Plan for Enhancing Internet Security, Stability, and Resiliency

June 2009

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 5
2. Challenge and Opportunity 6
3. ICANN Role 8
4. ICANN Contributors to Security, Stability and Resiliency Efforts 11
5. ICANN's Ongoing Programs Related to Security, Stability and Resiliency 13
5.1 Core DNS/Addressing Security, Stability and Resiliency 13
5.1.1 IANA Operations 13
5.1.2 DNS Root Server Operations 15
5.2 TLD Registries and Registrars Security, Stability and Resiliency 16
5.2.1 gTLD Registries 16
5.2.2 New gTLDs and IDNs 17
5.2.3 gTLD Registrars 17
5.2.4 Whois 18
5.2.5 Contractual Compliance 19
5.2.6 Protecting gTLD Registrants 19
5.2.7 ccTLDs 20
5.2.8 IANA Technical Requirements 20
5.2.9 Collaborative Response to Malicious Abuse of Domain Name System 21
5.2.10 Enabling Overall DNS Security and Resiliency 21
5.3 Engaging with the Regional Internet Registries 22
5.4 ICANN Corporate Security and Continuity Operations 22
5.5 Activities of ICANN Supporting Organizations and Advisory Committees 23
5.6 Global Engagement to Enhance Security, Stability and Resiliency 25
5.6.1 Global Partners and Activities 25
5.6.2 Regional Partners and Activities 26
5.6.3 Working with Governments 27
6. ICANN FY10 Plans to Enhance Security, Stability and Resiliency 28
6.1 Core DNS/Addressing Functions 29
6.1.1 IANA Operations 29
6.1.2 DNS Root Server Operations 30
6.2 Relationships with TLD Registries and Registrars 30
6.2.1 gTLD Registries 30

6.2.2 New gTLDs 31
6.2.3 IDNs 31
6.2.4 ccTLDs 32
6.2.5 Registrars 32
6.2.6 Contractual Compliance 32
6.2.7 Collaborative Response to Malicious Abuse of Domain Name System 33
6.2. 8 Enabling Overall DNS Security 33
6.3 Engaging with the Regional Internet Registries (RIRs) 34
6.4 ICANN Corporate Security and Continuity Operations 34
6.5 ICANN Support Organizations and Advisory Committees 35
6.6 Global Engagement 35
6.6.1 Extend Existing Partnerships 35
6.6.2 Commercial Enterprise 36
6.6.3 Participation in Global Cyber Security Dialogue 36
7. Conclusion 37
Appendix A 38
Appendix B – Glossary of SSR Plan Terms and Acronyms 46

Executive Summary

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

The ICANN 2009-2012 Strategic Plan (www.icann.org/en/strategic-plan/strategic-plan-2009-2012-09feb09-en.pdf) states "Security, stability and resiliency will remain a top priority and ICANN will work effectively with other Internet stakeholders to enhance and protect the security and stability of the Internet, paying particular attention to ICANN's mission to protect the security, stability and resiliency of the Internet's systems of unique identifiers." The strategic plan identifies a number of objectives across the broad range of ICANN's security, stability and resiliency responsibilities. The Strategic Plan addresses security, stability and resiliency concerns under Priority 2 – Enhance security, stability and resiliency in the allocation and assignment of the Internet's unique identifiers. Priority 2 states: 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 improve 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. The principal objective for this priority is to ensure that the Internet's unique identifier systems remain viable and its operation robust over the life of the plan.

Specific objectives identified within Priority 2 of the Strategic Plan are:

1. Deliver plan for consultation that sets out ICANN's role in Internet security, stability and resiliency; identify appropriate partners and commence joint work. Define ICANN's role so that scope of efforts, costs and deliverables are well understood and initiate a process that leads to agreement by the community and the Board in 2009. Effectively work with partners to pursue multi-

[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.

stakeholder approaches and conduct programs that contribute to the global security, stability and resiliency of the Internet. Metrics for these programs will be established by the end of 2009 and initial program evaluations by mid-2010.

2. Provide mechanisms that will allow users to validate the authenticity of the Internet identifiers that ICANN publishes and contribute broadly to technical efforts to provide more securable Internet naming and addressing systems. Specifically, ICANN will endeavor to work with key stakeholders to ensure the DNSSEC signing of the DNS root zone by the end of 2009 and to foster the implementation of rPKI to enhance addressing security and stability.

