ICANN Consultation on
Proposed Strategic Initiatives for Improved DNS Security, Stability and Resiliency
and the Global DNS-CERT Business Case

Response from Nominet

Introduction

Nominet is the registry for the .uk country code top-level domain. With over eight million registered domains, we are the third largest country-code top-level domain. Nominet is a long-standing and active participant in ICANN and in ICANN's country code Names Supporting Organisation.

We welcome the opportunity to contribute to ICANN's consultation on initiatives for Improved Security, Stability and Resiliency. This input also responds to the consultation on the Global DNS-CERT Business Case.

We support the contributions put in to the consultations by CENTR and by the ccNSO.

Initiatives for Improved DNS Security, Stability and Resiliency

We generally welcome and support ICANN's strategic focus on DNS security and stability. We recognise the importance of this work – highlighted by the Affirmation of Commitment as one of the key areas.

"ICANN … is a … **partnership** of people … dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers" (www.icann.org/en/participate/what-icann-do.html, emphasis added). In this framework, we strongly support the concept of ICANN working with others to ensure effective planning and response to threats confronting the DNS.

The contribution from Assistant Secretary Strickling (US Department of Commerce, NTIA) (http://forum.icann.org/lists/strat-ini-ssr/pdfpdEZkwJSTg.pdf) underlines the importance of working together: "Preserving the stability and security of the Internet DNS is a shared responsibility among all actors in the DNS arena". (We also note and agree with the NTIA statement that the AoC does not mandate these particular initiatives: the security and stability of the DNS depends on broad-based, active engagement of all the parties involved in the operation of the DNS – and in the wider Internet infrastructure.)

Action needs to be in **cooperation** with other relevant organisations. It should aim to improve overall planning, coordination, and effectiveness of response. This should be in partnership with other operators of Internet infrastructure as well as those directly involved in the DNS, and could also usefully be extend to working in partnership with others active in communications and computer network security. In this way we should be able to ensure effective channels to infrastructure operators, major users and security solution providers.

Accordingly, we believe that, before any decisions are made on initiatives for improving DNS security, stability and resilience, more work needs to be done to engage with the various groups and organisations already involved in this work to assess how to avoid duplication of effort and how best to get value from cooperation. In particular, this could: look to where there are gaps in coverage;

focus on how to improve capacity building and access to specialist advice and support; and help to extend effective communications using and developing existing channels.

Initiative 1: System-wide DNS Risk Analysis, Contingency Planning and Exercises
(www.icann.org/en/topics/ssr/strategic-ssr-initiatives-09feb10-en.pdf - Proposed Initiatives for Improved DNS Security, Stability and Resiliency section 5.1)

We welcome this approach in principle. Collaboration should be wider than the "DNS community" (5.1.1), working with the wider technical community and security experts to ensure an holistic approach. This should help others understand issues associated with the DNS and help them access sources of expert advice.

Fundamental in this approach should be to embed DNS expertise (primarily by developing good contacts with local sources of advice) in the existing computer and network security response capability, ensuring best use of their existing networks. This will draw on CERTs' links to the wider community dependent on the good functioning of the Internet and should improve the understanding of specific DNS-related risks. In particular, it should allow and encourage the development of local expertise backed by international support.

In this way, the ideas identified in this initiative would more clearly be about working in partnership and cooperation with other initiatives (including those identified in paragraph 5.1.3 of the paper), not in competition with them.

The paper gives no clear idea about how the new expert advisory/working group will relate to existing ICANN advisory committees (both SSAC and RSSAC) or with expertise in the different ICANN communities: care is needed to avoid making it difficult to understand where expertise and responsibility lie.

The various initiatives identified in paragraph 5.1.1 could usefully be carried out in cooperation with other organisations with a well-embedded continuity planning and exercises capability and addressing a wider community than just the ICANN community. However, they do need to be developed with the support of the many experts, initiatives and organisations already active in ensuring the security, stability and resilience of the DNS.

Initiative 2: DNS-CERT
(www.icann.org/en/topics/ssr/strategic-ssr-initiatives-09feb10-en.pdf - Proposed Initiatives for Improved DNS Security, Stability and Resiliency section 5.2 and www.icann.org/en/topics/ssr/dns-cert-business-case-10feb10-en.pdf - Global DNS-CERT Business Case: Improving the Security, Stability and Resiliency of the DNS)

We fully agree with the importance of improving the industry's capacity to respond to attacks, threats and vulnerabilities. However, we do also have serious concerns over the way this initiative appears to be being presented. As a top-down initiative it:

i. Does not seem to have good community support and appears to be an initiative in competition, rather than in partnership, with other initiatives addressed at improving the security, stability and resilience of not just the DNS, but of computer and communications networks in general;

ii. Appears to put the DNS into a "silo", rather than seeking to embed it in (and therefore benefit from) other computer emergency response work; and

iii. Focuses on establishing operational and organisationally heavy structures (points of contact, geographical coverage) at the expense of improving handling and communications strategies.

We do accept that ICANN can – and should – have a major role in helping to underpin the security of the DNS. In particular, we understand the need to improve awareness and capacity among smaller operators, which might have more limited resources available for responding to DNS attacks. However, we would like to see effort focussed on ensuring capacity building – in the industry and among existing CERTS more generally – rather than in building new organisational capacity.

Recommendations

We would suggest that:

i. In the first instance, ICANN should focus on identifying work that could be addressed under the initiative on System-wide DNS Risk Analysis, Contingency Planning and Exercises, subject to the comments made above and working with other related initiatives. This should be in partnership with the many organisations already active in ensuring the security, stability and resilience of the DNS. As such, we strongly support the ccNSO proposal for a joint SO/AC working group to draw on this expertise.

ii. Work should also look at building and developing contacts between organisations active in the operation of the DNS and emergency response teams (FIRST and key CERTs and CSIRTs) to ensure that they have embedded knowledge about the operation of, and attacks on, the DNS, and up-to-date contacts within the industry. This could perhaps be achieved by widening membership of a joint SO/AC working group;

iii. In particular, effort needs to be put in to developing industry best practice guidelines and encouraging TLD operators and registrars to be involved and active in local CERTs, raising awareness of DNS issues in the CERTs and improving their own understanding of security response procedures. We also recognise the need to raise the level of competence of all players to make it easier and more useful for partners to share information. In particular, there probably does need to be improved contact information available to enable rapid information exchange, something easier to ensure at local (regional or national) level;

iv. We recognise that some operators will need assistance to develop their resources and that national capacity might be weak. However, it will be more important to encourage the development of national capacity to respond to incidents, than to seek to substitute for it without embedding skills in the country;

v. Should this work reveal that a stand-alone DNS CERT is needed, this would then naturally lead to an industry bottom-up initiative drawing on an identified demand. A resulting CERT would then be seen as part of the DNS landscape and accepted more readily by other CERTs and their partners.

Martin Boyle
Senior Policy Advisor
Nominet
14 April 2010