
# Global DNS-CERT Business Case: Improving the Security, Stability and Resiliency of the DNS

**Presented by**

**Internet Corporation for Assigned Names and Numbers (ICANN)**

**For Public Comment**

**12 February 2010**
**through**
**29 March 2010**

# 1. Executive Summary

The Internet's operation relies heavily on the Domain Name System (DNS), which now serves as a critical element for a much broader range of namespace mapping services. A widespread or persistent failure of the DNS could render the Internet unusable by most individuals. Although DNS failures can be sometimes be attributed to natural phenomena, they are most often associated with intentional attacks.

The creation of a Domain Name System–Computer Emergency Response Team (DNS-CERT) devoted to both proactive and reactive measures related to DNS security, stability and resiliency would lessen the impact of future attacks against or failures of the system. Several external bodies have also called for the establishment of such a capability.

We are aware of a wide range of existing organizations and activities that currently support improving security awareness, response and resiliency across the DNS. A major driver for establishing the DNS-CERT is to ensure availability of dedicated staff to orchestrate the existing community efforts and address services and stakeholder needs currently not addressed. To be effective, the effort must explicitly avoid duplication of existing efforts and information sharing mechanisms.

## 1.1 Mission

1.1.1 The proposed mission of the DNS-CERT is to:

*Ensure DNS operators and supporting organizations have a security coordination center with sufficient expertise and resources to enable timely and efficient response to threats to the security, stability and resiliency of the DNS.*

1.1.2 The mission statement calls out three key factors: expertise, resources and timeliness. The DNS-CERT must maintain situational awareness so it can reach out to the right expertise and stakeholders at any time.

## 1.2 Operational Concept

1.2.1 Working within the mission parameters, the goals of the DNS-CERT will be to:

- Gain situational awareness and share information
- Improve coordination within the DNS operational community
- Improve coordination with the broader security community

1.2.2 In addition to its operational goals, a CERT must serve and be responsive to its constituency, provide a public interface related to DNS security, and disseminate appropriate information to its stakeholders. A focus area will be fusing available data. The DNS-CERT will be evaluated by its stakeholders on an ongoing basis, and this is the key criterion by which its success will be measured. The definition of functional requirements for providing DNS-CERT core capabilities will occur through community-based analysis involving the stakeholders and potential collaborators for a DNS-CERT and will be documented in a Concept of Operations.

1.2.3 An additional facet of the DNS-CERT's operation is that it plans to integrate key individuals from the DNS community into an extended virtual response team. While facilitating access to key human resources in the DNS community, such an approach

provides a well of deep expertise and greater time zone reach to the team while controlling costs related to dedicated staff.

## 1.3 Services Analysis

1.3.1 Because of its unique position, the DNS-CERT will be able to provide both proactive and reactive services to its constituency. This is particularly important for two reasons:

- Proactive threat landscape information can help the DNS community plan for threats through training and exercises.
- Reactive incident handling services can aid constituents with significant resource constraints, such as registrars in lesser-developed regions of the globe.

## 1.4 Governance and Funding Models

1.4.1 The DNS-CERT may be launched with ICANN support, but its structure should allow it to operate as a free-standing organization based on a community dialogue regarding the best approach. In this respect, oversight of the DNS-CERT will be performed by a sponsor-based Board of Governors that can ensure accountability to the CERT's constituency and evaluate the activities of DNS-CERT based on the needs of the stakeholders served by the team.

1.4.2 Based on an evaluation of national CERT teams of a similar size and level of responsibility, we believe that the DNS-CERT can function adequately with an annual budget of $4.2 million USD, which would provide for sufficient staff, facilities and support.

# 2. Background

As we consider the evolution of the Internet, we can reflect upon how a communications research project has grown to become one of the most powerful and widely available means of communication, reaching to every corner of the globe. Relied upon not only by individuals, the Internet provides services necessary to the functioning of governments, corporations and financial institutions, not to mention schools, medical facilities and merchants small and large.

Extensive use of the Internet by such a wide variety of parties has naturally caused the volume of sensitive or valuable data carried on the Internet—such as financial transactions, medical data and other proprietary data—to grow rapidly. Consequently, cybercrime is becoming more organized and established as a transnational business, seeking technical means to subvert the Internet for illicit purposes. In addition, individuals and groups seeking to advance political or other causes continue to invest in the development of tools and techniques to attack systems and information, pursuing objectives ranging from economic gain to sustained disruption of communications.[1]

In addition to malicious acts, software and other technical failures often cause, or are contributing factors toward, failures and system outages. Although the design of the Internet reduces single points of failure to a large extent, operational failures or the widespread use of software that contains common vulnerabilities can cause network failures and disruptions having broad impact.

