Proposed Initiatives for Improved DNS Security, Stability and Resiliency

Presented by

Internet Corporation for Assigned Names and Numbers (ICANN)

For Public Comment

12 February 2010
through
29 March 2010

Proposed Initiatives for Improved DNS Security, Stability and Resiliency

1. Overview

This paper presents the rationale, key features and projected costs of two strategic initiatives related to the security, stability and resiliency of the Domain Name System (DNS) that ICANN believes are necessary to fulfill its obligations under its bylaws, the 2009 Affirmation of Commitments and the 2010–2013 ICANN Strategic Plan. This paper provides a basis for a multi-stakeholder discussion of these proposed initiatives, ICANN's responsibilities in establishing proposed capabilities and how the community might proceed in organizing efforts to support such initiatives. High-level staffing and resource implications are identified, but funding alternatives for these initiatives are not analyzed.

Note: These initiatives are proposed as efforts beyond those identified in the FY11 ICANN Operational Plan and Budget framework posted for discussion at the Nairobi meeting.

2. Assumptions

2.1 The Domain Name System has become a fundamental, underlying service powering the Internet. The DNS enables name resolution for users of the Web and also underpins e-mail, text messaging, Internet-enabled voice and other key Internet services and protocols. At the same time, the DNS exists in an environment of increasing threats and risks. The technical operations of the system are exposed to a range of attacks such as Distributed Denial of Service (DDoS) attacks against authoritative name servers and resolvers at levels up to and including the root name servers; cache poisoning attacks that impact the integrity of DNS resolution as described by security researcher Dan Kaminsky; and other methods including social engineering that allow malicious attacks to misdirect and misuse DNS services. Additionally miscreants and criminals exploit user dependence on the DNS and use the system in various ways to conduct a wide range of malicious activities.

2.2 Currently, the community of operators that provides DNS services actively collaborates with vendors, security researchers, law enforcement and response teams to react to emerging threats in a largely ad-hoc fashion. Initiatives exist within the DNS community to improve information sharing, to identify malicious activity and to enhance collaboration related to DDoS and other system-wide attacks. These collaborative efforts generally involve efforts of DNS and security community members coming together voluntarily to address emerging situations. Several calls to action on addressing and mitigating systemic DNS risks have been made in that past year.[1] The frequency and serious nature of these calls to action expose a growing need for system-wide risk assessment, contingency planning and standing response capabilities.

[1] See http://www.enisa.europa.eu/media/press-releases/improving-resilience-3-tips, and http://www.enisa.europa.eu/media/press-releases/guide-to-mitigate-vulnerabilities-threats-cyber-attacks, and http://www.it-scc.org/documents/itscc/IT-SCC_ITSRA_Release_08_21_09_clean_final2.pdf.

2.3 The current efforts to address the range of threats and risks to the DNS are not systemically focused. At an operational level, well-resourced, security savvy operators within the DNS have developed strong mechanisms for understanding threats and taking action to mitigate risks to themselves and their customers. However, collaboration in the this area does not generally extend to less capable and less well funded DNS operators and other stakeholders who are not aware of threats and risks and who lack capabilities to adequately respond when such threats to security, stability and resiliency are realized. Moreover, existing efforts have demonstrated that sustained focus on monitoring, responding, and remediation is needed to contend with threats that are not amenable to easily localized technical fixes. At a higher level, the DNS lacks system-wide focal points for accountability related to key capabilities in risk assessment, contingency planning and exercises, and dedicated, sustained response. Such activities must look holistically at the DNS and respond to the needs of the individual components and operators.

2.4 Fundamentally, these types of capabilities cannot rely wholly on the efforts of volunteers acting without dedicated organizational support, refined operational approaches and long-term resource commitments. Efforts to ensure the stability and resiliency of the DNS must attain levels of effectiveness and accountability in line with other critical aspects of communications infrastructure requiring similar levels of investment in full-time staff and support.

3. ICANN Role and Responsibilities

3.1 The DNS must operate in a secure, stable, resilient fashion. ICANN has numerous commitments that require it to undertake efforts to achieve this objective. Article I of the ICANN bylaws states, "The mission of ICANN is to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems." The 2009 Affirmation of Commitments (http://icann.org/en/announcements/announcement-30sep09-en.htm) asserts that the DNS serves as a critical function within the Internet environment and therefore risks related to operation must be appropriately managed. ICANN has committed to "preserve the security, stability and resiliency of the DNS." The Affirmation additionally calls for ICANN to identify current and future threats and to conduct appropriate contingency planning.

