at&t

AT&T Comments on ICANN’s Proposed Global DNS-CERT Business Case and Proposed Initiatives for Improved DNS Security, Stability and Resiliency April 14, 2010

AT&T respectfully submits these comments in response to ICANN’s proposed Global DNS-CERT Business Case and Proposed Initiatives for Improved DNS Security, Stability and Resiliency. We support ICANN’s increased focus on security, stability and resiliency issues, and we welcome the opportunity to comment on the proposed initiatives. AT&T’s comments highlight some fundamental considerations for ICANN as it engages with the broader community on these important issues.

As it considers potential initiatives for improved DNS security, stability and resiliency, ICANN should take a forward-looking approach which reflects the reality that threats to the DNS – and the Internet generally – continue to expand and evolve. Not only are there many different types of security threats, but DNS security is just one component of the larger issue of Internet security. This broader perspective will help ICANN to develop initiatives that reflect its important, but defined, role within the global Internet ecosystem.

AT&T supports the development of proactive initiatives to enhance DNS security and stability, with input and inclusion from all appropriate Internet stakeholders. A good starting point would be to build on ICANN’s longstanding Security and Stability Advisory Committee (“SSAC”) and the recently established Risk Committee. The perspective of these committees can be enhanced by including representation from a broader set of stakeholders, since the overall risks to the DNS cannot be assessed by examining only the DNS infrastructure. Moreover, broader community input is needed in order to ensure that the full impact of any security and stability initiatives on Internet services and users is taken into account.

AT&T has some concerns about ICANN’s proposal for a DNS-CERT. While improving the security, stability, and resiliency of the DNS is certainly a worthy objective, the ICANN proposal as written would appear to move the organization somewhat away from the fundamental purpose for which ICANN was created – namely to coordinate the various activities and components that comprise the DNS. Further, the proposal appears to put ICANN in a potentially conflicting or overlapping position with other entities involved in the technical design and operations management of the DNS and the global Internet, including the IETF, root server operators, domain name registrars and service providers, such as AT&T, who operate the access and transport facilities that link the DNS together. ICANN should develop an approach that complements and builds on the existing roles, responsibilities, and capabilities of these other stakeholders.

The ICANN proposal correctly points out that response to cyber incidents tends to be ad hoc. It is not clear, however, that the establishment of an ICANN DNS-CERT would help to provide a more structured or effective response. Most developed nations already have some sort of CERT and efforts are underway via bilateral, multi-lateral, and regional discussions to link these established CERTs together to improve coordination and response.

Moreover, many voluntary groups have formed to analyze and respond to cyber attacks. These groups have been effective means of assembling a broad cross-section of Internet stakeholders to work cooperatively on security issues. As just one example, the Conficker Working Group was assembled to deal with a specific, but persistent and evolving, security threat. In addition, tier one Internet Service Providers ("ISPs") have developed the capability to monitor traffic flows and security alarms within their network infrastructure to provide a real-time picture of malicious cyber activity, including those focused against the DNS. Rather than create yet another CERT, it would be more effective for ICANN to focus on how it can better leverage the existing capabilities across the broad range of global Internet stakeholders to identify and remediate threats to the DNS. This should be a priority task for the SSAC, with broader participation from other Internet stakeholders such as ISPs.

AT&T looks forward to working with ICANN and the Internet community on the important issues related to safeguarding and enhancing the security, stability and resiliency of the DNS.