Addressing the global Internet

ICANN

Sent via e-mail:
cheryl@hovtek.com.au
ceo@auda.org.au
cgomes@verisign.com

Rod Beckstrom
CEO and President

August 11, 2010

Ms. Cheryl Langdon-Orr, Chair, ALAC
Mr. Chris Disspain, Chair, ccNSO
Mr. Chuck Gomes, Chair, GNSO

Dear Cheryl, Chris and Chuck,

Thank you for your April 30 letter seeking clarification on key issues relating to ICANN's proposal to establish a DNS-CERT. We appreciate your continued engagement and the ICANN community's ongoing commitment to a more secure, stable and resilient DNS. We have taken some time to respond to your letter to allow Greg Rattray, our Chief Information Security Officer, to work with you in public meetings and conversations. Now that you are developing a draft charter, it seems an appropriate time to share our views.

Issuance of the Strategic Initiatives paper and global DNS-CERT business case in February and our continued efforts since then are intended to promote community engagement on projects in the 2010-2013 ICANN Strategic Plan. The DNS-CERT concept was among the top six of more than 20 priorities in all prioritization votes on the three Strategic Plans, starting with the public session at the Seoul meeting. Staff papers following informal discussions with the community were posted for public comment and are available at: http://www.icann.org/en/topics/ssr/strategic-ssr-initiatives-09feb10-en.pdf.

The DNS-CERT has been the subject of much debate over the past twelve months, generating a broad range of perspectives and substantial interest and debate. It was driven, in significant part, by our experience with ccTLD operators in capacity building sessions, and our collaborative efforts to combat the spread of the Conficker worm. That experience indicated a strong demand for a well-resourced source of assistance on DNS-related security incidents.

More than 10,000 references to a DNS-CERT can be found online: (http://www.google.com/#hl=en&client=hp&q=%22dns+cert%22&aq=f&aqi=g1&aql=&oq=&gs_rfai=&pbx=1&fp=ec903f46ceabe964). Furthermore, the Canadian Internet Registration Authority "recommends the Government of Canada enhance its ability to respond to emergencies... through a DNS-CERT" (http://www.cira.ca/2010-IC-consultation/). Paul Vixie, CEO of the Internet Systems Consortium, published a widely read blog piece entitled "Towards a DNS-CERT Definition" (http://www.isc.org/community/blog/201006/towards-dnscert-definition). Many other opinions and calls for action have been published.

Against this background, your organization's willingness to take on this considerable challenge is welcome, and we do not underestimate the importance of this undertaking. The community voted during the Strategic Planning process to "establish a DNS-CERT." This raises many questions: how, where and with what funding? What will its functions be? What is ICANN's role as the global coordinator of the DNS? What role for the community? For private operators? Should there be a new non-profit foundation or organization, or both, to help build a DNS-CERT? What questions should be asked to define the problem and to shape a solution that can be implemented successfully?

This is a challenge and an opportunity.

Given continuing threats by malicious actors across the cybersecurity spectrum, it is important to develop a solution quickly and to find appropriate financial support. As Paul Vixie noted in another blog posting, "Perspectives on a DNS-CERT," in 2002 the industry recognized the need for a 24/7 monitoring and response function, yet it has not happened. As a result, for the past eight years the DNS - the core of the Internet - has not been as secure as it could have been.

Some have incorrectly stated that ICANN plans to operate a DNS-CERT, and that it is funded in the FY11 budget. Neither is true. The community voted for the establishment of a DNS-CERT in the Strategic Plan, but it was not put into the Operating Plan because we were waiting for community feedback on how best to implement it.

As the only organization with responsibility for the security and stability of the DNS, a role for ICANN seems logical, but that role must be defined. A majority of the community does not support ICANN assuming an operational role in a DNS-CERT, although the term "operational" also needs to be defined in this context. Moreover, what other group or body would take on this responsibility, on what basis and with what community review?

Accordingly, we see establishment of Joint Supporting Organizations and an Advisory Committee working group as a positive development. We look forward to creation of the working group's charter, work plan and schedule, and we welcome the opportunity to engage with the working group on this, in addition to providing staff expertise and support.

To ensure the working group's efforts are integrated into relevant ICANN activities, we invite the group to lead public consultations on the DNS-CERT concept at the Cartagena Meeting. We also request that your Supporting Organizations and Advisory Committee deliver formal written analysis and recommendations for community consideration one month prior to the March, 2011, North American meeting.

This approach will enable the ICANN Board and community to discuss your recommendations, and consider whether they represent a viable, functional and affordable solution. If they do, the Board can consider, as a part of the solution, allocating appropriate ICANN support and resources through the normal planning and budgeting process. If not, other alternatives will need to be considered to implement the community's strategic decision.

For your information, the ICANN staff is working with the CERT Coordination Center (CERT/CC; http://cert.org/) and the European Network and Information Security Agency (ENISA; http://www.enisa.europa.eu/) on a survey of national CERTs regarding their interactions with ccTLDs on DNS security. ICANN is also participating in the IT Sector Coordinating Council's (IT SCC; http://www.it-scc.org/) DNS Risk Mitigation Strategy, which is looking at DNS risks and potential mitigation measures.

ICANN has also proposed a system-wide DNS Risk Assessment as part of its Strategic Initiatives.

In relation to the DNS-CERT Operational Requirements and Collaboration Analysis Workshop on April 6-7, ICANN's security staff selected experts in DNS security response and focused on ensuring representation from a full range of the stakeholders that would interact with a DNS-CERT. These were chosen in response to community feedback and to ensure a deeper understanding of the mission and its requirements. We also sought participation from organizations,such as DNS OARC and RISG, that conduct activities in this area and would be likely collaborators with the DNS-CERT. A summary of the workshop, including a list of the participants, is available at http://www.icann.org/en/topics/ssr/dns-cert-collaboration-analysis-24may10-en.pdf.

The ICANN community can and should work together to come to grips with the growing security challenges that threaten the security and stability of the global Internet. The community will succeed in meeting this challenge only through collaboration. On behalf of the ICANN staff, we look forward to working with you on this important proposal.

Sincerely,

Rod Beckstrom

Rod Beckstrom