3. Conduct focused programs to enhance the understanding of risks and enhance the security and resiliency of organizations associated with the TLD community. Programs will include working with partners to establish an effective approach to sharing best practices across the community by end of 2009 and conducting ongoing regionally based training and exercise programs for this community over the life of this plan.

4. Work with stakeholders across the ICANN community to orchestrate ongoing collaboration to understand risks and to enhance the security and resiliency of the DNS against a full spectrum of threats over the life of the plan. ICANN will work with partners to establish approaches to measuring operational risks to the DNS and its users by mid 2010.

The ICANN Plan for Enhancing Security, Stability and Resiliency provides the document called for in objective 1, further delineating ICANN's specific role in addressing security, stability and resiliency, overviews the ICANN programs in this area, and details planned activities that will enhance its contributions through the next operational year. The first version of the plan is intended as a foundation for ICANN and its community regarding its role and to establish the framework for organizing its security, stability and resiliency efforts. The plan does not envision major new roles or programs for ICANN in this area.

ICANN's Role

ICANN acts in accordance with its bylaws in conducting multi-stakeholder, consensus-based processes to establish its 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 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 the 2009–2010 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*** – In accordance with the ICANN 2009-2012 Strategic Plan, ICANN should be operationally ready to implement DNSSEC for the authoritative root zone, as well as work with the Internet community to remove obstacles to adoption of DNSSEC.

ICANN is ready, willing and able to sign the root. Per its September 2008 proposal, ICANN's current and planned efforts are addressed in sections 5.1.1 and 6.1.1. Other initiatives include 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 Generic top level domain (gTLD) and Internationalized Domain Name (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 with country code top level domain (ccTLD) registries on maturing the joint Attack and Contingency Response Planning (ACRP) program that has been established in conjunction with the Country Code Names Supporting Organization (ccNSO) and the regional top level domain (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 March 09 Amendments to Registrar Accreditation Agreement (RAA) and identify potential involvement of contracted parties in malicious activity for compliance action.
- ***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.
- ***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 establishment of a sound foundation of documented plans and supporting procedures.
- ***Ensure Global Engagement and Cooperation*** – ICANN will continue to enhance partnerships to include the Internet Engineering Task Force (IETF), Internet Society (ISOC), Regional internet Registries (RIR)s and Network Operators Groups (NOG)s, and the DNS–Operations, Analysis and Response Center (DNS-OARC). 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

This 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 FY10 Plans to Enhance Security, Stability and Resiliency
- Section 7: Conclusion
- Appendix A: ICANN FY 10 Security, Stability and Resiliency Program Objectives, Partners, Milestones/Deliverables and Resourcing

As stated in the Executive Summary, this plan builds upon the vision and objectives laid out in the ICANN 2009–2012 Strategic Plan. The first version of the plan is intended to be a foundation for ICANN and its community regarding its role, and to establish the framework for organizing its security, stability and resiliency efforts. The plan does not envision major new roles or programs for ICANN in this area. The plan will be updated annually 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. Increasing concern has been expressed over the past few years by the full range of Internet stakeholders: 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 FY10 activities, milestones and associated resources. A major focus of the ICANN security staff's FY10 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 to establish 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 risks and threats. 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 or dialogues related to the use of the Internet for cyber-espionage and cyber war. Also, ICANN will not involve itself in discussions as 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 spam) 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) to include signing the DNS root zone. ICANN has proposed an approach that allows the uninterrupted continuation of the DNS root distribution mechanism, a shared task between ICANN, VeriSign, NTIA and root server operators in the operation of DNSSEC. ICANN has provided flexible solutions that accommodate an interim approach that can transition to a permanent solution, and has made operational preparations to play this role. Other key efforts will focus on improving the system-wide understanding of risks, enabling root-level implementation of 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 has entered into contracts 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 the major focus of the activities going forward.
- 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. 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. The IANA functions' staff has established plans for implementation of DNSSEC at the root level and for ICANN managed DNS zones. Specific activities related to security, stability and resiliency are outlined below.
- ***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 Relations/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.