3.2 The implication of these commitments for ICANN is clear. The Affirmation of Commitments requires that ICANN undertake collaborative efforts to identify and mitigate risks to security and resiliency throughout a distributed DNS system, which includes a broad range of stakeholders who operate and use DNS services.[2] Due to the nature of the DNS, reliable, resilient operations of the root server system and the top-level domains must be a first-tier ICANN priority. The growth of the DNS through the

[2] As ICANN plans to address its role in managing the risks to the security, stability and resiliency of the DNS, it does not address issues related to national security competition between states in the realm of cyber war or espionage or address control of content hosted on the Internet as addressed in the ICANN Plan for Enhancing Internet Security, Stability and Resiliency. See http://www.icann.org/en/topics/ssr/ssr-draft-plan-16may09-en.pdf.

natural increase in use, and the introduction of new technologies and proposals to establish new TLDs (including those using Internationalized Domain Names) further require that ICANN understand and seek to reduce the risks to the system. It is important to note that ICANN has sought to improve the security, stability and resiliency of the DNS since its inception. The ICANN *Plan for Enhancing Internet Security, Stability and Resiliency* (http://www.icann.org/en/announcements/announcement-2-21may09-en.htm) addresses the broad range of existing programs and activities. The initiatives outlined in this paper address further efforts ICANN must undertake to meet these commitments.

3.3 The imperatives to improve systemic understanding and mitigation of DNS risk and to address its commitments will require that ICANN collaborate with the DNS community to initiate further work that builds on both past efforts and current collaboration. To that end, the 2010–2013 ICANN Strategic Plan makes improving the stability, security and resiliency of the DNS one of ICANN's four areas of focus during this period. The Strategic Plan specifically addresses the requirement for ICANN to establish an approach for a Domain Name System-Computer Emergency Response Team (DNS-CERT) as well as for contingency planning and exercising for the DNS. ICANN seeks to move forward to ensure establishment of system-wide approaches to assess risk, to plan and exercise contingencies against potential threats and to orchestrate collaborative incident response capabilities to improve the overall security, stability and resiliency of the DNS system. ICANN also plans to initiate efforts to improve system-wide metrics so that the DNS community can obtain a clearer understanding of the security, stability and resiliency of the DNS, anticipate challenges and respond effectively.

3.4 The prospective utility and operational success of the initiatives outlined below will require community support and engagement. Community review, feedback and planning related to implementing these initiatives will be integrated into ICANN's operational planning and budgeting processes.

4. Risks to the Operation of the DNS

4.1 As we begin 2010, the Internet ecosystem remains vibrant. 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. The ecosystem is also threatened by growing levels of malicious activity conducted by a variety of actors, with strong indications that involvement by criminal organizations is growing rapidly. The threat landscape includes fraud, extortion, and other illicit online activity, which undermine user confidence in Internet-based services, and Denial-of-Service (DoS) attacks and other disruptive activities that destabilize the Internet's infrastructure. In particular, the ability of malicious actors to conduct attacks against the functioning of the DNS itself and the ease and frequency by which these actors use both name resolution and registration services to enable a range of malicious or criminal activities presents growing risks to the proper functioning of the

Internet and calls into question the integrity and reliability of the Internet as a global communications platform.

4.2 Three major categories of security, stability and resiliency risks exist: malicious activities (attacks against the DNS or attacks that exploit the name resolution or registration systems), technical risks to the stability of the DNS, and organizational risks related to the DNS.

