From: <bmanning@vacation.karoshi.com>
To: <dnssec@ntia.doc.gov>, <aheineman@ntia.doc.gov>
Date: Thu, Nov 20, 2008 9:17 AM
Subject: Comments on Docket Number 0810021307-81308-01

Ms Alexander,

NTIA has requested comments on docket number 0810021307-81308-01 (Enhancing the Security and Stability of the Internet's Domain Name and Addressing System). Attached are my comments. Acknowledgment of receipt would be appreciated.

My comments are based on my history as a root name server operator, DNS and DNSSEC developer and operator of perhaps the longest running persistent DNSSEC test bed.

First, it is important to improve the security and stability of the DNS as a whole, not just a particular delegation. To that end, having a signed root is an necessary but not sufficient condition. Any approach to a signed root must be taken with due care and diligence and without inappropriate hesitation or delay.

To the points raised in the NOI. There seem to be two driving factors, the recently demonstrated attacks and concerns regarding key management. The attacks themselves have been known in the technical community for years and there are now mitigation techniques that do not depend on signed data. These are not a cure or panacea but can address point infection. The concerns about managing large numbers of keys or trust anchors in the intermediate and end systems is of interest but in some forms is a solved problem. The average internet browser has to manage many keys today. A few hundred TLD keys should not be a problem.

It is my opinion that the problems are important but not urgent. This is crucial in considering ways forward. Considering the two proposals submitted, both focus on the specific parts of the DNS path between the TLDs and the root, accepting crypto information from the TLDs and signing the root zone. Technically, these operations are now well known and understood - there are no credible technical reasons to delay -if- these were the only considerations for the security and stability of the DNS as a whole. From a strictly pragmatic point of view, NTIA has two contractors who have proposals on how to sign the root zone. One of those contractors has a clearly superior position in deployed capability and depth of operational experience. In my opinion, neither proposal should be accepted at this time.

The missing technical component in each proposal is any method for performing either a scheduled or emergency root key rollover. There are no implementations of RFC 5011. For keyrollover, ICANN has not has a response while Verisign has indicated that they would expect to follow SSL practice and create keys with lifetimes in the range of multiple decades, thus ignoring the problem and pushing its solution out into an unknown, untested future time.

Presuming a comprehensive technical solution could be fielded today, the

comments by J. Scott Marcus point out some of the non-technical ramifications of signing. For a successful deployment, considering the economic and political ramifications of a strategy should carry as much weight as strict technical considerations. With this in mind, I will point out that one of the strengths of the root of the DNS is diffusion of operational and management responsibilities. The option of providing more inputs into the management of the root seems like a opportunity not to be passed over lightly. I could not argue in good faith for assigning the key management tasks to an existing contractor.

In summary, the issues are important but not urgent. There are outstanding, unsolved technical problems in key management and potential opportunities to be more inclusive in the ways key management will be maintained. I posit that we have perhaps a 24-36 month window in which we could work on these issues before proceeding with the signing of the production DNS root. And as the NOI points out, there are several functional test beds where these issues can be worked on before an RFP might be released for signing the root zone.

I would like to see one or more of the test beds tasked with developing and fielding at least one implementation of RFC 5011 before the root is signed and at least one of the test beds tasked with working out operational issues with both MofN and Threshold signing - while in political and economic fora, the USG finds a way to include other parties in DNS root management.

These efforts should feed into an RFP, which should be ready for release sometime around 4a2010, for the production signing of the DNS root.

Regards
Bill Manning

CC: <bmanning@vacation.karoshi.com>, <falexander@ntia.doc.gov>