Subject: Business Constituency (BC) comment on Plan for Root Zone KSK Change
Date: Monday, October 5, 2015 at 9:08:15 AM Eastern Daylight Time
From: Steve DelBianco
To: comments-root-ksk-06aug15@icann.org

The BC appreciates the opportunity to comment on this important implementation.

We recognize that ICANN's security team puts much thought and energy to planning and executing its key-signing ceremonies.

The BC noticed that a few considerations by the security team offer the opportunity for greater success of its key-signing ceremonies overall, and the pending critical RZ KSK key rollover specifically.

#1: The current key generation algorithms are based on security technology considered weak by today's standards. We support thought and planning toward moving to RSA/DSA 2048 (or stronger) encryption for both the key-signing key (KSK) and zone-signing key (ZSK), in whatever way ensures the greatest opportunity for maintaining the security, stability and reliability of the Internet.

#2: The BC notes the lack of any measurements during implementation – no metrics, no documented post-mortem. Developing metrics, using NIST SP 800-55 or some other implementation performance framework, will serve the current team, future teams, and the community. Reporting on collected measurements will give visibility to successes and failures, and provide greater transparency overall.

The BC agrees with SSAC (SAC063: https://www.icann.org/en/system/files/files/sac-063-en.pdf) that we should begin to tally DNSSEC misconfigurations, and determine the level of misconfigurations considered acceptable. Metrics also for the Communications Plan will be useful for planning and improving future key-signings, encryption upgrades, and other maintenance having the potential to impact the Internet community at large.

The BC acknowledges that a data collection scheme will require great planning and efficiency, and likely dedicated resources to organize and execute. The BC supports making efforts toward a plan for uniform collection and reporting.

#3: The document does not address an issue that has been raised in the past by SSAC. Namely, that smaller DNS operators may not be aware of the KSK change. This points to the need for word to be spread far and wide, sharing about the risk of their Internet communications being interrupted. The BC recommends a communications program in advance of this change to inform ISP communities around the world.

#4: Among the ICANN planning team, the BC notes that all contributors appear to be from Verisign, NIST, NTIA, and ICANN. The BC encourages the Team to actively solicit and include qualified resources from more than just these four organizations

--
This comment was drafted by Angie Graves, with contributions from Stephen Coates and Steve DelBianco.
It was approved in accord with our charter.