**DNS Operations, Analysis and Research Center**

# DNS-OARC Public Comment on ICANN's DNS-CERT Business Case

## Introduction

DNS-OARC http://www.dns-oarc.net was established in 2004 to address a forseen and growing need to improve the stability, security and understanding of the Internet's DNS infrastructure. Initially funded by the Internet Systems Consortium and a National Science Foundation grant, it is now an established nonprofit with over 60 DNS registries, registrars, operators, researchers and vendors comprising its membership.

DNS-OARC's mission is: *to build trust among its members through forums where information can be shared in confidence; to enable knowledge transfer by organizing semiannual workshops; to promote research through data collection, analysis, and simulation; and to increase awareness with publicly available tools and services.*

DNS-OARC has been following the DNS-CERT proposals closely as there is much in common between its existing mission and that proposed for DNS-CERT. To date DNS-OARC has worked closely with ICANN in these areas, including collaboration on running the 2 Global DNS Security Stability and Resilience symposia, and participation in the recent DNS-CERT gap analysis workshop.

We are grateful for the co-operation we have received from ICANN in this collaboration, and for ICANN's support both as a member and in funding of our data gathering and analysis related to the DNSSEC signing of the root zone.

In general DNS-OARC welcomes the additional attention that ICANN has brought to the subject are of its mission, and we agree with ICANN's position that additional funding and resources for this area would be beneficial. We do however have some concerns about potential overlap, and some aspects of the approach proposed, which are detailed below.

The views represented in this paper should be noted as being representative of the view of DNS-OARC in its own right, and not necessarily those of OARC's individual members.

## DNS-OARC's Capabilities

In the 6 years since its inception, DNS-OARC has developed a number of capabilities with which to fulfill its mission. Many of these are in established widespread use by the DNS operator community, and have contributed both to the response to specific large-scale incidents the global DNS infrastructure has faced, and to the standards of knowledge and best practice within the wider community. Many of these capabilities are compatible with the mission of DNS-CERT, and should be considered as resources that DNS-OARC can "bring to the table" of DNS-CERT's mission.

These capabilities include:

- Regular open and member-only meetings.
- A website which places substantial key knowledge, resources and information in the public domain, together with a private section which include a member operational contact directory.
- Data gathering, monitoring and analysis infrastructure.
- Archive Data Sets, amounting to over 40 Terabytes dating back 5-10 years.

- Open, member-only, closed-user and vetted-only mailing lists for knowledge and information sharing, together with a PGP encryption key repository for secure e-mail exchange.
- Secure real-time Jabber/XMPP-based instant messaging service for members to instantly get in touch and co-ordinate responses during incidents.
- Publicly available tools for testing, verifying, probing and scanning DNS infrastructure for appropriate behavior and vulnerabilities. Use of many of these tools generate further data sets.
- Relationships with researchers which allow for analysis and characterization of data, incidents and attacks.
- Formal relationships with our members which establish DNS-OARC as a self-governing, self-funding neutral membership organization, and places legally-binding confidentiality requirements on all participants.
- Governance structures including a Delaware legal entity with 501(c)3 nonprofit status and a board of Directors elected by its members.
- Full-time staff dedicated to fulfilling DNS-OARC's mission.

### Partnership with Existing Initiatives

There are various global initiatives that resemble a CERT-like organization. DNS-OARC wishes to draw attention to their existing activities and emphasize the important of working collectively with them.

- Mailing lists: there are several which require vetting and which share global incidents (OARC's dns-secureops list, NXD, NSPSEC etc).
- Meetings: There are several technical colloquia that allow for operationally-relevant DNS meetings, such as DNS-OARC, CENTR-TECH, ICANN's ccNSO-TECH/DNSSECWG, RISG.
- Active Incident Handling: what might not be shared on the afore-mentioned lists and meetings, is the actual coordination/mitigation of an attack or threat. There are however established CERT organizations that handle those incidents. Some ccTLD registries already operate a CERT on a national level. Lastly, some do have a helpdesk, publish abuse contact addresses, various online tools, and are monitoring lists to handle incidents with actively participating staff, though they do not call it a CERT.

DNS-OARC encourages all organizations to develop a CSIRT-like internal organization or structure. The subsequent step would then be to join FIRST (a vetted membership organization) and/or DNS-OARC in order to share incidents and mitigated threats in a bi-lateral and trusted way.

## DNS-OARC Position on a Global DNS-CERT

It is DNS-OARC's view that in order for DNS-CERT to have some impact as a CERT, there needs to be a constituency for it to operate in, including some form of jurisdiction over that constituency, for it to be effective. A CERT needs to gain trust from outside constituencies and other CERTs, in order to share incidents and effectively mitigate threats. This can not be dictated top down, or by unilateral proclamation.

It is also DNS-OARC's experience that sharing of information, whether though data gathering or incident notification, is something that is both essential to DNS infrastructure protection and is something that cannot be compelled. Trust is a very necessary pre-condition for such sharing, but even with trust we have seen that information is not always shared, and some valuable lessons have been learned about what practical limits exist on information sharing.

While ICANN might forsee that extending its jurisdiction could be a means to create a stick for the new gTLDs to participate in DNS-CERT, there is no comparable carrot for the ccTLDs. Additionally, it is unclear what incentives registrars might have to voluntarily co-operate, as co-operation will inevitably lead to loss of income when domains have to be canceled, on top of the labor costs involved to monitor and cancel those.

For an organization such as DNS-CERT to generate the trust it requires to be effective, ICANN needs to allow this entity to be governed and operated outside of the realm and reach of ICANN, working with already established and trusted organizations within the Registry/Registrar/ISP world.

It is projected that the DNS-CERT operating budget will be about US$4.2M annually. ICANN proposes that it is operated by an independent, free-standing entity, governed by a sponsor-based board. At present however there is currently only one sponsor: ICANN. This carries a risk of 'capture' - DNS-CERT can only be truly independent if funded by diverse sponsors and not just ICANN.

**Conclusion**

DNS-OARC encourages education and awareness in mitigation of threats and handling incidents, and welcomes ICANN's raising the profile of the need for this. We feel it is necessary that this awareness is developed inside organizations that already have a responsibility for parts of the DNS community (such as TLD registries). Subsequently, these organizations can join already established vetted communities like FIRST or DNS-OARC.

DNS-OARC strongly encourages ICANN to work in co-operation with it to build upon DNS-OARC's existing established capabilities within the context of wider DNS security co-operation and initiatives. DNS-OARC would not support any DNS-CERT activity to the extent that it would unnecessarily duplicate DNS-OARC's own capabilities.

We remain to be persuaded of the requirement for developing a single, global DNS-CERT. ICANN has correctly identified some gaps between the capabilities of the existing established DNS security organizations and activities, and DNS-OARC welcomes this analysis. Given the large size of the total potential problem and solution space, we think that it would be overly ambitious to attempt to establish a single over-arching new organization to address all of it. Rather it would be far more effective to fully recognize established activities, and dedicate a more modest budget on addressing the gap. This can be through support and funding to establish, assist and enhance trust and co-operation between these existing organizations.

Building education and awareness of incident handling and mitigation of threats, including development of response teams within, and further consensual co-operation between, existing ICANN constituency organizations will lead to a decentralized global cooperative. We believe that this will be far more effective, with greater ultimate reach and legitimacy than a single central DNS-CERT.

---

*14-Apr-2010*