ONS) and how such plans might involve the DNS to ensure that identification of potential issues related to security, stability and resiliency are identified early.

6.3 Global Security Outreach

6.3.1 Extend Existing Partnerships

The core of ICANN's global engagement strategy in relation to security, stability and resiliency is to build upon and use the existing work conducted by Global Partnerships and to further extend strong partnerships. Specific activities planned for FY 11 with these partners include:

- ***Internet Society (ISOC)*** – ICANN plans to collaborate in maturing the ongoing joint ISOC/ICANN program to provide training to TLD operators with additional plans to include technical training in how to improve security and mitigate cyber attacks and disruptions.
- ***DNS-OARC*** – ICANN will continue collaboration with DNS-OARC and other interested stakeholders in support of the SSR Strategic Initiatives and DNS-CERT concept. ICANN has also engaged with organizations in order to conduct education and training in partnership with others to improve understanding of the functioning of the unique identifier systems, ICANN's role, and challenges to managing risks to these systems.

6.3.2 Commercial Enterprise

ICANN will build on the February 2009 and 2010 DNS Security, Stability, and Resiliency Symposium on understanding enterprise reliance on, and risks associated with the DNS. In the upcoming

year, efforts in security, stability and resiliency will be incorporated as part of the ICANN CEO outreach program in seeking to ensure incorporation of a broad range of corporate perspectives.

6.3.3 Participation in Global Cyber Security Dialogue

ICANN will engage these dialogues seeking to ensure a clear understanding of its specific role and contributions. Specific activities envisaged by ICANN in this area during the next year include:

- ***Forum of Incident Response and Security Teams (FIRST)*** – ICANN and FIRST conducted a joint cyber security workshop in Nairobi, Kenya in March 2010 for African incident response teams. ICANN is collaborating with FIRST on a survey of Computer Emergency Response Teams in FY 11, and participating in FIRST programs.
- ***European Network and Information Security Agency (ENISA)*** – ICANN plans to collaborate with ENISA in a European cyber exercise and on cyber incident response activities.
- ***Internet Governance Forum (IGF)*** – ICANN will participate at the IGF meeting in Vilnius, Lithuania in September 2010 and supports the continuation of the IGF by the United Nations General Assembly.

ICANN will actively pursue opportunities with other entities and academic institutions on leadership in identifying challenges regarding security, stability and resiliency.

ICANN plans to continue collaboration with the ASO (and through the ASO, the NRO and RIRs) and to participate in activities of mutual concern related to security, stability and resiliency. ICANN staff will seek to engage the NRO on which collaborative activities to enhance to ensure the security, stability and resiliency of the DNS. These discussions will include understanding NRO's intent regarding the possible misuse of legacy IPv4 address space and the potential need for regional or possibly global policy to address identified concerns.

6.4 ICANN Corporate Security and Continuity Operations

ICANN staff will ensure its security programs are conducted within overall corporate risk management, crisis management and business continuity programs. A major focus continues to be the establishment of a sound foundation of documented policies,

processes and supporting procedures. Recent initiatives have focused on improvements to ICANN enterprise level risk management and continuity posture, including creation of formal ICANN business continuity/crisis management plans and conducting ICANN internal exercises in conjunction with other activities to include gTLD continuity exercises and meeting preparations. ICANN has initiated use of physically distributed alternative operations sites to enhance business continuity and disaster recovery capability for ICANN's IT infrastructure.

As part of ongoing operations in 2010, ICANN staff continues to improve the full spectrum of corporate information, personnel, and security processes. As with risk management and continuity planning, a major focus will be the establishment of a sound foundation of documented plans and supporting procedures. Specific initiatives underway in 2010 to improve ICANN's security posture include improvements to logical and physical access controls, change management, logging/auditing and data backup procedures, security awareness training for staff, building incident response capabilities and improvements to mobile device security. Documented security plans for personnel and ICANN Global Meetings have been prepared and outside validation and review of those plans is scheduled for late 2010. ICANN will ensure that evolving community collaboration and outreach IT tools are developed and deployed with proper security controls in place.