## 2.1 Domain Name System

2.1.1 Underpinning the Internet's operation is the Domain Name System (DNS), which was conceived and deployed in the early 1980s as a means for translating natural language names into computer network addresses, but which now serves as a critical element for a much broader range of namespace services. Because users and software routinely assume the presence of a functioning DNS, its widespread or persistent failure could render large portions of the Internet unusable by most individual users.

2.1.2 By design, the nature of the DNS is that it is both hierarchical and distributed, meaning that there is no central nexus of control for the namespace mappings. In effect, once a higher level of the DNS hierarchy delegates authority for a subordinate namespace, or *zone,* then the DNS operator to whom the delegation is made is capable of complete management of the delegated namespace.

2.1.3 While this delegation is practical and, in fact, an essential element of the DNS, it also leads quite naturally to questions of how to best identify and respond to failures. Moreover, it raises the question of how to best ascertain the status of health of the DNS on a global basis because there is no single coordination point among the diverse universe of operators who affect the provision of DNS service.

[1] U.S. Congressional Research Service; Foreign Affairs, Defense and Trade Division. 2008. *Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.* Washington, DC: Government Printing Office.

## 2.2 Computer Emergency Response Teams

2.2.1 Exploitation of security problems on the Internet is not a new phenomenon. In 1988, the *Morris Worm* incident occurred[2] and caused a large percentage of computers on the network at that time to be compromised and temporarily placed out of service. This incident resulted in a call for the development of a single point of contact to be established for Internet security problems, resulting in the formation of the CERT Coordination Center (CERT/CC) at Carnegie Mellon University.

2.2.2 Incident response teams, commonly called "Computer Emergency Response Teams" or CERTs, serve as clearinghouses for security information and as incident handlers for their respective constituencies.

2.2.3 In the years since the CERT/CC was established, the creation of incident response teams has become the norm, with these teams representing their respective universities, corporations, software vendors, nations or geographic regions.[3] Although the principal role of a CERT is to coordinate response, it also serves as a clearinghouse for information related to threats against IT systems.

## 2.3 Situational Analysis

2.3.1 The organization and motivation of individuals and groups who intend to attack or cause harm to the Internet has changed significantly in the past two decades,[4] with the emphasis shifting strongly away from curiosity seeking toward a desire to achieve specific aims. A recent analysis of threats against the DNS[5] identified four principal objectives for man-made deliberate threats against the DNS function:

- Politically-motivated attempts to influence or disrupt DNS operations
- Desire for financial gain
- Demonstration of technical superiority; and
- Gratuitous defacement or damage

2.3.2 A variety of practical attack scenarios have been developed that support these objectives, including the potential for Internet namespace fragmentation, DNS service disruption, corruption of DNS databases, misdirection of DNS service, and attacks against specific enterprises or economic sectors.

## 2.4 Potential Impact

2.4.1 Although the potential of a wide-scale coordinated attack against the DNS could result in significant economic and political fallout, there is no central point of technical and policy coordination for identifying and responding to such an incident.

---

[2] For a detailed description, see http://en.wikipedia.org/wiki/Morris_worm.
[3] Pethia, Richard D. and Kenneth van Wyk. 1992. "Computer Emergency Response: An International Problem." Pittsburgh, PA: Carnegie Mellon University, 1992.
[4] Meyer, Gordon R. 1989. "The Social Organization of the Computer Underworld." Thesis. Northern Illinois University, Department of Sociology, p 17.
[5] U.S. Dept. of Homeland Security, Information Technology Government Coordinating Council. 2009. *Information Technology Sector Baseline Risk Assessment.* Washington, DC: Government Printing Office.

In April 2009, the Global DNS Security, Stability and Resiliency Symposium specifically noted the security response gap in the DNS and recommended action:[6]

*Information sharing within the DNS community is sorely lacking and, related to that, incident response procedures, capabilities, and [the] capability to detect, respond [to] and defeat malicious activity are limited at all levels, from root operators, to registries, to service providers, to end users.*

*[...]Currently, it is professional networks that facilitate information sharing. A trusted, common ground, where operators, researchers, law enforcement, policy makers, and other stakeholders can connect with each other is desired.*

*[...]CERTs worldwide perform similar [incident handling] functions, but there is no community of practice devoted to the DNS as of yet.*

2.4.2 A failure to rapidly detect attacks against the DNS could result in significant and lasting economic consequences. According to a 2009 Information Technology Sector Risk Assessment,7 incident response forms a key line of defense for the DNS against situations that could cause this kind of impact:

*A lack of **common situational awareness** among incident responders could leave critical assets, systems, networks and functions vulnerable.*

*The inability to determine [...] the cause of an attack. [This problem can be exacerbated by] a possible gap in **24-hour incident management** capability; a lack of availability of incident handlers and technical responders.*

2.4.3 Consequently, the assessment explicitly cites the critical role of DNS and recommends that incident response capabilities, as well as training and awareness programs, be instituted in a way that addresses "cross-sector cyber infrastructure issues."