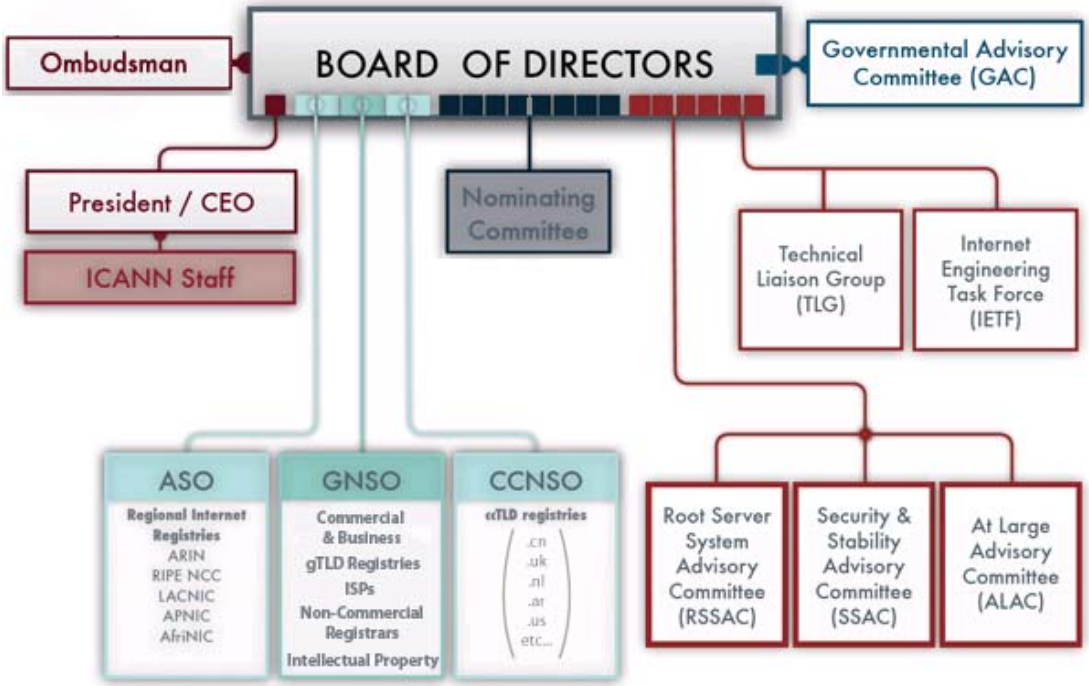


Figure 1 – ICANN organization structure

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

This section delineates 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 3.4, 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 authentication 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.

ICANN has advocated for the need to implement DNSSEC at the root-level, made a proposal to Department of Commerce regarding the IANA functions' role in conducting root level signing in September 2008, and conducted preparations to fulfill that role as well as to sign the .int and .arpa domains. These 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.

Additionally, ICANN has worked with RIRs and the IETF on the development of rPKI technology to introduce authentication of assigned numbering resources. 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.

5.1.2 DNS Root Server Operations

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.

ICANN will continue work to formalize relationships with root name server operators as it committed to in the "2006 ICANN Board Affirmation of Responsibilities for ICANN's Private Sector Management." In 2008, ICANN reached a mutual responsibilities agreement with the Internet Systems Consortium regarding operation of the F-root that reinforced a "commitment to further enhancing the stability, security and interoperability of the Internet's Domain Name System (DNS) from a global perspective and for the benefit of the global Internet community in an evolutionary manner on the basis of a peer relationship."

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.

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. Additionally, gTLD registries each have a contract with ICANN. While some elements of these contracts 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 by ICANN. Other provisions of the agreement 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 a gTLD 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 deal with 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.

5.2.2 New gTLDs and IDNs

As ICANN prepares to open processes for new TLDs 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. The process for introduction of IDN ccTLDs will follow a different process as this initial introduction is limited to noncontentious strings that represent countries and territory names corresponding to the existing ccTLDs. SSAC provided comments on the impact of IDNs on the security and stability at the root-level of the DNS in July 2007 informing implementation planning and testing processes.

An independent team of experts will conduct the technical evaluation of applicants and their proposed TLDs. Additionally, the new gTLD process provides for an upfront RSEP process to assess potential security or stability issues of new registry services that are proposed in the gTLD application. For IDN TLDs, the technical string requirements and associated evaluation is the same for the IDN gTLDs and the IDN ccTLDs.

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.

5.2.3 gTLD Registrars

ICANN also collaborates with the registrars on issues related to security, stability and resiliency. Contractually, ICANN's relationship with registrars is governed by a standard RAA. 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.

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 and will continue efforts to address these concerns.