4.2.1 Malicious Activity Risks

4.2.1.1 At the core, the primary risk of concern to ICANN is the availability of the DNS to resolve names and facilitate a wide variety of transactions across the Internet. A major threat to availability can come in the form of DoS attacks against those operating DNS services at various levels of the systems. The impact of DoS attacks depends on both the types of services targeted as well as the sophistication and traffic volume of the attack. Over the past decade, the operations of root servers as well as top-level domains (TLDs) have been directly attacked. Four instances stand out: (1) on October 21st 2002the first documented case of a coordinated attack against the thirteen DNS root servers took place (http://d.root-servers.org/october21.txt); (2) in February of 2006 attacks took place against name servers operated by a key TLD name service provider (http://www.icann.org/en/committees/security/dns-ddos-advisory-31mar06.pdf); (3) in February of 2007 an attack took place against six of the thirteen DNS root servers (http://www.icann.org/en/announcements/factsheet-dns-attack-08mar07.pdf); and (4) more recently, in December 2009, DoS attacks against DNS providers were in the news again when an attack against NeuStar's UltraDNS service affected many e-commerce sites (http://www.cnn.com/2009/TECH/12/24/cnet.ddos.attack/index.html). This history of attacks demonstrates the ongoing increase in resources available to those conducting attacks as well as the sophistication of the perpetrators.

4.2.1.2 Significant efforts to mitigate these risks are ongoing in terms of providing provisioning bandwidth to deal with DDoS and the establishment and deployment of technologies and methodologies, such as anycasting, whereby data is routed to the best or nearest destination. As an example of deployment of anycast solutions the DNS root server system has grown from a presence in thirteen locations (systems) to a presence in over two hundred locations (see detail at http://www.root-servers-org). There are also growing levels of planning and collaboration among DNS operators, with the establishment of organizations like the DNS Operation Analysis and Research Center(DNS-OARC) (http://www.dns-oarc.org), the Registry Internet Safety Group (RISG) (http://registrysafety.org/website/) and efforts to understand the risks associated with the DNS such as the Global DNS Security, Stability and Resiliency Symposium (http://www.gtisc.gatech.edu/pdf/DNS_SSR_Symposium_Summary_Report.pdf). However, the threats are also increasing as ever-larger botnets under the control of criminal and other malicious actors pose the risk of very significant attacks in terms of both sophistication and scale. Planning for such disruptions must also address the possibility that DNS services are disrupted as a result of malicious attacks against systems that the DNS relies upon ranging from electric power to Internet routing.

4.2.1.3 The open and distributed nature of the operation of the DNS, coupled with the broadly distributed administration of name servers and resolvers, exposes users to a number of additional risks. The DNS protocol (without use of security extensions) is vulnerable to attacks that employ *misdirection* of queries. Specifically, the attack returns false information in response to a DNS query (*poisoning* or *pharming*) or information that is different from what a domain name authority intended (redirection, or response modification). Such attacks deceive DNS users in a wide variety of ways: directing users to web sites with fraudulent content or malicious code, making e-mails appear to come from spoofed sources, and so on. Techniques for executing attacks that would allow systematic poisoning of DNS caches and hence misdirection of Internet traffic present the opportunity for malicious activity that may pose risks to the integrity of the DNS as a whole.

4.2.1.4 Domain name registration services provide another attack vector for miscreants. Attackers will exploit technical (web site vulnerabilities) or operational weaknesses of a registrar or domain name registrant (staff who can be socially engineered) to gain unauthorized control of a domain name registration account (for detail, see SAC040 http://www.icann.org/en/committees/security/sac040.pdf). Once in control of the hijacked registration account, the attacker alters the DNS configuration of, potentially, all the domains in a hijacked account to point to a name server controlled by the attacker, giving the attacker control over name resolution for the compromised domain's web, email, and other Internet applications. Such domain name or account hijacking attacks are used to deface web sites, disrupt email or other services offered by the registrant, or to capture sensitive or personal information.

4.2.1.5 While the DNS is intended to serve Internet users, it is regrettably also exploited by miscreants to facilitate a wide range of criminal conduct and abuse. This unintended consequence is best exemplified by the manner in which the DNS is exploited to facilitate a malicious activity commonly referred to as *phishing*. Phishers register domain names specifically to support attacks launched from networks of compromised or *botted* computers, called *botnets*. The attacker often uses some of these malicious domain names to operate a *crime DNS*, a collection of DNS resolvers that are specifically programmed and deployed to resolve DNS queries issued by phishing victims. Other malicious domain names are used to host impersonation web sites. Responses to a victim's DNS query for a seemingly legitimate domain name of a financial institution, e-business, charity, government agency, or similar entity instead direct these unwitting users to a deception or impersonation web site. The victim innocently interacts with this deception site as he would normally do with the legitimate sites of financial institutions, e-business, charities, or government agencies. These malicious sites, however, are designed to steal identities, bank account and credit card information, sell illegal or bogus products to the victim, defraud a charity, and more. [3]

[3] US Dept. of Homeland Security, Information Technology Government Coordinating Council. 2009. Information Technology Sector Baseline Risk Assessment. Washington, DC: Government Printing Office, pp 32–33.

