PayPal™

Information Risk Management
SAN JOSE OFFICE

April 14, 2010

To: Mr. Peter Dengate-Thrush
Chairman of the Board of Directors, ICANN

Mr. Rod Beckstrom
CEO and President, ICANN

Dear Peter and Rod,

PayPal welcomes the opportunity to provide comments on ICANN's Proposed Initiatives for Improved DNS Security, Stability and Resiliency and Global DNS-CERT Business Case: Improving the Security, Stability and Resiliency of the DNS . Our business, like many others, relies heavily on the Internet, its continued availability, reliability, and security and we wholeheartedly endorse activities that promote the same.

The "Proposed Initiatives" document proposes an extension of ICANN's role beyond what was spelled out in the Plan for Enhancing Internet Security, Stability, and Resiliency. The May 2009 plan does not mention either of the initiatives called for in the paper now under review. It is apparently the activities under the May 2009 plan – not any new additions – that will form the basis for one of the reviews established in the September 2009 Affirmation of Commitments.

The DNS is an integral part of the Internet and as such it is essential that its security, stability, and resiliency are preserved as noted in the recent Affirmation of Commitments. However, nothing in that Affirmation requires that either of the initiatives in the "Proposed Initiatives" proposal be undertaken; establishes a timeline for their implementation; or clearly provides for a review in order to determine that these initiatives are carried out in the public interest or are "consistent with ICANN's limited technical mission."

The "Proposed Initiatives" document sets forth two initiatives. With regard to "System-Wide DNS Risk Analysis, Contingency Planning and Exercises", section 5.1.2.4 Assumptions reads:

> Risk analysis would leverage threat information and analysis from DNS-CERT. Root server information sharing system would leverage Web 2.0 portal developed for DNS CERT to support information sharing.

Given the reliance of the first initiative on the second, it is difficult at best to evaluate on its own merits. We believe that some benefit can be gained by doing system-wide risk analysis and contingency planning provided that it is properly scoped to fall within ICANN's "limited technical mission". However, we are not convinced that the proposal, as presented, is properly scoped.

A simple financial review reveals that projected average staffing costs are 250k USD per person which compares unfavorably with the approximately 175k USD per person cost of the second proposal. No explanation for this discrepancy is provided and the reader is left to assume that the first initiative requires significantly more senior staff than the second. Further there is little or no substantiation for some 850k USD in "support" costs.

The second initiative, spelled out in more detail in the Business Case paper calls for ICANN to establish a DNS-CERT.

Subsequent to the Affirmation of Comments, ICANN adopted a 2010-2013 Strategic Plan whose "DNS Stability and Security" focus area stated that "ICANN will work in partnership with other organizations to develop an approach to the establishment of a DNS Cert". Yet the proposed initiative, besides going beyond the Affirmation of Commitments, also does not track to the Strategic Plan that ICANN recently adopted.

The current proposal's mission for a DNS-CERT is to:

> Ensure DNS operators and supporting organizations have a security coordination center with sufficient expertise and resources to enable timely and efficient response to threats to the security, stability and resiliency of the DNS.

Given the proposal's reliance on the Strategic Plan, one might expect that the mission would read:

> Work in partnership with other organizations to ensure that DNS operators and supporting organizations have sufficient expertise and resources to enable coordinated, timely, and efficient response to threats to the security, stability and resiliency of the DNS

Such a mission would be consistent with the Affirmation, Strategic Plan, ICANN's traditional non-operational role, and would serve to partially answer some of the thoughtful concerns submitted by several organizations[1]. It would also properly limit ICANN to a cooperative role and the DNS CERT's role to one of responding to actual incidents and attacks - emergencies.

While we share the belief that a DNS CERT has merit and deserves consideration, this proposal fails to substantiate either the demand or need for the organization as envisioned. It is unclear who is calling for the creation of the DNS CERT in this form and it is even less clear that either the structure or scope of the organization contemplated is appropriate.

Without suggesting that ten incident managers is an appropriate number, our analysis of the proposed organization and budget finds that administration, management, and travel levels are considerably higher than industry norms and raises questions about the process

[1] ccNSO; US Gov't; ALAC, ccNSO, and GNSO; APTLD; AFNIC; CENTR

used to develop the 4.1mm USD budget. (We suspect there may be math or transcription errors in the 4.2mm USD budget as presented in 4.2.2.1.)

The proposal calls for a budget of 4.2mm USD but offers little to substantiate the need for such a large amount or why staffing, equipment, space, or travel levels are projected at their current levels. Without such information, no prudent business would authorize such expenditure. There simply is no way to determine if 4.2mm USD is the right amount or if it even remotely approximates the magnitude of the amount required to carry out the mission described.

Consequently, we do not support ICANN's formation of a DNS CERT as described in the proposal and suggest that alternatives be seriously considered. We believe that many of the proposed benefits could be obtained through a more fiscally responsible expenditure in this area, for example by ICANN's directly providing limited assistance to existing mechanisms and/or establishing a coordination center. This would potentially free up funds for other activities, such as contract compliance, that would enable a more effective response to clearly established problems including the known deficiencies in Whois Data. This is clearly an ICANN responsibility and one we would like to see it live up to. If it is determined that ICANN should be active in the DNS-CERT area, it could best advance the cause of security, stability, and resiliency by a more fiscally prudent plan that would accommodate increased investment in contract compliance.

As a final comment, the Proposed Initiatives states in 5.1 that "The two initiatives here address critical needs in establishing necessary capabilities for ICANN to meet the security, stability, and resiliency commitments identified earlier. … This paper does not presuppose that ICANN will fund or staff these initiatives." On the one hand the proposal states that these initiatives are "critical", presumably essential, for ICANN to honor its commitments to the community and on the other, that ICANN has no plans to fund them. If both are true, the reader is left to wonder on what basis ICANN signed the Affirmation of Commitments.

We appreciate the opportunity to provide comments on these proposed initiatives and look forward to a continued dialogue on this and other subjects of interest to the Internet community.

Sincerely,

Andy Steingruebl
Manager, Internet Standards and Governance
PayPal Information Risk Management