## 2.5 Geographic and Resource Constraints

2.5.1 The operational characteristics of an incident response capability should take into account the **policy desires** of the global Internet community as well as the **resource constraints** that exist in lesser-developed regions of the world.

2.5.2 Many DNS operators are not adequately resourced and, as a result, are limited in developing robust security and resiliency efforts. Such organizations may not know where to seek assistance or encounter language or geographic barriers that impede assistance. Such organizations may become weak points within the DNS as a whole.

2.5.3 Taking note of this resource disparity, the 2009 Global DNS Security, Stability and Resiliency Symposium pointed out that:

*...resource constrained organizations have difficulty establishing networks of professionals to reach out and solicit information from. An organization will instinctively turn to its professional network, either in reaction to an*

[6] Proceedings of Global DNS Security, Stability and Resiliency Symposium, April 2009.
[7] U.S. Dept. of Homeland Security, op. cit.

*event/incident or for proactive assistance. It is imperative that organizations know where to begin establishing their networks.*[8]

2.5.4 A DNS-CERT would leverage many existing efforts that seek to identify threats, share information and facilitate response. A list of specific organizations and efforts that would be potential collaborators in this area can be found at the end of this section.

2.5.5 An effective CERT capability for the DNS should not be limited geography because of the dispersed nature of operations. In this sense, what might ordinarily be considered to be *critical national infrastructure* may have impacts far beyond a national border.[9]

## 2.6 Lessons Learned from Previous Incidents

2.6.1 Naturally, attackers have become more sophisticated in their methods over time; however, attacks against the DNS—as well as attacks that rely on exploitation of DNS weaknesses—are not new. The recent history of these incidents can help chart a path for better incident response in the future.

### 2.6.1 Conficker worm

2.6.1.1 In late 2008, Internet security researchers and operating system and antivirus vendors discovered an infection, now known as "Conficker,"[10] that would go on to infect untold millions of computers with a software worm that can enlist its victim computer into a botnet.[11]

2.6.1.2 The scale of the worm's penetration, as well as attempts to disable its command and control (C&C) system, eventually required action in the DNS environment to proactively capture, block or disable domain names through which various payloads and C&C information could be exchanged. During the Conficker response and remediation efforts, DNS registrars, along with ICANN, security researchers, law enforcement and operating system and security software vendors collaborated to establish a coordinated response to the aspects of Conficker that involved the DNS.

2.6.1.3 While these efforts proved useful, a principal lesson learned by the Conficker Working Group was that having a **dedicated and sustained incident response coordination capability** would have enhanced the global response to this issue.

### 2.6.2 DNS protocol vulnerability

2.6.2.1 In mid-2008, security researcher Dan Kaminsky identified a cache poisoning attack strategy with a vast potential for exploitation. The attack exploited certain timing and sequencing assumptions in the DNS protocol to permit the intentional misdirection of requests for a period of time. Due to the nature of the attack, many in-place systems were vulnerable to exploitation.

---

[8] Proceedings of Global DNS Security, Stability and Resiliency Symposium, April 2009, p. 11.
[9] European Parliament. 2006. The European Programme for Critical Infrastructure, Memo/06/477.
[10] Conficker was also known by a variety of other names, including "Code Red," "Blaster," "Sasser," "Downandup" and "SQL Slammer."
[11] Honeynet Project. "Know Your Enemy: Containing Conficker." (Downloaded from http://www.honeynet.org/papers/conficker)

2.6.2.2 Although the DNS community began remediation very quickly, if the same vulnerability had been identified under different circumstances it might have been used for illicit purposes without any warning. In addition, without a clear understanding of the problem, the DNS vendors might not have coalesced in the face of the vulnerability. In such a case, a **response coordination capability by a known and trusted entity** would have benefitted policymakers, who wish to be alert to threats against a healthy and functioning Internet and to the DNS community itself.