4.2.1.6 Increasingly, the DNS is also playing a prominent role in enabling *botnets for hire*, attack networks that are offered for service in a thriving underground economy. Botnets composed of hundreds of thousands or even millions of compromised computers (bots) are remotely controlled to perform many types of malicious attacks (for example, DDoS) or support criminal activities (human trafficking, distribution of illegal pharmaceuticals, spam, and the like). To control the bots efficiently and with considerable resiliency against countermeasures by security practitioners and law enforcement agents, the attackers program the bots to use the DNS to identify the address of the command-and-control or *rendezvous points* that issue commands to the bots. Recently, certain malware such as variants of the Conficker malware have used approaches that seek to rely on sets of predetermined domain names as a key aspect of controlling the bots.

4.2.2 Technical Risks

4.2.2.1 The operation or integrity of the DNS can be adversely affected should widespread use of questionable operational practices result in a disruption of service, or should a technical change result in an unanticipated vulnerability that miscreants or criminals exploit to facilitate malicious activities. Instances of the latter kind of problem and the largely reactive manner in which such problems are currently addressed occurred in 2008. Security expert Daniel Kaminsky discovered a serious vulnerability in the DNS protocol, and subsequently publicly demonstrated that a practice called DNS response modification could be exploited by attackers to hijack web sites of major corporations using web hosting services entirely out of the administrative reach of those organizations. ICANN's Security and Stability Advisory Committee (SSAC) later published an advisory warning of the potential threat DNS response modification posed to the community (http://www.icann.org/en/committees/security/ sac032.pdf). Ad hoc systems were put in place so that DNS operators and users could test their systems for the vulnerability and take preventive or remedial measures. The ICANN community has begun and continues several initiatives that may contribute to a more coordinated disclosure of and more organized response to DNS-related threats of these sorts. This includes ICANN working with partners to conduct annual symposia to bring experts together to study the threat landscape, collectively assess risk and make recommendations regarding how to address the risk. The first symposium was conducted in February 2009 in conjunction with Georgia Tech Information Security Center (GTISC).

4.2.2.2 The operation of the DNS can also be adversely affected should technical changes to the DNS alter the system's behavior or result in traffic loads that require substantial changes in current or planned capacity. To reduce the potential for the adoption of operational practices that can disrupt the security and stability of the DNS at the TLD level, in 2009 the ICANN Board implemented steps to prohibit the use of redirection based on the risks this practice poses to the stability of the DNS as identified by the Security and Stability Advisory Committee (SAC041 http://www.icann.org/en/committees/security/sac041.pdf). In 2010, the DNS community will continue a comprehensive review of the potential impacts that might result from a series of proposed changes to the root level of the DNS: the

implementation of DNS Security Extensions (DNSSEC), the implementation of IPv6 and the need for IPv6 glue records to be added to the root zone file, fast track introduction to enable the use of Internationalized Domain Name (IDN) labels at the DNS top level, and the introduction of new TLDs.

4.2.3 Organizational Failures

4.2.3.1 The potential failure of organizations that perform key roles in DNS operation to function effectively also constitutes a significant risk category. At the core of the DNS, the ability of ICANN, root server operators, TLD registries and registrars to provide services without interruption is essential to overall DNS security and stability. Each of these entities is individually responsible for its own financial viability, business continuity and risk management, but at the system level provision must be made for contingencies when an organization can no longer perform its function, as appropriate, and how services will be restored, perpetuated or reconstituted to ensure continued effective DNS operations and to protect registrants.

4.2.4. Measuring Risk and Security, Stability and Resiliency

4.2.4.1 Currently, there is little consensus on the right measures and acceptable performance levels for the system as a whole related to risk and security, stability and resiliency. Individual operators and independent researchers have measured various aspects of the DNS, but to date little progress has been made in defining and implementing standard, system-wide metrics or acceptable service levels. Efforts to improve risk management related to DNS security, stability and resiliency must be guided by an improved ability to measure these characteristics and assess the utility of programs and resource investments.

