Canadian Internet Registration Authority

Autorité canadienne pour les enregistrements Internet

Comments on ICANN's
Global DNS-CERT Business Case
April 14, 2010

The Canadian Internet Registration Authority (CIRA) is the not-for-profit corporation responsible for operating the .ca country code top level domain. CIRA is a member of ICANN's country code Name Supporting Organisation (ccNSO) and a member of CENTR, an association of Internet Country Code Top Level Domain Registries. CIRA is pleased to have the opportunity to provide comments on ICANN's Global DNS-CERT Business Case.

As a DNS operator, CIRA supports ICANN's focus on ensuring the stability and security of the DNS. However, as a user of existing response mechanisms, we would like to express concerns over ICANN's proposed DNS-CERT.

There is no consensus currently within the Internet community that ICANN should be operating a DNS-CERT. The business case quotes from the summary report of the April 2009 Global DNS Security, Stability and Resiliency Symposium, the first of its kind to bring together cross-functional stakeholders to address risks to the DNS. The quote pulled from the Symposium's report supports the position that gaps in DNS security require action, and the business case then draws the conclusion that ICANN must take that action.

However, the Symposium report also reveals that attendees of the Symposium, participants from a wide range of areas collaborating on cross-functional solutions to DNS risks, were of two camps: one supportive of ICANN's involvement in a DNS-CERT, and one "vehemently" opposed to ICANN's involvement.

More recently at ICANN's 37th meeting in Nairobi in March 2010, many community members also expressed opposition to ICANN's proposed management of the DNS-CERT for a variety of reasons, including the following:

1. **Lack of consultation and analysis**

As stated, CIRA shares ICANN's preoccupation with DNS security and stability. One of CIRA's top priorities is a robust DNS, and we empathise with ICANN's CEO's desire to continuously improve DNS stability and security. However, we do not believe that sufficient analysis has been conducted to support the solution ICANN proposes.

First of all, little effort appears to have been made to consult with existing security stakeholders and analyse where the gaps are in current response mechanisms. Unilaterally forging ahead with an ICANN-centric solution is contrary to the multi-stakeholder model required of ICANN in the Affirmation of Commitments. As well, such an approach will undoubtedly lead to duplication of efforts and resulting misspending of the community's funds.

In addition, ICANN has not provided sufficient detail with respect to the threats to and vulnerabilities of the DNS that prompted the development of this proposal. More detailed information and analysis is required in order to clearly identify what model would best address the gaps and risks, and suit the community's needs.

2. Concern over the budget

There are concerns as well with respect to the manner in which ICANN has allocated the budget for the DNS-CERT, which is estimated at $ 4.2 million USD. This is a considerable financial commitment to undertake without a thorough examination of existing organisations and community consultation to determine if the money could be better spent supporting other initiatives. Given that ICANN's revenue is nearly entirely generated from community stakeholders, it concerns us that ICANN would attempt to undertake such a substantial financial commitment without proper prior consultation with those who will ultimately be responsible for funding the initiative. We also question whether the community should be paying for something which would be better or preferably managed by another organisation.

3. Concern that managing the DNS-CERT is outside ICANN's mandate

The DNS-CERT business case states that ICANN has committed to "preserve the security, stability and resiliency of the DNS," and draws the conclusion that, as a result, ICANN should spearhead the DNS-CERT initiative. We would argue that this may not be a correct conclusion.

ICANN does play an important role with respect to its commitment to preserving the security of the DNS. As ICANN's July 2010 – June 2013 Strategic Plan states, ICANN is and will continue to be undertaking many activities in order to carry out this commitment, including supporting the implementation of DNSSEC, lowering DNS abuse, providing more secure TLD operations, and improving DNS resilience to attacks. However, nothing in the Affirmation of Commitment nor ICANN's by-laws mandates the DNS-CERT initiative, and it is not necessarily a natural conclusion that the initiative is an essential undertaking for ICANN to fulfill its obligations. In fact, we would argue that it is outside of ICANN's core functions and would contribute to so-called "mission-creep." We question whether the community wishes to be responsible for funding initiatives which are outside of ICANN's mandate.

Future discussions on a global DNS-CERT must involve active engagement of all stakeholders in order to ensure a cross-functional solution. We look forward to contributing to future consultations in this dialogue.