ICANN plans to have an outside review and audit of its security and continuity programs conducted during the second half of 2010.

6.5 ICANN Support Organizations and Advisory Committees

SSAC plans to focus its upcoming efforts on DNSSEC deployment, protection of domain registration, and reduction in misuse of domain names and address system stability.

In January 2009, the GNSO Council issued an Initial Report on fast flux hosting for public comment and further council action and is also considering numerous possible studies of related Whois. The GNSO Council has a working group focusing on the second of six planned policy development efforts addressing various aspects of inter-registrar transfers. The GNSO has convened a Registration Abuse Working Group and is considering an initiative related to post-expiration domain name recovery. To bring the wide range of ICANN stakeholders with interests in these topics together, several ICANN international public meetings have included an

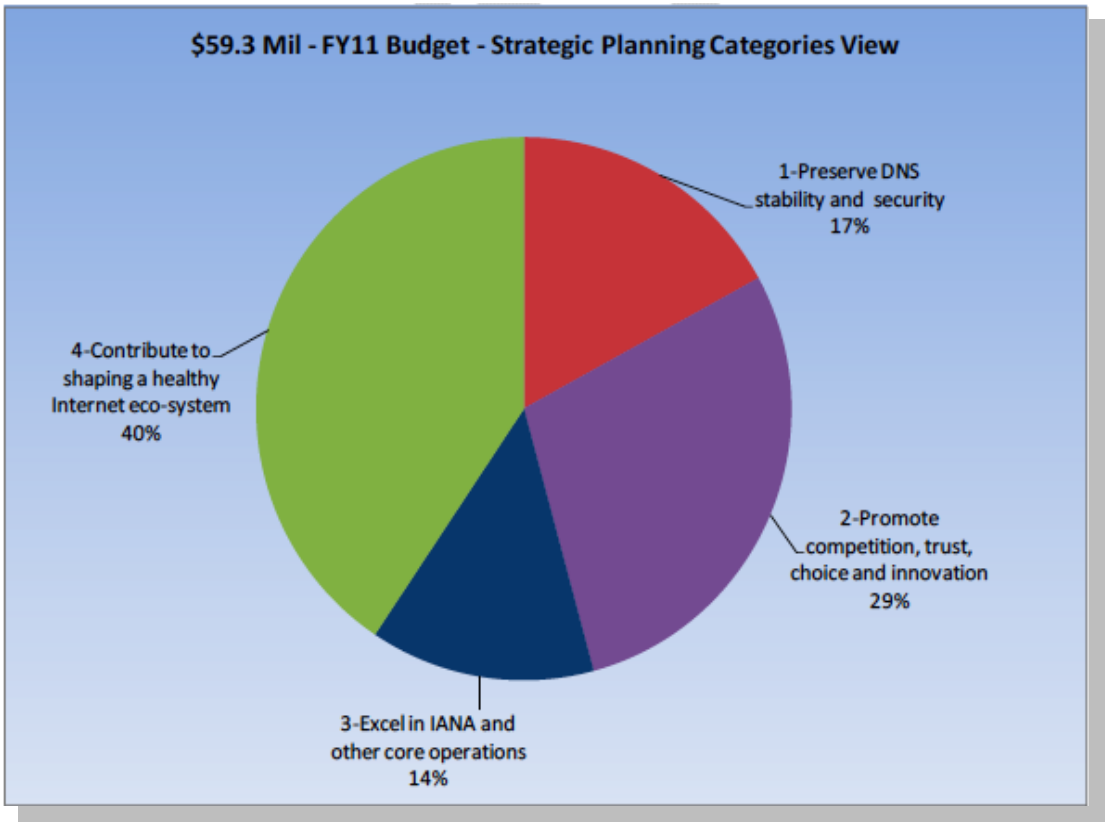
extended workshop on e-crime and registration abuse (in Mexico City, Seoul, Nairobi, Brussels).