4.2.4.2 A key enabler of improving this situation will be to ensure that composite parts of DNS operations are correctly instrumented and measured. The 2009 Root Server Study Team (RSST) report on scaling the root (http://www.icann.org/en/committees/dns-root/root-scaling-study-report-31aug09-en.pdf) calls for the “establishment of effective mechanisms for detecting and mitigating risks as they become visible” related to the root server system. The establishment of metrics and instrumentation does pose some interesting challenges. Specifically the distributed nature of the DNS calls for a cooperative measurement model, requiring participation by multiple players and organizations. The topic of Internet Early Warning Systems is being studied in various for a, including the European Network and Information Security Agency (ENISA), which is holding its first workshop on Internet Early Warning and Network Intelligence in March of 2010 (http://www.enisa.europa.eu/events/ee/ EWNI2010). ICANN, in conjunction with Kyoto University, held the second global symposium on DNS Security, Stability and Resiliency in February of 2010, with a specific focus on measurement. ICANN plans to encourage and to participate in activities that will improve the state of understanding how to measure DNS risks and the health, security, stability and resiliency of the system as a fundamental enabler in establishing effective risk assessment, contingency planning/exercises and response capabilities.

5. Strategic Initiatives

5.1 The two initiatives presented here address critical needs in establishing the capabilities necessary for ICANN to meet the security, stability and resiliency commitments identified earlier. As addressed at the start, this paper is intended to provide a basis for multi-stakeholder discussion of these proposed initiatives, ICANN responsibilities in establishing proposed capabilities, and how the community might proceed in organizing efforts to support such initiatives. High-level staffing and resource implications are identified but funding alternatives for these initiatives are not analyzed. This paper does not presuppose that ICANN will fund or staff these initiatives.

5.2 Initiative 2 regarding the need to establish a DNS-CERT is presented in more detail in the DNS-CERT business case which accompanies this paper.

5.1 Initiative 1 – System-wide DNS Risk Analysis, Contingency Planning and Exercises

5.1.1 ICANN will collaborate with the DNS community to proactively understand the key risks to the DNS, including analyzing emerging threats and risks as called for in the Affirmation of Commitments. Once these risks are analyzed, the DNS community must identify contingences of greatest concern to system-wide DNS security, stability and resiliency and ensure that planning efforts are in place to mitigate identified risks. ICANN believes it has an important role in enabling system-wide contingency planning and exercises as part of its responsibilities under the Affirmation of Commitments. Such a proactive program will complement the response capabilities that could be provided by a DNS-CERT in addition to leveraging the organization as a natural hub for supporting contingency and exercise planning.

5.1.2 The first aspect of this initiative would be to constitute a community-based approach to risk analysis that includes an accepted DNS risk framework and refining approaches to measuring risk. This effort will include establishing an approach to conducting regular DNS risk assessments and mitigation proposals. This effort would build on the work of the 2010 DNS Security, Stability and Resiliency Symposium as well as efforts by DNS-OARC, ENISA and others.

5.1.3 Another aspect of this initiative is to enhance community-wide collaboration in contingency planning and use that as a basis for directing the efforts to establish response capabilities. The basis for contingency planning should commence from consensus around a system-wide DNS risk framework that identifies the top risks to the DNS and key scenarios. This effort would build on existing efforts such as those conducted through public-private partnerships concerned with critical infrastructure protection such as the US Information Technology Sector Coordinating Council and ENISA, as well as those conducted as part of the DNS operational community such as by DNS-OARC and NL Net Labs. This proposed initiative also envisages close coordination with an emerging root server system information sharing mechanism and with the TLD registry operators. Analysis of risks and key contingencies would be used to assess the adequacy of current response mechanisms, to identify deficits requiring action, and to to produce contingency plans for identified contingencies. The effort should be supported by a standing, community-wide expert advisory/working group. ICANN would

assume responsibility for supporting the group and developing an action plan for community review that would constitute input to ICANN's annual cycle for its security, stability and resiliency and operational planning budgeting.