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. Complaints regarding possible RAA violations are investigated by contractual compliance staff 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 registrar and Intellectual Property constituencies (IPC), the WDPRS was redesigned in 2008 to address several concerns raised by the Internet community including limited functionality, limited capacity and the lack of compliance follow-up. The redesigned WDPRS was launched in December 2008. The Compliance team is continuing to improve this system with the objective of increasing Whois data accuracy.

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. The SSAC advisories have provided guidance to registrars about practices to improve the protection of domain names and concerns related to fast flux, misuse of Whois data and name hijacking as well as registrant concerns about issues such as renewal considerations. Beyond SSAC, 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. 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 for the range of agreements between individual ccTLD registries and ICANN. ICANN's principal focus in fostering enhanced security, stability and resiliency with the ccTLDs is, through teaming with 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, through the IANA functions, 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. ICANN is actively working with registries and registrars to ensure awareness and to facilitate dissemination of information. 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.

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. 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 domain and sub domain names.

ICANN plans to stress this 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.

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.

5.3 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 the .arpa domain and its subdomains. The RIRs are developing the means to enable authentication of IP addresses and AS numbers through the rPKI effort. In the near term, this effort will provide an authenticated correlation between the number resource holder and the number resource. This authentication system can serve as the basis for the development of a means to authenticate Border Gateway Protocol routes. ICANN will continue to seek to be a partner on these efforts.

5.4 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 has worked toward a full spectrum security program that manages risk across its information, personnel and physical assets. In fall 2008, ICANN hired a Director of Security Operations responsible for this program. ICANN provides information, processes sensitive data, and relies on use of Information Technology (IT) to conduct operations. The ICANN Information Security Plan is benchmarked from ISO 27002 standards and improvements to supporting procedures/ processes are under way. 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. Personnel security planning focuses on protecting ICANN personnel at both its principal work locations, and as they conduct ICANN's set of global activities, to include ensuring security at ICANN meetings. ICANN has established a planning process to manage

risks related to personnel security and leverages its own internal security team as well as support from security consultants. ICANN has established a planning process to manage risks related to physical facilities to include its main location in Marina del Rey, California, USA, as well as hub offices and backup facilities.

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

5.5 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. These global policies are developed by the separate RIR communities. 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/).

5.6 Global Engagement to Enhance Security, Stability and Resiliency

5.6.1 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 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.

5.6.2 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 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 and 2009 with the support of the German/American Marshall Center for Strategic Studies and both plan to continue collaboration.
- ***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 prior to the 34th ICANN international public meeting held in March 2009 and has planned future sessions with LACTLD. ICANN will also provide ccTLD training in conjunction with the African Top Level Domains Association (AfTLD) and ISOC-Africa. These activities were initiated in April 2009 at the African Top Level Domains Organization (AFTLD) meeting in Arusha, Tanzania.

5.6.3 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 Organisations 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.

6. ICANN FY10 Plans to Enhance Security, Stability and Resiliency

ICANN activities relating to enhancing security, stability and resiliency, and the resources allocated to these efforts, are guided by strategic and operational planning processes. Projecting forward into the 2009-2010 operating year, ICANN plans call for the conduct of a number of key initiatives, including:

- ***IANA Operations*** – Advocate, educate and prepare for DNSSEC implementation at the root level as called for in the ICANN 2009-2012 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 joint Attack and Contingency Response Planning (ACRP) 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 March 09 Amendments to Registrar Accreditation Agreement (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 establishment of a sound foundation 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, and the DNS–Operations, Analysis and Response Center (DNS–OARC). 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 10.

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.

Work with root zone management partners, the US Department of Commerce and VeriSign, and in consultation with the global Internet community to implement a DNSSEC signing process for the root zone. ICANN will continue to pursue implementation of a process as outlined in its September 2008 proposal. Per the priority laid out in the 2009–2012 strategic plan, ICANN will be operationally ready to deploy DNSSec in the root zone by the end of 2009. ICANN has proposed an approach that allows the uninterrupted continuation of the DNS root distribution mechanism, a shared task between ICANN, VeriSign, NTIA and root server operators in the operation of DNSSEC. ICANN has provided flexible solutions that accommodate an interim approach that can transition to a permanent solution, and has made operational preparations in order to play this role.