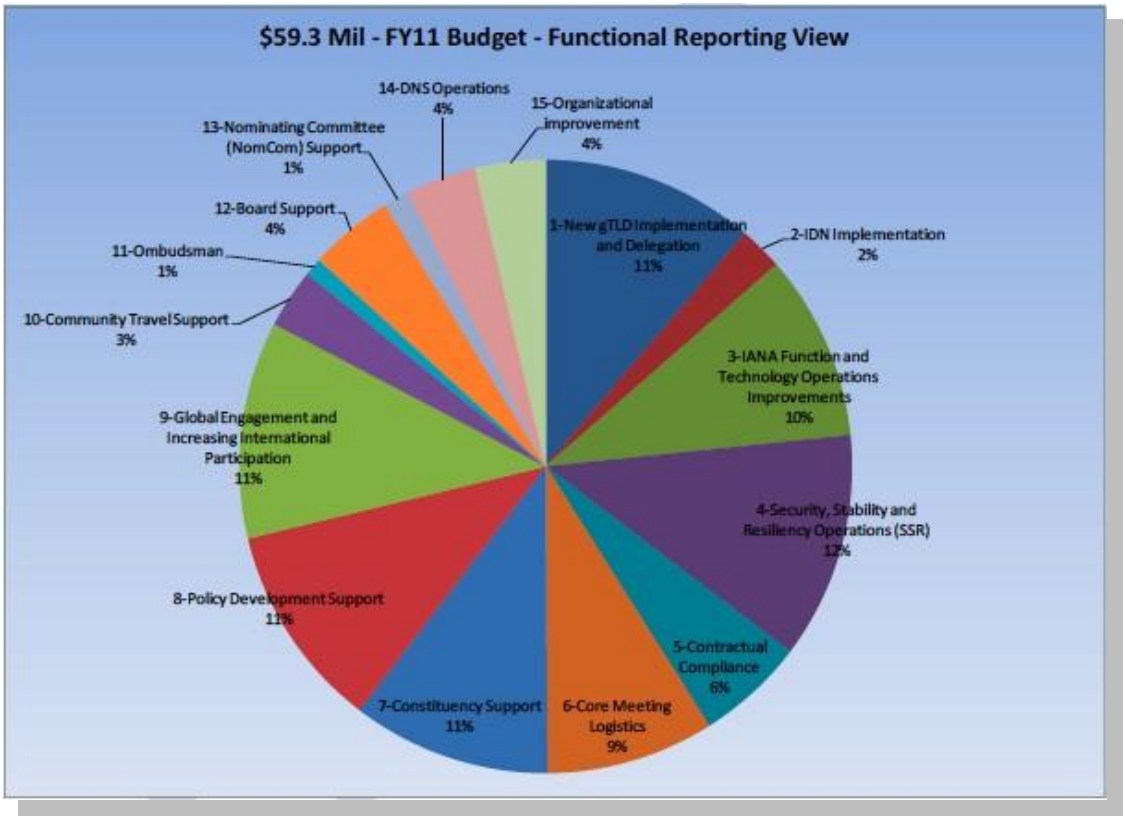
7. Conclusion

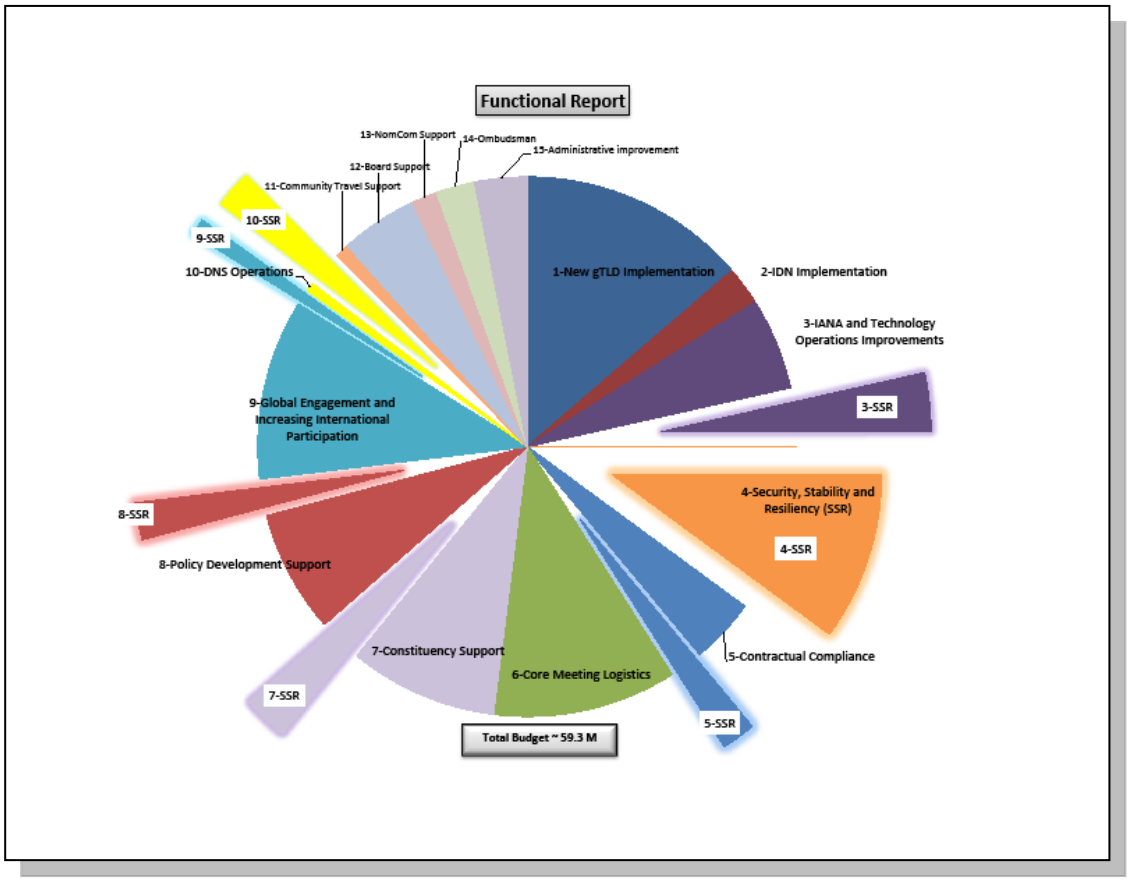
ICANN understands that, as a crucial aspect of its mission of public trust, its programs and activities must contribute to making the unique identifier systems a core aspect of a more secure, stable and resilient Internet environment. Challenges are growing and ICANN's efforts in this area are becoming more vigorous. ICANN also recognizes the limits to its role and resources, and plans its strategy in this area to rely heavily on collaboration. The Internet has thrived as a global environment, fostering innovation, and relying on multi-stakeholder coordination. ICANN's contribution to improving security, stability and resiliency of its unique identifier systems will rely on the same approach.