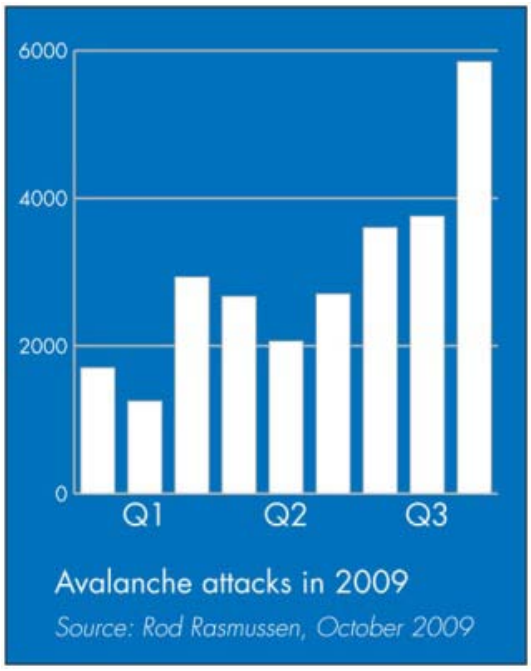
### 2.6.3 Domain hijacking

2.6.3.1 In early 2009, an attack, apparently mounted against several country code top-level domain (ccTLD) registration systems, allowed the unauthorized redelegation of DNS zones in order to serve content that was not provided by the legitimate domain name registrant, largely in support of the attacker's political agenda.[12]

2.6.3.2 The attack involved a series of registrars responsible for these domains, and no mechanisms existed for rapidly making these potentially targeted registrars aware of the ongoing threat. **Mechanisms for information sharing related to threats specifically involving the DNS** must be established.

### 2.6.4 Avalanche and the Zeus botnet

2.6.4.1 Beginning in December 2008, registrars were subjected to a new series of attacks, referred to as "Avalanche," which was targeting online financial services through the use of the Zeus botnet infector.[13] In this case, one key characteristic is that the attackers initiate a broad attack from domains registered through a very small number of registrars (from one to three) at any time.




2.6.4.2 This method appears to specifically take advantage of the **limited, or possibly nonexistent, incident response and legal resources available to smaller registrars**, who become unable to cope with the cascade of takedown requests and subsequent credit card chargebacks. As shown in the graph here, the rate of upward trend in attacks against registrars is increasing quarter-on-quarter, taxing the ability of registrars to respond in a timely fashion.

[12] ICANN Security Team. 2009. "Potential attack against ccTLD registration systems," ICANN Situation Awareness 2009-07-13.

[13] See Internet Identity. Phishing Trends Report: An Analysis of Financial Fraud Threats for Third Quarter 2009, available at http://www.internetidentity.com/images/stories/docs/phishing %20trends%20report%20-%20q3-2009%20internet%20identity.pdf

2.6.2 These case summaries illustrate the need for a standing DNS security response capability, as well as the wide range of contingencies and stakeholders that may be involved.

## 2.7 Response Design Challenges

2.7.1 Building an effective response capability requires flexibility in the face of a continuously changing threat landscape and a consistent and continuous effort to achieve success.

*2.7.2* ***Agility****.* Malware writers are not only agile and elusive, they are adaptable to changes in the operation of the Internet's infrastructure. It will not be possible to sustainably reduce their operations or put them out of business without adopting a similarly agile response model.

*2.7.3* ***Continuity****.* In the cases cited here and in others, success has rested on community collaboration. But collaboration can be difficult to sustain and complex to manage. Because the continuity of collaboration can be more fragile than botnets, the risk-versus-reward equation currently favors botnet creators and those conducting sustained phishing campaigns.

*2.7.4* ***Availability****.* Naturally, because it is a global resource, the health of the DNS must be established on a round-the-clock basis. As a direct consequence, aberrations to a healthy DNS should be identified as quickly as possible, prioritized, triaged and handled with all due speed. This kind of availability speaks strongly to the need for a 24-hour incident response capability. Additionally, the stakeholder base of a DNS-CERT will require that staff and communications materials to be available in an appropriate variety of languages.

## 2.8 Stakeholders

2.8.1 By its very nature, the DNS is relied upon by a substantial number of organizational entities, from which DNS-CERT stakeholders would arise. While a comprehensive and validated list of DNS stakeholders is not yet established, such a list would include:

- Operators, such as DNS root operators, ccTLD registries, gTLD registries and registrars
- Regional Internet Registries (RIRs), National Internet Registries (NIRs), Local Internet Registries (LIRs) and Internet Service Providers (ISPs)
- Computer Emergency Response Teams (CERTs)
- Governments and Critical Information Infrastructure Protection (CIIP) authorities

2.8.2 Moreover, because of the fundamental nature of the DNS, an extremely large number of entities can claim to be stakeholders, among them:

- End-users and registrants
- Industry vertical markets, such as financial institutions, e-commerce enterprises and large brands that operate a substantial portion of network infrastructure
- DNS vendors

- Organizations that now provide some type of DNS security response service
- Policymaking bodies

2.8.3 The DNS-CERT must leverage and partner with a wide range of existing organizations and activities that currently support improved security awareness, response and resiliency across the DNS, such as the DNS Operations, Analysis and Research Center (DNS-OARC) and the Registry Internet Safety Group (RISG). The activities of the DNS-CERT can help collaborate in coordinating these efforts and provide services in areas currently not covered or with stakeholders that are not engaged in these efforts. The capacity analysis here shows an initial appraisal of possible partners for a DNS-CERT.