ICANN will also pursue a range of activities to enable broader DNSSec implementation throughout the DNS globally. 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), running its testbed and facilitating lessons learned effort among those involved in DNSSEC implementation.

Other 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 secure 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.

6.1.2 DNS Root Server Operations

ICANN will continue to seek mutual recognition of roles and responsibilities with root operators as part of its overall role in coordination of the DNS. ICANN also 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. 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. Additionally, ICANN plans to work with DNS–OARC to establish a portal for information sharing related to security, stability, and resiliency best practices and collaborative efforts for use by the full registry community.

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 over the following 18 months. Their report on this study is expected September 2009. 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, to include a live test of the data escrow system. 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 will continue to work with the IETF in their general role in establishing Internet protocols to ensure the finalization of the revision and hence approval of a secure, stable IDN protocol. In the event the IETF-developed protocol is not fully approved, ICANN, with recommendations from the technical community, may establish additional specific requirements on the IDN TLDs to ensure that they will work long-term as well when the protocol revision is finalized. 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.

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 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 ACRP 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. Over the next year ICANN plans to establish a capability to deliver the ACRP program in non-English languages and to work with the Software Engineering Institute at Carnegie-Mellon University to use its Resiliency Engineering Framework (REF) in a voluntary program to assess the maturity of TLD security, stability and resiliency efforts.

6.2.5 Registrars

ICANN will continue policy development to enhance 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 to include increasing the size of the Contractual Compliance staff. Major new areas of activity will include initiating audits of contracted parties as part of implementing the March 09 Amendments

to Registrar Accreditation Agreement (RAA). Additionally, in 2009 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 studies under way 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 DNS Security, Stability, and Resiliency Symposium 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 Engaging with the Regional Internet Registries (RIRs)

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 will be to establish a sound foundation of documented plans and supporting procedures. Specific initiatives to improve ICANN risk management and continuity posture through mid-2010 will include formalizing ICANN business continuity/crisis management plans and conduct of ICANN internal exercises in conjunction with other activities to include gTLD continuity exercises and meeting preparations. ICANN will improve its use of alternative sites as part of IT continuity implementation. A major effort will establish a secure IT center and backup facilities to support ICANN continuity programs. ICANN plans to conduct an enterprise security risk assessment by mid-2009.

During the next year, ICANN staff will ensure that a full spectrum of information, personnel, and security processes are in place across its operations. 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 to improve ICANN's security posture through mid-2010 will include improvements to logical and physical access controls, employee awareness and incident response training, the traveler security plan and meeting security planning and response. ICANN will ensure that evolving

community collaboration and outreach IT tools are developed and deployed with proper security controls in place.

ICANN staff plans to work with the Software Engineering Institute (SEI) at Carnegie-Mellon University to leverage the SEI Resiliency Engineering Framework (REF) to ensure its security, continuity and risk management programs incorporate best practices, and to measure improvements to maturity over time. By the end of 2009, ICANN plans to have assessed its baseline process maturity in line with the REF approach. Additionally, ICANN plans to have an outside review and audit of its security and continuity programs conducted during the first 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, the 34th ICANN international public meeting in Mexico City, March 2009 included an extended workshop on e-crime and a second workshop exclusively focused on registration abuse.

6.6 Global Engagement

6.6.1 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 10 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 sponsor the formation of a DNS–OARC hosted portal for information exchange and sharing of security, stability and resiliency best practices within the TLD community. 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.
- ***Asia*** – ICANN plans to explore a relationship with the new international cybersecurity center being supported by the Malaysian government with a focus on how ICANN can contribute to global efforts to combat malicious cyber activities that may threaten Internet unique identifier systems.

6.6.2 Commercial Enterprise

ICANN will build on the February 2009 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.

6.6.3 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:

- ***Center for Strategic and International Studies (CSIS)*** – ICANN plans to jointly sponsor a series of workshops during 2009–2010 to include addressing the issue of the role of multi-stakeholder organizations in global cybersecurity. These collaborative efforts will include workshops with CSIS partner institutions outside of the United States.
- ***Atlantic Council*** – ICANN plans to collaborate with the Atlantic Council on activities related to addressing the growing vulnerabilities of smaller nations and organizations in the face of growing cyber attacks and protests. ICANN will focus on its role in enabling DNS resiliency in the face of such activity.