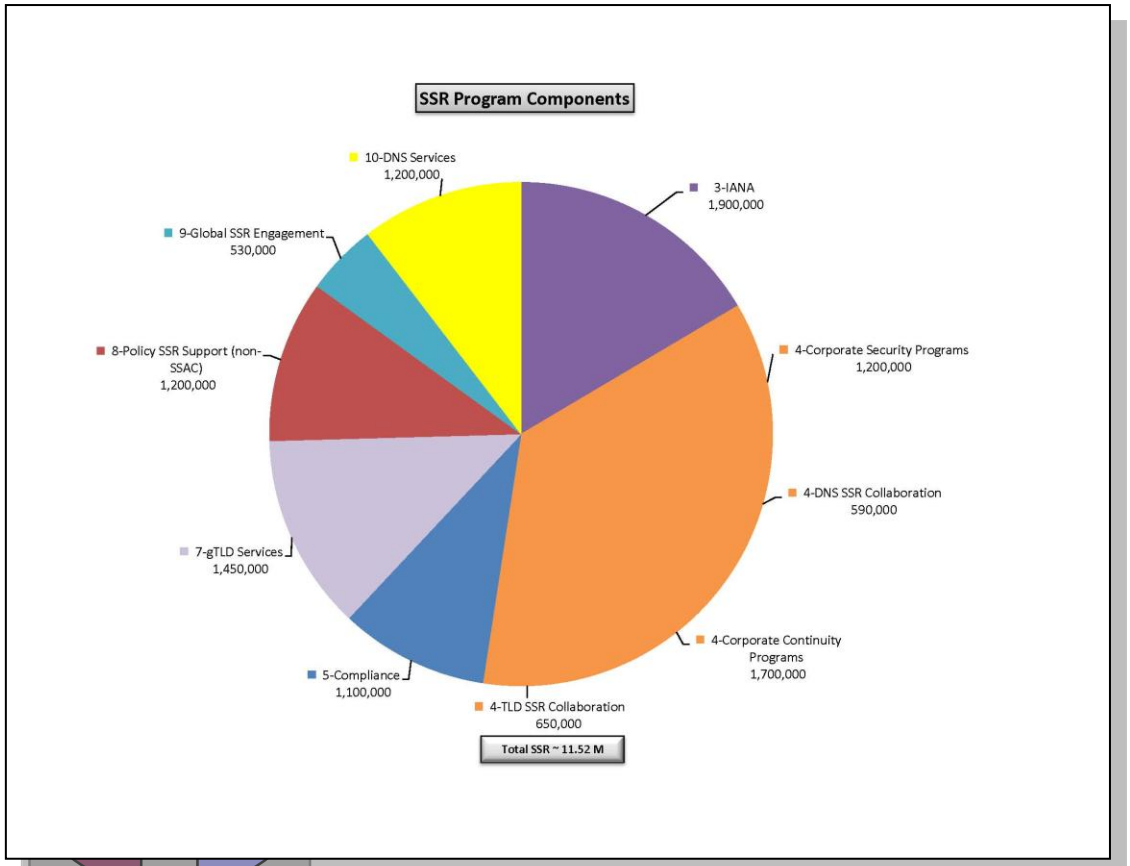
Since its inception ICANN has conducted programs and activities to improve the security, stability and resiliency of the Internet that include efforts related to core DNS/addressing functions; working with the TLD registry and the registrar communities; engagement with the NRO and RIRs; corporate security and continuity programs; activities of the supporting organizations and advisory committees, and participation in global and regional Internet security, security and stability activities. The intent of this first version of the plan is to provide a foundation on which to develop ICANN's role and the framework around which ICANN organizes its security, stability and security efforts. The plan will evolve over time as part of the ICANN strategic and operational planning process allowing ICANN efforts to remain relevant and to ensure its resources are focused on its most important responsibilities and contributions.

Appendix A–FY 11 SSR Resourcing




$59.3 Mil - FY11 Budget - Functional Reporting View
1-New gTLD Implementation and Delegation 11%
2-IDN Implementation 2%
3-IANA Function and Technology Operations Improvements 10%
4-Security, Stability and Resiliency Operations (SSR) 12%
5-Contractual Compliance 6%
6-Core Meeting Logistics 9%
7-Constituency Support 11%
8-Policy Development Support 11%
9-Global Engagement and Increasing International Participation 11%
10-Community Travel Support 3%
11-Ombudsman 1%
12-Board Support 4%
13-Nominating Committee (NomCom) Support 1%
14-DNS Operations 4%
15-Organizational improvement 4%


