ARIN
American Registry for Internet Numbers

www.arin.net

November 24, 2008

Fiona Alexander, Associate Administrator
Office of International Affairs
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Room 4701
Washington, DC 20230

Notice of Inquiry "Enhancing the Security and Stability of the Internet's Domain Name and Addressing System" Federal Register Vol 73, No 197, d.d. October 9, 2008

The American Registry for Internet Numbers (ARIN) strongly supports the goal of DNSSEC deployment at the root level by having the root zone signed. ARIN recommends using great care to diligently pursue the necessary technical and procedural mechanisms to accomplish this goal. We appreciate NTIA reaching out to poll the community for their thoughts on DNSSEC and are pleased to respond with our views.

ARIN recognizes that DNSSEC introduces complexities to the current operating environment and therefore strongly recommends retaining as much of the existing functionality as possible to ensure stability and to encourage timely deployment. Introducing additional complexity by transferring operations to another operator or introducing a third party to the existing day-to-day operations would be suboptimal, generating delays in rollout and risking stability with the change to an inexperienced operator. With that in mind, ARIN recommends the Zone Signing Key (ZSK) be held by the entity generating the root zone file, the Root Zone Maintainer (RZM). This would reduce the opportunity for problems or the need to introduce new security procedures by maintaining these operations within the same entity.

ARIN recognizes the issues associated with the Key Signing Key (KSK) such as the generation, use and storage of the key, as well as the selection of the N shared-key recipients are very complex and a major factor in the decision to deploy DNSSEC. ARIN supports the M of N or shared-key framework for generation and use. We recommend that an open process be used to select key stakeholders to be the N shared-key recipients. Further, we recommend that a neutral third party be the secure repository for the KSK, and that this party can be easily, physically reachable by both the RZM and the N shared key holders. ARIN looks forward to working with the community to accomplish this goal.

Regards,

General Dale Meyerrose
Major General, USAF (Ret)
Interim CEO, ARIN

Mark Kosters
CTO, ARIN

3635 Concorde Parkway
Suite 200
Chantilly, VA 20151
Tel: +1.703.227.9840
Fax: +1.703.227.0671