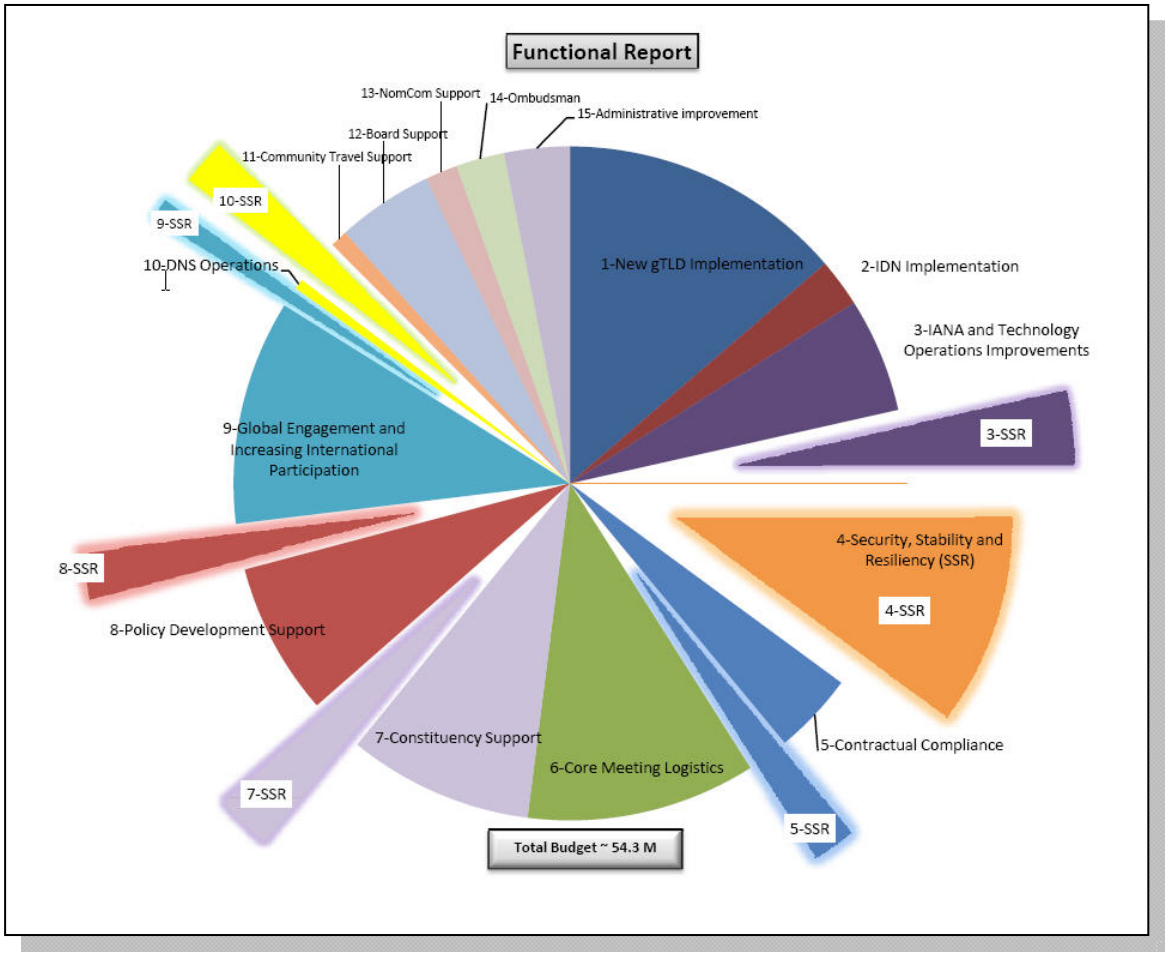
ICANN will actively pursue opportunities with other think-tanks and academic institutions on leadership in identifying challenges regarding security, stability and resiliency.

