From: Jon Kibler <Jon.Kibler@aset.com>
To: <DNSSEC@ntia.doc.gov>
Date: Sat, Oct 11, 2008 4:25 PM
Subject: Comments Regarding the Deployment of DNSSEC

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Hello,

In my professional opinion, deployment of DNSSEC a year ago would have already been too late. DNSSEC needs immediate deployment. The root zones must be signed, and all top level domain zones (both global and country based) must also be singed. This simply cannot happen fast enough.

The urgency in pushing out DNSSEC deployment cannot be over emphasized. Until DNSSEC is widely deployed, there is simply no basis to being able to trust DNS query results with absolute certainty.

To deploy DNSSEC, the root zones must be first signed, and then must be used as the basis for the signing of the TLDs. Second level domain trust registration services must be supplied by the domain registrars, and this registry would be the basis for trust for all second level domains.

In other words, the root zones must serve as the trust anchors for the TLDs. The TLDs must then serve as the trust anchors for either all second level domains directly, or indirectly by serving as the trust anchor for all domain registrars. If the TLDs serve as the trust anchor for all domain registrars, then the domain registrars would then serve as the trust anchor for all second level domains registered through that registrar.

To encourage the rapid deployment of DNSSEC by domain registrants, DNSSEC trust point services must be considered a standard part of all domain registrars' registration services, and must (repeat, MUST) be provided at no additional cost to the domain registrant.

The schedule for deploying DNSSEC must be expedited!
-- All root zones must be signed by the end of this year (2008).
-- All TLD zones must be signed by the end of Q1, 2009.
-- All TLD zones currently signed, must use the root zones as their trust anchor by the end of Q1, 2009.
-- Likewise, all domain registrars must offer trust anchor services at no additional cost to their domain registrants, and this service must be fully implemented and available by the end of Q1, 2009.
-- The industry goal should be that all domains are signed, and DNSSEC universally deployed by the end of Q2, 2009.

The critical nature of getting DNSSEC deployed "immediately" cannot be over emphasized.

Jon R. Kibler
- --
Jon R. Kibler
Chief Technical Officer
Advanced Systems Engineering Technology, Inc.

Charleston, SC USA
o: 843-849-8214
c: 843-224-2494
s: 843-564-4224
http://www.linkedin.com/in/jonrkibler

My PGP Fingerprint is:
BAA2 1F2C 5543 5D25 4636 A392 515C 5045 CF39 4253

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.8 (Darwin)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org

iEYEARECAAYFAkjxDR0ACgkQUVxQRc85QlPC6wCeKOkowthMWodJftvUC2clH2f3
2EgAn3S7PXUf3uPViRoo+YiSr++PRjc1
=5O9A
-----END PGP SIGNATURE-----