Functional Report
13-NomCom Support
14-Ombudsman
15-Administrative improvement
12-Board Support
11-Community Travel Support
10-SSR
9-SSR
10-DNS Operations
1-New gTLD Implementation
2-IDN Implementation
3-IANA and Technology Operations Improvements
3-SSR
9-Global Engagement and Increasing International Participation
4-Security, Stability and Resiliency (SSR)
4-SSR
8-SSR
8-Policy Development Support
7-Constituency Support
6-Core Meeting Logistics
5-Contractual Compliance
7-SSR
5-SSR
Total Budget ~ 59.3 M


SSR Program Components
10-DNS Services
1,200,000
3-IANA
1,900,000
9-Global SSR Engagement
530,000
8-Policy SSR Support (non-SSAC)
1,200,000
4-Corporate Security Programs
1,200,000
4-DNS SSR Collaboration
590,000
7-gTLD Services
1,450,000
4-Corporate Continuity Programs
1,700,000
5-Compliance
1,100,000
4-TLD SSR Collaboration
650,000
Total SSR ~ 11.52 M

Overview of Major Components of ICANN Security, Stability, Resiliency (SSR) Program

- IANA - $1.9 M
- DNS Services - $1.2 M
- DNS SSR Collaboration - $590 K
- gTLD Services - $1.45 M
- Compliance - $1.1 M
- TLD SSR Collaboration - $650K
- Global SSR Engagement - $530K
- Corporate Security Programs - $1.2 M
- Corporate Continuity Programs - $ 1.7M
- Policy SSR Support (non-SSAC) - $550K
- SSAC Support – $650K

OVERALL SSR - $11.52M

IANA Security, Stability and Resiliency (IANA)

Objectives	Deliverables (milestones)
- Automation of key elements in root zone change process - DNSSEC management - Test rPKI implementation - Business continuity	- Implementation of automated RZM (dependent on partners NTIA & VeriSign) - Implement DNSSEC signing of .ARPA (date depends on coordination with IAB & NTIA) - Coordination with rPKI testers - IANA Continuity Plan (exercised in Jan 2010, on-going exercise of plan in FY 11)
Key Stakeholders	**Resources**
- IANA, Security, IT - DOC/USG; Verisign - SSAC; RSSAC - IETF; DNS operator community - RIRs; routing operational community	- Staffing – 6.5 FTE (including 2.5 FTE for related IT and other staff support) - Financial – $1.9 M to support FTEs; staff support/travel; professional services; application development

ICANN DNS Operations

Objectives
- DNSSEC activities and periodic key rollover
- Implement ICANN signing .arpa and zones
- Trust Anchor Repository (TAR)
- Secure, resilient L-root operation

Deliverables (milestones)
- Key rollover in FY 11, at Culpeper and LAX facilities
- DNSSEC signed ICANN zones
- Trusted repository in operation
- L-root improvement

Key Stakeholders
- ICANN DNS Ops, IT Teams
- ICANN IANA staff, DoC, VeriSign
- ICANN Security Team

Resources (FY 11)
Human – 7.0 FTE (including related IT and other staff support)

Financial – $1.2M to support FTEs; planned capital investments for back-up services; DNSSec, L-root, improvements; backup facilities; professional services and travel

ICANN gTLD Registry/Registrar Services (Services)

Objectives
- Ensure implementation new gTLD/IDNs addresses SSR issues
- Continue maturing data escrow process & gTLD continuity plan
- Conduct RSEP/RSTEP processes

Deliverables
- Enhanced gTLD implementation process from SSR perspective
  - Root Scaling complete (in FY 11)
  - Improved Applicant Guidebook (Nov 10)
- Data escrow exercises (Aug-Nov 10)
- HSTLD RFI (Sept-Nov 10)
- Malicious Conduct provisions