5.1.4 Once contingency planning is established, a system-wide DNS exercise program is necessary to ensure response capabilities are evaluated and deficits identified.[4] As with the DNS-CERT and contingency planning efforts, development of an exercise program should build on existing activities and incorporate efforts such as the existing TLD contingency exercise efforts as sub-elements of a larger program. The goal should be to initiate a program of activities that culminates in a biannual system-wide DNS exercise focused on response to key contingencies. Additionally, the program should include integration with other exercise programs such as the multi-national cyber storm exercise series and other international multi-stakeholder exercises. As identified in the Affirmation of Commitments, ICANN has a responsibility to support a community-wide approach to such a program, facilitating subelements of a program as appropriate and orchestrating the biannual system-wide DNS exercise.

5.1.1 Specific Proposed Steps

5.1.1.1 Establish a DNS Risk Assessment and Contingency Planning expert advisory group. This group would be composed of experts from the DNS operations and cyber security communities. ICANN would support the group with staff. Initial focus of the group would be establishing a community-accepted framework for systemic DNS risks and identification of key existing risks by 3rd quarter 2010. Additionally, the group would build on work from the 2010 DNS SSR Symposium on metrics to establish a community-accepted framework for measuring the health, security, stability and resiliency of the DNS by early2011. The group would also be responsible for establishing baseline contingency planning scenarios by 2nd quarter 2011. The group would conduct an annual DNS risk and mitigation report with the first report to be delivered in 3rd quarter 2011.

5.1.1.2 Establish a DNS Root system information sharing mechanism which would be a collaborative effort in conjunction with the root server operator community and others involved in the root server community based on recommendations of the 2009 Root Scaling Study. A working group supported by ICANN staff will be formed to identify functional and performance monitoring requirements. Key capabilities would include maturing DNS root system modeling, improved information sharing among organizations involved in the root system, potential deployment of necessary sensors, and dedicated analytic support to assess current health of the DNS root system and provide warning of emerging problems. Efforts will take place to work with the community to implement and deploy sensors and measure those metrics that will allow an overview of the root server and TLD system and how it behaves. This effort will require collaboration with the operators of the TLDs, the root server operators, NTIA, ICANN and others involved in the operation and management of the core DNS infrastructure. We envision that this system will be established in a mutually supportive fashion along with development of the DNS-CERT.

[4] The requirement for such a program for the DNS is specifically identified in the DHS IT Sector Risk Assessment.

5.1.1.3 Continued support of root server operators' contingency planning and exercises. Following successful communications exercises and an initial table top exercise by the second half of 2010, ICANN will plan work with the operators to institute a programmatic approach to contingency planning and scenario-based exercises. ICANN will deploy communications capabilities that will complement and enhance existing systems used in its own root server operations.

5.1.1.4 Continued maturation of the TLD continuity planning and exercises. ICANN and TLD registry operators to conduct data escrow testing throughout 2010 and into 2011 based on the development of the data escrow specification for the new generic top-level domain (gTLD) process. Additional exercises are planned with focus on communications and crisis response elements between ICANN and TLD registry operators.

5.1.1.5 Initiate development of a DNS-wide exercise and evaluation program. Such a program would include leveraging existing efforts and require involvement by a wide range of stakeholders including those involved in DNS operations, DNS vendor and user communities and the broader cyber security community. This program would also involve understanding and leveraging the intersection with other cyber security and associated exercise and evaluation programs. By the end of 2010, this effort would assess the nature and adequacy of existing efforts and identify key gaps. By mid-2011, a proposed DNS exercise program concept paper would be developed for community review. Additionally, ICANN will sponsor a limited system-wide exercise in the second half of 2011 as a prototype with voluntary participation from across the range of stakeholder's intent on establishing long-term planning and execution processes. Planning for this prototype exercise would begin in 2010. ICANN staff and other members of the DNS community will be participating in the multilateral Cyber Storm III exercise and may also participate in other international exercises.

5.1.2 Resource Projection

5.1.2.1 Project the need for five full-time staff positions:

- Senior Coordinator, Risk Assessment, Contingency Planning and Exercise Program
- Contingency Planning Coordinator
- Exercise and Evaluation Program Coordinator
- Exercise Planner
- Systems Analyst/Modeling Expert, Root System Information Sharing System

5.1.2.2 Support requirements would include requirements definition for root server system information sharing; support to risk analysis and root server information sharing efforts; infrastructure and associated costs to include licensing and software/hardware support for modeling, a root server system information sharing and communications systems and prototype deployment of sensor system; travel and meetings costs for working groups and staff; and physical facilities and IT support for additional staff.

