

Nominet's Comments on ICANN's Plan for Enhancing Internet Security, Stability and Resiliency (FY11)

Introduction

Nominet is the registry for the .uk country code top-level domain. With nearly nine million registered domains, we are the second largest country-code top-level domain.

Nominet welcomes the opportunity to comment on ICANN's Plan for Enhancing Internet Security, Stability and Resiliency for 2011. We provided input to ICANN's consultation on the Proposed Strategic Initiatives for Improved DNS Security, Stability and Resiliency and the Global DNS-CERT Business Case (<http://forum.icann.org/lists/strat-ini-ssr/msg00006.html>).

General Comments

In his response to the consultation on initiatives to improve DNS security, stability and resilience, Lawrence Stricking, Assistant Secretary for Communications and Information in the US Department of Commerce, stated that ensuring the security, stability and resilience of the Internet is a shared responsibility among all actors in the DNS arena (<http://forum.icann.org/lists/strat-ini-ssr/msg00002.html>). He welcomed the public discussion on these issues, but also suggested that further data gathering and community input was needed.

However, we see little evidence in this document of work to develop this common base for developing initiatives. What work there is appears more focussed outside the DNS industry: there appears to be a real need to do a more complete risk assessment and gap analysis and to assess how best to embed DNS expertise in the existing computer and network security response capability, ensuring best use of existing networks. This should help others understand issues associated with the DNS and help them access sources of expert advice.

We welcome ICANN continuing to develop its capacity-building initiatives by working with other organisations. We recognise the importance of a culture of emergency preparedness in the DNS community and of embedding best practice across the industry. However, we are concerned that many of ICANN's initiatives (eg its engagement with FIRST) do not involve the DNS industry.

Bearing in mind that the summary of comments and analysis on the consultation on strategic initiatives was produced in May, it is disappointing that the 2011 Plan, produced in September, does not take this input into account: it is little more than a minor update from the May 2009 Plan.

We note that there are few dates against deliverables.

DNS-CERT

There is still significant emphasis on the creation of a DNS-CERT, without any clear justification for this. While we welcome the clear statement in the Plan that it is not in ICANN's remit to operate it, we believe that it is important to be quite clear about how such a capability would fit in with other initiatives. In particular, care will be needed to avoid an international response capability substituting for the development of local capacity, rather than encouraging it.

It should be noted that many ccTLDs already provide a national DNS-CERT-like capability and are well networked with other operators in their local infrastructure. It is unfortunate that ICANN has not held any direct consultation with ccTLDs to identify the nature of their engagement and to see whether there are examples of best practice that could inform future decisions.

The regional ccTLD associations are involved in some capacity building, resource sharing and information dissemination exercises: it is good to see some firm commitments to working with them and would welcome more information about some of the joint initiatives included in the Plan.

The creation of the new Joint Security and Stability Analysis Charter Drafting Working Group (with involvement from ALAC, ccNSO, GAC, GNSO and NRO) is greatly welcomed. This working group should feature in the Plan, bearing in mind that its creation was proposed in the joint letter from the Chairs of the GNSO, ccNSO and ALAC dated 25 March and referred to in a number of submissions in response to the consultation on the proposed strategic initiatives.

It is, of course, useful for ICANN to develop its relationship with FIRST. However, this will not give a full picture of what is happening in the industry: ccTLDs and not formally designated as CERTs and are not members of FIRST: simply talking to the CERT community will not give a clear picture of local capacity and gaps.

Detail

Although we are active members of the ccNSO, we were not aware of the ccNSO's involvement in the Attack & Contingency Response Planning or the Registry Operations Course. More detail of what has been achieved and what future work is planned would be useful.

Address space management: there is no discussion about the management of IPv4 exhaustion and any security, stability and resilience implications associated with this. It might be useful to programme some cooperative work with the NRO to assess the risks.

The implementation of e-IANA is mentioned on page 39, but is not then picked up in the deliverables on page 53. This has been a long-delayed implementation, with no explanation as to why the initiative has been delayed and no indication of likely timescales.

It would be useful for the Plan to mark clearly those activities from the 2009 Plan that have been completed. It would also be helpful to be clearer about success metrics in the Plan: it is hard to assess the utility of some of the activities.

A handwritten signature in black ink, appearing to be 'Martin Boyle', with a stylized, sweeping flourish extending to the right.

Martin Boyle
Senior Policy Advisor
Nominet

3 November 2010