Key Stakeholders
- Registries/Registrars
- ICANN Services staff
- ICANN Security & Continuity staff
- GNSO/SSAC

Resources (FY 11)
Human – 2.75 FTE

Financial – TBD new gTLD budget - includes portion of evaluation staff/support for new gTLD/IDN activities to include TAS security; dedicated RSEP/RSTEP funds; support for testing/contingency exercise; staff travel/support

Contractual Compliance (Services)

Objectives	Deliverables
- Improved ICANN compliance process - Improved compliant and WDPRS system - Improved WHOIS data accuracy	- Conduct audits as part of 2009 RAA implementation - Improvements to WDPRS (Aug-Nov 10) - Additional WHOIS studies dependent on GNSO Council recommendation
Key Stakeholders - gTLD registry/registrars - ICANN Compliance staff - ICANN Security/Continuity staff	**Resources (FY 11)** Human – 3 FTE Financial – $1.1M support for FTEs, staff/travel support; professional services to conduct studies and support systems improvements;

TLD Security, Stability & Resiliency Collaboration

(Security)

Objectives	Deliverables (milestones)
- Mature DNS Capacity Building Program - Establish joint ISOC/ICANN tech training program - Conduct TLD exercise planning workshops - Establish program metrics	- Conduct ACRP training sessions remaining in 2010 - Joint technical training with ISOC plan, transition in 2010 - Conduct exercise planning workshops - Prototype metrics from DNS Symposium
Key Stakeholders - ccTLD operators - ccNSO, regional TLD operators - ISOC/NSRC - ICANN staff	**Resources (FY 11)** Human – 1 FTE Financial – $650K for FTE, staff/travel to support; professional services for developing and conducting training programs

DNS Security, Stability & Resiliency Collaboration

(Security)

Objectives	Deliverables (milestones)
- Establish collaborative response mechanisms to DNS abuse - Share key SSR practices - Conduct community-based DNS risks and collaboration - Enhance root server SSR collaboration	- Collaboration construct and on-going responses w/ partners - Conduct & report on symposium (Feb & Mar 2011) - Report on root ops exercise (TBA 2010)
Key Stakeholders	**Resources (FY 11)**
- ISOC, DNS-OARC, FIRST - Root Server community - Broader DNS ops community - ICANN staff - RSSAC/SSAC	Human – 1.25 FTE Financial – $590K for FTE, professional services for portal and collaboration support, travel to support activities

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

Objectives	Deliverables

- Improve and implement IT/Facilities/ Personnel Security Programs
  - Implement Formal Plans
  - Institute Security Training
- Implement Traveler and Meetings Security & Contingency Plans
	- Conduct Security Training Programs (embedded part of ICANN on-boarding as of Sep 2009)
	- Improved IT & Physical Access Control Systems implemented (improved IT authentication on key systems – Fall 09)
	- Exercise Traveler and Meetings Security (one drill per trimester)

Key Stakeholders	**Resources**
- ICANN Security & Resiliency Team - ICANN IT/IANA/DNS Ops - ICANN Human Resources - ICANN Global Meetings Team - Other ICANN Staff	Human – 2 FTEs (includes IT support for security) Financial – $1.1 M including FTEs, physical & IT access controls, professional services for conducting training and audits

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

Objectives	Deliverables

- Improve Business Continuity program
  - Establish formal plan
  - Establish secure data center
  - Establish formal drill/exercise programs
	- Internal ICANN Business Continuity plan (Oct 10)
	- Improve data center resiliency
	- Exercise Business Continuity/Crisis Management (Oct 10-Mar 11)

Key Stakeholders	**Resources**
- ICANN Security Team - ICANN IT/IANA/DNS Ops - ICANN Human Resources - ICANN Global Meetings Team - ICANN Staff	Human – 5 FTEs (includes planning and IT for data center) Financial – $1.7M including FTEs, capital support for data center, professional services for conducting training and audits