5.1.2.3 We anticipate costs to support this effort from July 2010–June 2011 at approximately $1.25 million USD for staff and $850,000 USD for support. Total projected first year annual cost for this initiative would be $2.1 million USD.

5.1.2.4 **Assumptions:** Risk analysis would leverage threat information and analysis from DNS-CERT. Root server information sharing system would leverage Web 2.0 portal developed for DNS CERT to support information sharing.

5.2 Initiative 2 – DNS-CERT

5.2.1 In addition to proactive risk assessment, contingency planning and exercising, the DNS community needs effective, operational, system-wide response capabilities to adequately address security, stability and resiliency challenges. A wide-scale coordinated attack against the DNS could result in significant economic and political fallout, yet no central point of incident management contact for technical and policy coordination related to identifying and coordinating response to such an incident exists for the DNS. In 2009, the Global DNS Security Stability and Resiliency Symposium made specific note of the security response gap in the DNS and recommended action to address this shortfall. Additionally, many DNS operators are not adequately resourced and as a result have limitations in developing robust security and resiliency efforts. Such organizations may not know where to seek assistance or have language or geographic barriers impeding assistance. Such organizations are likely to be vulnerable or exploitable points within the DNS as a whole. ICANN believes that a central point of contact, a DNS-CERT, is needed to provide technical and policy coordination for the DNS and to work with the DNS community to identify and coordinate responses to global DNS incidents.

5.2.2 A DNS-CERT would coordinate existing efforts with the DNS community to maintain situational awareness so the overall community can reach out to the right expertise at any time. Key stakeholders of such an effort would be DNS operators and users, vendors, security researchers, and incident responders. A DNS-CERT would leverage a number of existing efforts that seek to identify threats, share information and facilitate response across the DNS. DNS-CERT activities could assist in collaborating and helping coordinate these efforts and providing services in areas currently not covered or with stakeholders that are not engaged in these efforts. A DNS-CERT could be launched with ICANN support, but the specific organizational structure and resourcing model will be determined through dialogue with the community. In this respect, oversight of DNS-CERT would be performed by a sponsor-based Board that would ensure accountability to the CERT's constituency, as well as evaluate the activities of DNS-CERT based on the needs of the stakeholders served by the organization. The operations of the DNS CERT would be overseen by a core team of administrative and technical staff and would be assisted by an extended team consisting of virtual expertise augmenters who would provide tangible support to DNS-CERT while operating in a geographically dispersed fashion.

5.2.3 A DNS-CERT would provide both proactive (that is, threat analysis, DNS health and security monitoring, situation awareness and information sharing), and reactive services

(that is, a 365 x 24 x 7 point of contact, incident handling coordination, vulnerability management support and security advisory services) to its constituency. This approach is important for two reasons: (1) proactive threat landscape information can help the DNS community plan for threats through training and exercises; and (2) reactive incident handling services can aid constituents with significant resource constraints, such as registrars in lesser-developed regions of the globe. Threat information and analysis would also feed projected establishment of systemic DNS risk identification and analysis capabilities described in Initiative 1. Definition of functional requirements for core capabilities that a DNS-CERT will provide will occur through community-based analysis involving the stakeholders and potential collaborators for a DNS-CERT.

5.2.2 Resource Projection

5.2.2.1 Based on the evaluation of national CERT teams of a similar size and level of responsibility, we believe that the DNS-CERT can function initially with an annual budget of a staff of approximately 15 people that includes a director, two senior managers, a ten-person incident management team, and staff administration/legal support. Projected staff cost is $2.6 million USD. Support costs for staff travel, communications and analysis tools, physical facilities and IT support is estimated at $1.6 million USD. Total estimated first-year cost for this initiative is $4.2 million USD. More detail is provided in the DNS-CERT Business Case that accompanies this paper.

6. Conclusion

The security, stability and resiliency challenges facing the DNS are rising. ICANN has significant responsibilities under its bylaws and the Affirmation of Commitments to work with the DNS community to address those challenges. Specifically, the establishment of system-wide DNS contingency planning, exercise and collaborative response capabilities are required. This concept paper provides a basis for a multi-stakeholder discussion of these proposed initiatives to address these requirements.