Country Code Names Supporting Organization

Comments on ICANN DNS-CERT proposal

April 2010

The ccNSO welcomes the opportunity to comment on ICANN's draft business case for the development of a Domain Name System Computer Emergency Response Team (DNS-CERT)[1]. In addition to this response, a number of ccTLD managers and regional country-code organisations may also provide individual responses to ICANN's call for comments.

While ccNSO members support and share ICANN's focus on ensuring the security and stability of the DNS, many hold significant concerns with the proposed CERT project. These concerns relate to:

- an apparent lack of consultation and possible overlap with existing network security stakeholders;
- A lack of clarity regarding the perceived need for a DNS-specific CERT and the types, severity and frequency of threats the CERT would address;
- the structure of, and budget for, the proposed CERT; and
- the speed at which the initiative has been developed and tight timeframes for implementation.

At the broadest level, we are concerned that ICANN has made a number of assumptions regarding perceived weaknesses in current network security measures, the level and frequency of threats, the need for a new coordination body, and the position this body will assume. ICANN also appears to be moving with undue haste to act upon these assumptions.

Our recommendations to address the short-comings of the current proposal are listed at the end of this commentary.

Consultation and co-ordination with existing network security stakeholders

Although ICANN's DNS-CERT business plan acknowledges existing security stakeholders such as CERT/CC and the CERT network, FIRST and DNS-OARC and other involved parties such as RIRs, DNS Root Operators, registrars and ccTLD and gTLD registries, little effort appears to have been made to engage these groups in developing the DNS-CERT proposal. This lack of dialogue leads to the potential for duplication of efforts and confusion, rather than clarification, of specific roles and responsibilities.

The range of operators listed by ICANN serves to indicate precisely the breadth of existing initiatives and experience. These networks are well established and a key element of their operation and inter-relation is the mutual levels of trust generated from years of operation. In the diagram on page 14 of the business case, ICANN has placed the DNS-CERT squarely at the centre of DNS-threat response efforts. ICANN must be mindful of, and move to mitigate, the potentially disruptive influence this could have, and the damage that could be caused to the chain of trust, should the project proceed without the buy-in and support of all players.

[1] http://www.icann.org/en/public-comment/#dns-cert

Demand for a DNS-CERT

ICANN's DNS-CERT draft business case lacks detail regarding precisely which industry stakeholders have called for the development of this initiative. It would be very helpful for ICANN to provide those commenting on this proposal with a clearer understanding of *who* has asked for this initiative and precisely *what* issues it is expected to mitigate. ICANN must complete a detailed survey of the range, severity and frequency of current and potential threats to the security and stability of the DNS and an analysis of whether these threats can be mitigated by existing structures and stakeholders.

Specifically, it would be valuable for ICANN to clarify:

- What is the DNS-CERT expected to tackle now and what future processes and needs might this also encompass?
- What is the capability of the current organisations and CERTs already in existence?
- What is the gap that is not currently being addressed by these organisations?

This analysis cannot be done in isolation and must involve all relevant players from both the DNS operations and broader computer security communities.

Currently, ccNSO members are unaware of any ground-swell of concern regarding either current security measures, or specific issues that cannot, or are not, being capably addressed by other bodies.

In addition, ICANN's justifications for establishing a new organisation are regrettably vague, and presented without an appropriate evidentiary basis. For example, in section 2.5 of the business case, ICANN cites resource, language and geographic constraints experienced by "many DNS operators" as points of vulnerability and proposes the DNS-CERT as the entity to assist in resolving these constraints. In this particular example, it is critical for ICANN to identify who and where these potentially vulnerable "operators" are, and to collaborate with existing stakeholders to confirm whether a lack of support does, in fact, exist.

Proposed DNS-CERT structure and budget

The DNS-CERT business case currently envisages the organisation as an independent body, with initial guidance and funding from ICANN. This aspect of the proposal is relatively - and possibly prematurely - advanced, with considerable detail regarding sponsorship, governance arrangements and team roles and responsibilities. Given significant set-up, infrastructure and staffing costs, the proposed annual operating budget is approximately US$4.2 million. This is a considerable financial commitment and it is unclear whether ICANN, as initial sponsor, intends to provide all of these funds through its own internal budget, should it be unable to achieve support from third parties. The size of the exercise and financial commitment also gives rise to questions regarding whether establishing a new, dedicated DNS-CERT is the best solution to perceived capacity gaps, or whether this amount of funding could be better spent supporting current activities.

As such, detailed consideration of budgetary issues should be included in the threats, risks and needs analysis proposed above. At the earliest possible stage, ICANN should also approach those stakeholders who are calling for a DNS-CERT to confirm whether they would be willing to provide financial support for the initiative.

Speed of implementation

As the ccNSO noted at the Nairobi ICANN meetings, ICANN is moving with un-justified haste in developing a solution to a perceived problem at the risk of under-valuing or even undermining existing initiatives.

As an example of the possibility of haste damaging current arrangements, the comments of ICANN's CEO and President, Rod Beckstrom, to governmental representatives in Nairobi, have the potential to undermine the productive relationships established under ICANN's multi-stakeholder model, cause damage to the effective relationships that many ccTLD operators have developed with their national administrations and discounted the huge efforts of many in the ICANN and broader security community to ensure the ongoing security and stability of the Internet.

As stated in Nairobi, the ccNSO shares and supports ICANN's focus on security-related issues, though recommends a measured, strategic, inclusive response. ICANN must follow due process in consulting stakeholders, gathering evidence and developing a response strategy, rather than proposing a solution to a problem that is not clearly identified.

Recommendations

ccNSO members recommend that ICANN establish a joint SO/AC Working Group to draw upon their collective expertise and to solicit input on:

- the broad concept of a DNS-CERT;
- the current work being undertaken to mitigate DNS-related threats;
- the actual level, frequency and severity of these threats;
- the gaps (if any) in the current security response to DNS issues;
- whether or not a DNS-CERT is a proposal they support; and
- if so, the logistics of the proposal.

The Working Group should have the option of inviting participation from external experts and the group's recommendations and findings must be circulated to the broader Internet security community for comment. Any final proposals ICANN and its immediate community arrive at should also be widely consulted upon, and should seek the support of all existing security stakeholders. This group could be formed at the ICANN meeting in Brussels in June, if not sooner and ccNSO members look forward to contributing their knowledge, networks, expertise and experience to this dialogue.

Chris Disspain
Chair – ccNSO Council