Global Security, Stability and Security Engagement

(Global Partnerships & Security)

Objectives	Deliverables
- Sustain partnerships with key organizations (ISOC; IISI; IMPACT; EC/ENISA; CSIS; Atlantic Council) - Continue participation in IGO sponsored cyber security dialogues OECD, IGF, others) - Collaborate with others on global cyber security response	- Conduct joint activities with partner organizations (One per trimester) - Engagement in forums across all major regions (On-going) - Membership in Forum of Incident Response and Security Teams (FIRST)
Key Stakeholders	**Resources (FY 11)**
- Global/international organizations - ISOC; IETF; ITU; IGF - Cyber security forums - Governments/Commercial Stakeholders - ICANN Global Partnerships Team & Security Staff	Human – 1.5 FTE Financial – $530K for FTEs; staff/travel support; support to ICANN-led or supported forums; professional services support for metrics development

Policy Support for SSR-related efforts (Policy)

Objectives	Deliverables
Set by supported SO/ACs conducting SSR activity - GNSO; ccNSO - GAC - RSSAC; ALAC	- Derive from FY 11 work plans as they are established
Key Stakeholders - Named SO/ACs - ICANN policy staff - ICANN security staff	**Resources (FY 11)** Human – 2 FTE Financial – $550K for FTEs and limited additional funding support for SSR-related activities

Security and Stability Advisory Committee (SSAC)

Objectives	Deliverables
- Foster DNSSEC Deployment - Ensure Root Zone stability with growth and complexity - Protection of domain registration - Reduction in domain name abuse - Address system stability	- Reports, Advisories, Comments - Root Scaling Studies - Domain name protection study - Registration data study: display, access, accuracy
Key Stakeholders - External Internet security community - IANA and Root Server community - GNSO and CCNSO - ALAC - ASO - ICANN staff - GAC and Board	**Resources (FY 11)** Human – 1.5 FTE Financial – $650K for FTEs and limited additional funding support for related travel and publications; support for completing root scaling studies

Appendix B – Glossary of SSR Plan Terms and Acronyms

ACRP – Attack Contingency Response Planning

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

APWG – Anti Phishing Working Group

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

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

ccTLD – country code Top Level Domain

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

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

FIRST – Forum of Incident Response and Security Teams

gTLD – generic Top Level Domain

IANA – Internet Assigned Numbers Authority

IDN – Internationalized Domain Name

IETF - Internet Engineering Task Force

IP – Internet Protocol specifies the format of packets and the addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which

establishes a virtual connection between a destination and a source. By itself IP is something like the postal system. It allows you to address a package and send it using the system, but there's no direct link between your packet and the recipient. TCP/IP creates the connection between two hosts so that they can send messages back and forth.

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

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

ISOC – Internet Society

IT – Information Technology

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

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

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

Distributed Denial-of-Service attack (DDoS) – a type of denial of service attack in which an attacker uses malicious code installed on multiple systems in order to attack a single target. This method has a greater effect on the target than is possible with just a single attacking machine. On the Internet, a distributed denial-of-service attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. DDoS attacks are most effective

when launched via a large number of open recursive servers: distribution increases the traffic and decreases the focus on the sources of the attack. The impact on the misused open recursive servers is generally low, but the effect on the target is high. The amplification factor is estimated at 1:73. Attacks based on this method have exceeded 7 Gigabits per second.

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

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

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

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

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

income from advertisements being placed on the domain's website.

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

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

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

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

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

NOG – Network Operations Group

NRO – Number Resource Organization

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

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

RAA – Registrar Accreditation Agreements

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

Registrar - a company authorized to register Internet domain names

RIR – Regional Internet Registry

RPKI – Resource Public Key Infrastructure

RSEP – Registry Services Evaluation Process

RSTEP – Registry Services Technical Evaluation Panel

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

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

TLD – Top Level domain

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

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

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