Capacity gap analysis ** Private/selective groups are excluded from the list **

| Framework | Project Sponsor | Public/Private | Participants – function | Participants Geographical distribution | Scope/mission | Operating funding model |
|---|---|---|---|---|---|---|
| **DNS OARC** | DNS OARC, inc. | Public | Key operators, implementers, security providers, and researchers | Global | Information/data sharing (DNS-ops), workshops, data analysis, tools | Membership fee |
| **Registry Internet Safety Group (RISG)** | .ORG The Public Interest Registry, SIDN, Affilias, etc | Public Membership organization | gTLD, ccTLD registry- focused, domain registrars, security vendors and law enforcement agencies | North America | Data sharing, ML, Combat Internet identity theft, share data to improve overall Internet user security | No annual membership fee but members contributes activities cost |
| **CWG** | Microsoft and others | Public | Collaborative effort with technology Industry leader/academia | North America | Collaborative response for Conficker Warm | Organization/ individuals Voluntary base |
| **FIRST** | FIRST.Inc | Public / membership | Vetted community of CERTs/ CSIRTs | Global | Information sharing for Cyber security incident/ threat response | Annual Membership fee |
| **ISC SIE** | ISC | Private | Network operators (ISPs, enterprise, academic, and research), law enforcement (internationally), security companies (anti-virus, intrusion detection, &etc), research (academic, Internet do-gooder, government, and commercial) | | Information/data sharing in the Internet Security field. Shares mainly DNS information. Supports DNS security measurements and also information (e.g. passive DNS discovery of fast flux DNS names) | Fee structure |

# 3. Future State

The creation of DNS-CERT capability will afford the DNS community a **sustained** and **global** incident coordination capability that serves its broad spectrum of stakeholders.

## 3.1 Vision and Mission

3.1.1 The **vision statement** for the DNS-CERT is intended to describe our long-term hope and ambitions—our fully realized conception of such an organization and community—many years from today. This statement describes what the organization intends to become and should resonate with all stakeholders and staff, giving shape and direction to the organization's future.

3.1.2 The proposed *vision statement* for DNS-CERT is:

*To enhance the security, stability and resiliency of the Global DNS.*

3.1.3 The proposed *mission statement* for DNS-CERT is to:

*Ensure DNS operators and supporting organizations have a security coordination center with sufficient expertise and resources to enable timely and efficient response to threats to the security, stability and resiliency of the DNS.*

3.1.4 Both the vision and the mission statements should be reviewed on a regular basis to ensure they remain in step with the needs of the DNS-CERT constituency.

## 3.2 Goals and Objectives

3.2.1 To achieve its mission, the DNS-CERT must maintain and regularly measure its performance against a set of goals and objectives that support the group's mission.

### 3.2.1 Goal: Gain situational awareness and share information

3.2.1.1 The DNS-CERT should enhance the ability of the DNS operational community to gain and share situational awareness about threats, vulnerabilities and risks related to the global DNS. Such situational awareness will be focused toward stakeholders with limited security resources, such as small registries and DNS operators in the developing world.

3.2.1.2 **Objective:** Establish communications means and procedures to maximum number of players; exercise regularly.

### 3.2.2 Goal: Improve coordination within the DNS operational community

3.2.2.1 The DNS-CERT should improve coordination of actions taken across the DNS operational community.

3.2.2.2 **Objective:** Enable measurement and facilitate information sharing about the health, stability and resiliency of the DNS. Engage in appropriate situations: support contingency planning and exercises; undertake After Action Reporting (AAR). Engage with DNS-OARC and RISG, among others collaborators, to leverage expertise and existing operational response capabilities related to information sharing and analysis.

### 3.2.3 Goal: Improve coordination with the broader security community

3.2.3.1 The DNS-CERT should improve coordination of actions taken within the DNS community as well as the concerns of the global Domain Name System with the broader cyber security community.

3.2.3.2 **Objective:** Establish relationships with key partners (CERTs, security researchers, key security lists, vendors, antivirus companies, law enforcement and governments); participate in contingency planning and exercises; engage in appropriate situations; undertake After Action Reporting (AAR).