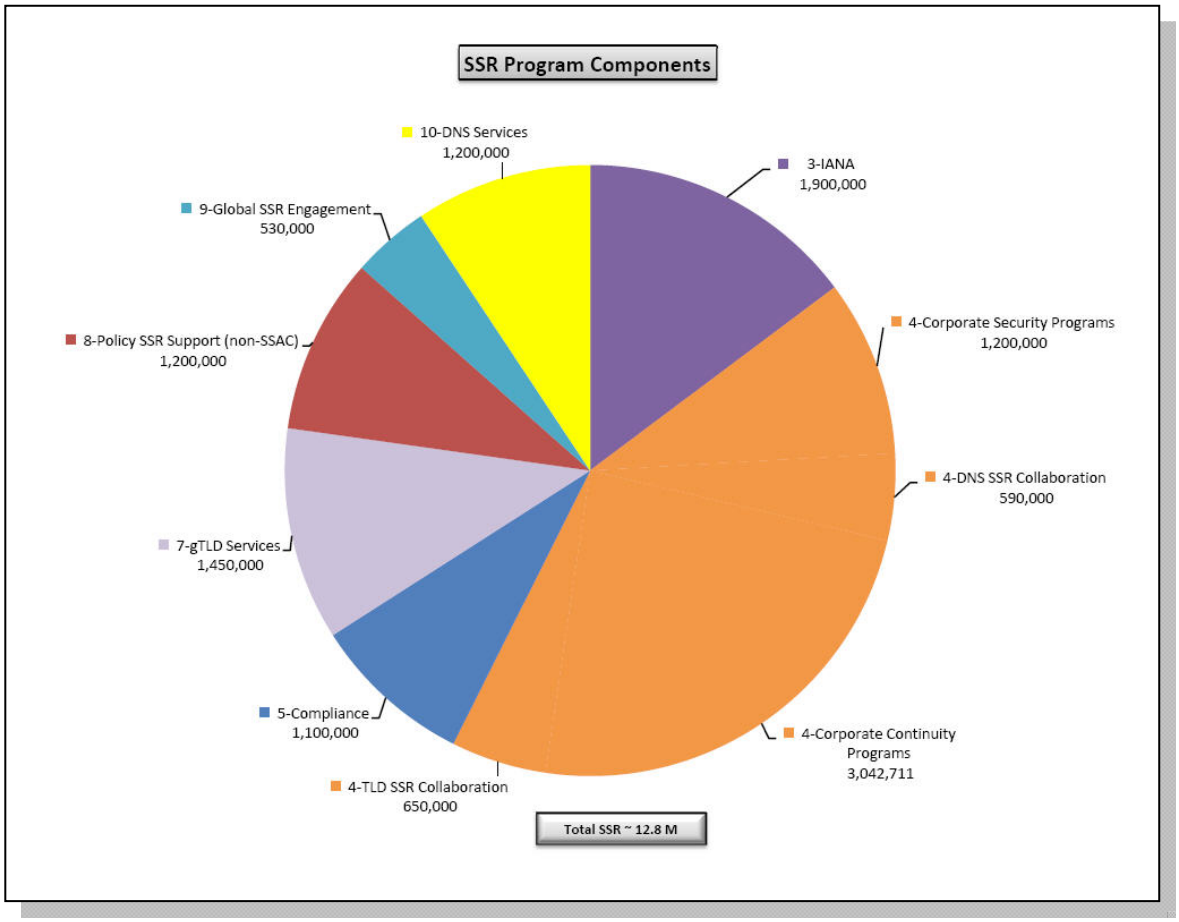
7. Conclusion

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


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 ~ 54.3 M


SSR Program Components
10-DNS Services
1,200,000
3-IANA
1,900,000
9-Global SSR Engagement
530,000
4-Corporate Security Programs
1,200,000
8-Policy SSR Support (non-SSAC)
1,200,000
4-DNS SSR Collaboration
590,000
7-gTLD Services
1,450,000
5-Compliance
1,100,000
4-Corporate Continuity
Programs
3,042,711
4-TLD SSR Collaboration
650,000
Total SSR ~ 12.8 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 - $3.0 M
- Policy SSR Support (incl SSAC) - $1.2M

OVERALL SSR – $12.8 M

IANA Security, Stability and Resiliency (IANA)

Objectives	Deliverables (milestones)
- Automation of key elements in root zone change process - DNSSec operational readiness - Test rPKI implementation - Business continuity	- Implementation of automated RZM (date depends DOC approval; plan to have ready prior to implementation of new gTLDs) - Implement DNSSec signing of .ARPA (date depends on coordination with IAB and DOC) - Coordination with rPKI testers (currently underway) - IANA Continuity & Disaster Recovery Plan (approved by August 2009)
Key Stakeholders	**Resources**
- IANA, Security, IT - DOC/USG; Verisign - SSAC; RSSAC - IETF; DNS operator community, RIR communities; NRO	- Staffing – 6.5 FTE (including 2.5 FTE for related IT and other staff support) - Financial – $1.9M to support FTEs; staff support/travel; professional services; application development