## 3.3 Scope of Operations

3.3.1 The DNS-CERT operations are expected to evolve and mature over time based on factors such as constituency needs, funding, exigencies, policy drivers and technical capability of the CERT itself. Although the team management will establish the specific stakeholders with whom the DNS-CERT interacts and to whom it provides services once it achieves an initial operational capability, we anticipate that the primary support will be channeled to DNS operators, registries, registrars, national CERTs and relevant vendors.

## 3.4 Services Provided

3.4.1 The team will be principally focused on DNS operators, in the form of reactive and proactive services such as:

- 365 x 24 x 7 point of contact
- Dashboard service to measure DNS health and security status
- Incident handling coordination or direct assistance
- Vulnerability management support
- Security advisory services
- Watch and warning services
- Education and training

3.4.2 Definition of functional requirements for providing core DNS-CERT capabilities will occur through community-based analysis involving the stakeholders and potential collaborators for a DNS-CERT and will be documented in a Concept of Operations. This analysis will include a focus on an initial set of DNS-CERT operating capabilities.

## 3.5 Strategic Partnerships

3.5.1 Beyond basic services, the DNS-CERT will launch with an initial set of strategic partners:

- Organizations involved in incident response (DNS-OARC, FIRST, ENISA, and the like)
- DNS related software and browser vendors (ISC, NL Net Labs, Microsoft, and the like)
- DNS security vendors (Internet Identity, Mark Monitor, and the like)
- Regional TLD associations

## 3.6 Situational Awareness and Information Sharing

3.6.1 The DNS-CERT must keep abreast of developments in, threats to, and ongoing remediation actions in the Domain Name System. This continuous situational awareness will be the cornerstone of the DNS-CERT, and will lead to information sharing within the DNS community (to the maximum extent permitted by policy). Pervasive situational awareness will allow the community, particularly DNS operators and vendors, to ensure that their own design or protective efforts meet the contemporary threat landscape.

## 3.7 Interagency and Inter-organizational Coordination

3.7.1 Using resources such as the projected **ccNSO incident response contact repository**, the **FIRST incident response team directory**, the **DNS-OARC**, the proposed **DDoS collaborative**, and continuous outreach to Internet related organizations, the DNS-CERT can provide rapid interagency and inter-organizational coordination that supports incident management, coordination drills or ad hoc information sharing requirements.

## 3.8 DNS-CERT Quality Enhancement

3.8.1 A Computer Emergency Response Team maintains its relevance by providing services that are deemed valuable by its constituency; by maintaining a high standard of objectivity and quality; and by ensuring quality improvement through feedback received both internally and from customers.

3.8.2 Therefore, the DNS-CERT will be measured internally, and by its Board of Governors, based in large part on customer input and feedback. The specific governance structure for this organization has yet to be determined.

## 3.9 Constituency

3.9.1 To ensure its effectiveness, DNS-CERT must have a clearly defined constituency. Although the community of those who rely on the DNS extends to every user of the Internet, a more relevant way to scope the constituency of the DNS-CERT would be based on the connection with DNS operations. This construct can be further delineated in terms of whether the organization participates directly, collaborates with DNS-CERT operationally, relies on it for operational purposes, or relies on it to support policymaking or other purposes.

### 3.9.1 Participants

3.9.1.1 Some external organizations may be in a position to supply human or technical resources at the disposal of DNS-CERT for periods of time in order to allow the team to achieve maximum impact in a limited amount of time. In nearly all cases, participants will also be constituents, although this need not be the case exclusively.

- ICANN staff entities
- DNS-related organizations
- DNS operators security teams

- Incident response organizations such as national CERTs, the Anti-Phishing Working Group (APWG), and Forum of Incident Response and Security Teams (FIRST)

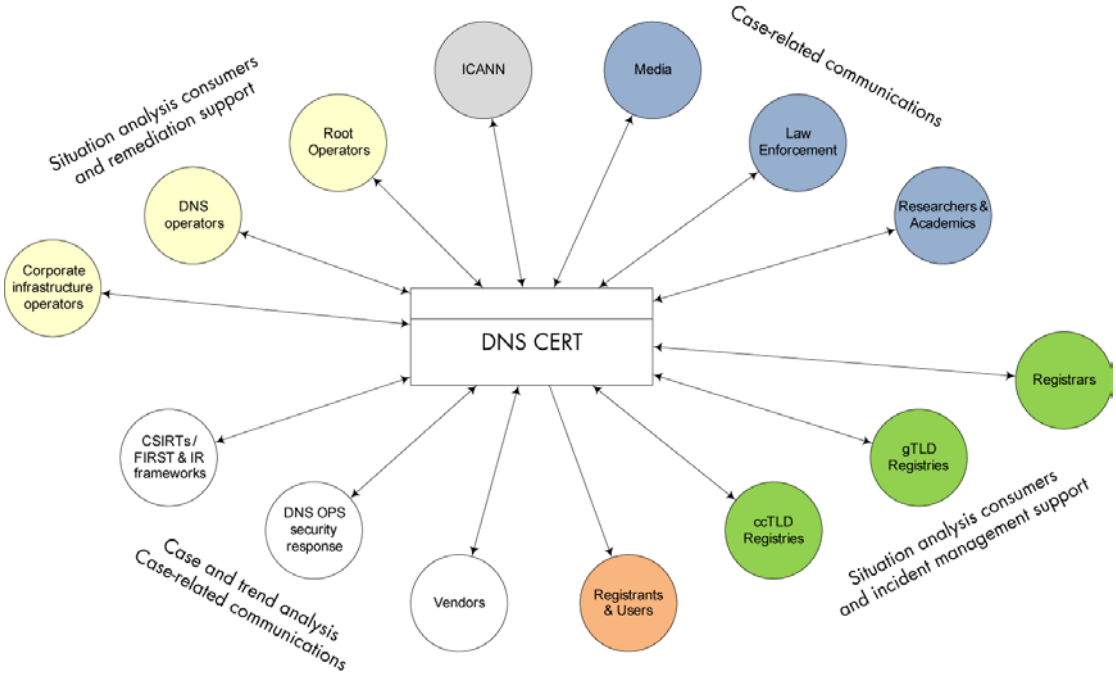
### 3.9.2 DNS operational community

3.9.2.1 The DNS operational community will have a natural connection to the DNS-CERT by virtue of the common interest in assessing and remediating problems with DNS health.

- Root server operators and supporting organizations
- Registries and registrars
- DNS vendors
- Other interested and qualified parties, as identified by the DNS-CERT management

### 3.9.3 DNS policy and decision-making community

3.9.3.1 In addition to the operational community, the governance and policy management of the Internet also requires an up-to-date understanding of threats to the DNS and the status of remediation activities underway related to such threats. The graphic here shows a concept of information gathering and distribution about threats to the DNS.



# 4. Implementation Strategy

The development of the DNS-CERT requires detailed analysis of its initial structure so that resources can be devoted to its operation, internal and external interactions can begin to be defined, and milestones toward the DNS-CERT's initial operational capability can be tailored.

## 4.1 Mission Analysis

4.1.1 To follow the Computer Security Incident Response Team (CSIRT) development guidelines recommended by CERT/CC, we have engaged the following analysis elements for establishing the DNS-CERT:

| | |
|---|---|
| 1. | Identify stakeholders and participants. |
| 2. | Obtain management support and sponsorship. |
| 3. | Develop a CSIRT project plan. |
| 4. | Gather information. |
| 5. | Identify the CSIRT constituency. |
| 6. | Define the CSIRT mission. |
| 7. | Secure funding for CSIRT operations. |
| 8. | Decide on the range and level of services the CSIRT will offer. |
| 9. | Determine the CSIRT reporting structure, authority, and organizational model. |
| 10. | Identify required resources, such as staff, equipment and infrastructure. |
| 11. | Define external interactions and interfaces. |
| 12. | Define roles, responsibilities, and the corresponding authority. |

4.1.2 In addition to addressing these issues in this business case, ICANN staff has developed a mission analysis briefing that is envisaged to be the basis for further development of this effort through community support and feedback.

## 4.2 Operating Funding Model

### 4.2.1 Initial sustaining commitment

4.2.1.1 Initially it is envisaged that ICANN will work to establish a funding approach to establish the team's initial operational, logistical and financial support. A long-term funding model will be determined through dialogue and support from the DNS operational community and the broader stakeholder base.

### 4.2.2 Estimated resource requirements

4.2.2.1 Based on resource estimates from other, relatively similar CERT capabilities at a national level, we estimate that the DNS-CERT can function with an annual budget of $4.2million USD at a satisfactory level. Staffing and support requirements will include:

- Head of CERT (responsible for strategic/budget planning, outreach and liaison to stakeholders)
- Operational Director (responsible for technical operations)
- 10 technical incident response managers (for regional global coverage, one of whom is Operational Director)
- Business Director (responsible for legal and budget matters)

- 2 overhead staff (administrative and accounting areas)
- Support for operations; coordination and travel; communications and IT; as well as physical facilities.
- (HR) 3 directors – $600K USD, IMs x 10 – 1M $700K USD, 2 overhead – $300K → $2M 700K USD
- (Others) travel – $250K USD, portal, communication and IT/tools – $850K USD, physical facilities – $250K USD, other admin – $150K → $1M 150K USD

## 4.3 Governance Structure and Accountabilities

4.3.1 Although we envisage the organization being established with initial support from ICANN, the DNS-CERT is intended to operate as much as possible as a freestanding organization, not directly dependent upon any one organization for its direction and operation. Therefore, to be successful, the DNS-CERT must be created with a governance structure that makes it accountable to key stakeholders and to the public at large.