ICANN DNS Services (IT Services)

Objectives	Deliverables (milestones)
- Prepare for DNSSEC zone signing for ICANN zones, ARPA-related zones and the root - Implement Trust Anchor Repository (TAR) - Secure, resilient L-root operation	- Trust Anchor Repository in full production: June 09 - L-root improvement (new design deployed at LA and Miami, 3rd node deployed at Prague): June 09 - Production infrastructure in place for signing root zone: Oct 09 - DNSSec signed ICANN zones: Oct 09
Key Stakeholders	**Resources (FY 10)**
- ICANN IT Services Team - ICANN IANA staff, DoC, VeriSign - ICANN Security & Resiliency Team	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	Deliverables

- Ensure implementation new gTLD/IDNs addresses SSR issues
- Continue maturing data escrow process & gTLD continuity procedures
- Conduct RSEP/RSTEP processes on registry services proposals
	- Enhanced gTLD implementation process from SSR perspective
	  - SSAC/RSSAC study complete (Fall 09)
	  - Improved applicant guidebook (Aug 09)
	- Conduct data escrow test (Aug-Sep 09 or Jan 10)
	- Community failover exercise (Jan 10)
	- RSEP/RSTEP studies as required

Key Stakeholders	**Resources (FY 10)**
- Registries/Registrars - ICANN Services staff - ICANN Security & Continuity staff - GNSO/SSAC	Human – 2.75 FTE Financial – $1.45M 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 revised RAA implementation (50-100 by summer 2010)
	- Reporting improvements to WDPRS (by June 2010)
	- Conduct WHOIS related studies to further understanding of systems
	  - Proxy usage (Oct 2009)
	  - Data accuracy (Dec 2009)

Key Stakeholders	**Resources (FY 10)**
- gTLD registry/registrars - ICANN Compliance staff - ICANN Security/Continuity staff	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 Attack & Contingency Response Program - Establish joint ISOC/ICANN tech training program - Establish TLD exercise planning workshops - Establish program metrics	- Conduct ACRP training sessions (5 in 2009); automate planning tool by Aug 09) - Joint technical training with ISOC plan (approve summer 09); first full program conducted fall 2009; two more by 2009) - Conduct exercise planning workshops (initial implementation Oct 2009) - Prototype metrics based on Resiliency Engineering Framework (fall 2009)
Key Stakeholders	**Resources (FY 10)**
- ccTLD operators - ccNSO, regional TLD operators - ISOC/NSRC - ICANN staff	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 & collaboration symposium - Enhance root server SSR collaboration	- Collaboration construct and on-going responses w/ partners (construct in place summer 2009) - Info Sharing Portal (Dec 09) - Conduct & report on symposium (Feb & Mar 2010) - Co-sponsor joint root community communications exercise (Fall 2009)
Key Stakeholders	**Resources (FY 10)**
- 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 - Establish Formal Plans - Institute Security Training - Implement Traveler and Meetings Security & Contingency Plans	- Conduct Security Training Programs (embedded part of ICANN on-boarding by 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
	- Initial ICANN Business Continuity plan (Oct 09)
	  - Improved Crisis Management plan (Aug 09)
	- Establish Secure IT Data Center (Sep 09)
	- Exercise Business Continuity/Crisis Management (Spring 10)

Key Stakeholders	**Resources**
- ICANN Security & Resiliency 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 – $3.0M 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) - Engage with Forum of Incident Response and Security Teams regarding ICANN role in response (initial findings Jan 2010)
Key Stakeholders	**Resources (FY 10)**
- 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 incl. SSAC (Policy)

Objectives	Deliverables

Set by supported SO/Acs conducting SSR activity
- GNSO; ccNSO
- GAC
- SSAC
- RSSAC; ALAC
	- SSAC Reports, Advisories, Comments
	  - Domain name protection study (Jun 09)
	  - Root Scaling Study with RSSAC (Sep 09)
	- Others will depend on SO/AC FY 10 work plans

Key Stakeholders	**Resources (FY 10)**
- Named SO/Acs - ASO - ICANN policy staff - ICANN security staff	Human – 3.5 FTE Financial – $1.2M for FTEs and limited additional funding support for SSR-related activities; support for SSAC/RSSAC root scaling study

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.