### 4.3.1 Project sponsor

4.3.1.1 Initial DNS-CERT development would be sponsored by ICANN until the organization can stand on its own. ICANN would designate a task leader to oversee the project and lead the steering committee until the DNS-CERT's initial operational capability is achieved.

### 4.3.2 Steering committee

4.3.2.1 During its creation and initial stand-up, we envision the creation of a stakeholder-based working committee to undertake the actions required to govern the implementation of the DNS-CERT until it achieves an initial operational capability. The role of the steering committee is purely related to the operational establishment of the DNS-CERT, and this committee will cease to function when the DNS-CERT achieves initial operational capability, on a date to be specified by the Board of Governors.

### 4.3.3 Board of Governors

4.3.3.1 Once operational, oversight of the DNS-CERT will be by a Board of Governors that represents a broad range of community stakeholders.

### 4.3.4 Roles, responsibilities and external interfaces

4.3.4.1 Beyond the governance bodies listed here, the roles and responsibilities for all DNS-CERT functions, whether direct-line responsibilities or cross-functional team relationships, will be described in a DNS-CERT Concept of Operations. The interfaces between DNS-OARC, other CSIRTs and external bodies or functions related to the mission of the DNS-CERT will also be detailed in the Concept of Operations. To the extent possible, authorities and responsibilities that appear to be ambiguous or overlapping between the DNS-CERT and other organizations will be clarified. The DNS-CERT is based on a collaborative approach but will not have the authority to respond directly to any stakeholders.

## 4.5 Organization Structure

4.5.1 The operations of the DNS-CERT will be overseen by a core team of administrative and technical staff and will be assisted by an extended team consisting of *virtual augmenters* who can provide tangible support to the DNS-CERT while operating in a geographically dispersed fashion.

### 4.5.1 Core team

4.5.1.1 A core team of staff will provide day-to-day administrative services and serve as a point of contact for the DNS-CERT team. Additional full-time staff joining from other organizations is also envisioned.

### 4.5.2 Extended team

4.5.2.1 Participating institutions and affiliates will be able to participate in the DNS-CERT in a virtual manner. DNS-CERT management, in consultation with legal support, will establish the level of participation and integration into the DNS-CERT operations. However, whatever the level of integration, the extended team of augmenters will provide the DNS-CERT with both geographic and time zone flexibility, while working toward meeting the team's global commitments.

### 4.5.3 Participating institutions

4.5.3.1 The DNS-CERT participants will come from the family of organizations, teams and individuals who have critical DNS operations expertise and incident response expertise, as well as those with system and vendor expertise. Moreover, the DNS-CERT management can tap others as the need arises, with the key objectives being flexibility, breadth of representation and geographic dispersion.

### 4.5.4 Professional support services

4.5.4.1 Aside from the technical and policy expertise that are required on a day-to-day basis, the DNS-CERT will require a variety of legal, public affairs and financial support on an ad hoc basis. Refer to paragraph 4.2.1, Initial sustaining commitment.

## 4.6 Communications Management Among Stakeholders

4.6.1 During the definition and stand-up phases of the DNS-CERT project, key stakeholders will be routinely apprised of project status to ensure that:

- The detailed plans for the DNS-CERT accurately reflect the needs of the broad-based constituency
- Stakeholders understand and shape the key factors driving the need for its establishment
- The DNS-CERT steering committee has an accurate understanding of recent and ongoing incidents that are shaping the DNS security and resiliency landscape, such as Conficker and domain hijacking attacks
- Stakeholders understand any incident response that is already under way, and how it might integrate into a new DNS-CERT function

4.6.2 In addition, during its stand-up, the DNS-CERT project management must address questions of data ownership, intellectual property (IP), and authority, particularly as these pertain to publications, products or information collected or developed by the

DNS-CERT. The answers to these questions will require legal and policy reviews before they are adopted.

4.6.3 Further, political and compliance issues, including any public, private, academic, governmental or military rules, regulations or policies that must be followed should be addressed while the DNS-CERT is being established. In connection with this review, the impact of any such rules, regulations or policies upon participating organizations must be clearly defined.