**Richard Lamb**

**From:** Vint Cerf <vint@google.com>
**Sent:** Friday, June 18, 2010 1:38 PM
**To:** Larry Strickling
**Cc:** Doug Maughan; Aneesh Chopra; Andrew Mclaughlin; vivek kundra; Howard A. Schmidt; Rod Beckstrom; Doug Brent; Richard Lamb; Mehmet Akcin; Joe Abley; Steve Crocker; Mark McLaughlin; Philip L Verveer; Alec Ross; pat gallagher; Cita Furlani
**Subject:** DNSSEC Key Generation Action, June 16, 2010

Dear Larry,

I participated in the June 16, 2010 Key Signing Key generation process for the Root Zone of the Internet Domain Name System. As one of the "crypto officers," I was present for the entire period of inaugurating, configuring, and activating the secure key signing devices on the US East coast in an impressively secured facility in Culpeper, Virginia.

First, I want to confirm and express my admiration for the level of professional planning that went into the process. There were on the order of 230 steps required to complete the process and to prepare materials that will be conveyed to the West coast for a similar enabling event. In addition the Zone Signing Key request from VeriSign was processed which will allow them to sign the Root Zone File of the Domain Name System once the entire system is made operational. This takes place after the July 12 activation of the West coast equipment.

Second, I want to draw attention particularly to Richard Lamb, Mehmet Akcin and Joe Abley (among many others) who managed this process from beginning to end. Mehmet was away from home for 5 weeks, in charge of preparing the physical facility for operational use, for example. There were many others deeply involved and my failure to list them explicitly here should be laid to my ignorance and not to any diminished significance of their roles.

Third, I think ICANN Board Member Stephen Crocker (who has also served as Chair of the Security and Stability Advisory Committee for many years) should be recognized for his persistence in advocating and working on the protocols and process by which the DNSSEC mechanism has reached penultimate fruition.

Fourth, I think it is notable that the participants in the DNSSEC operation include a remarkable range of international players of extraordinary talent, dedication, and commitment to the Internet's security and stability. It felt as if a high-tech equivalent of the United Nations was actively engaged. It is also important to note that most of these participants will have active roles on an ongoing basis while others will serve as the "back up of last resort" should the equipment and facilities in the East and West DNSSEC operations rooms become inoperable.

Fifth, I believe this represents a very important milestone in the long effort to increase the security of the Internet. There is still so much to do, but it would be hard to overstate the symbolic and substantive importance of this milestone.

Because the system will go operational after the planned July 12 West Coast activation, this gives ample time to prepare summary reports of the actions taken and the planned operations for the future prior to the ITU Plenipot and the IGF meetings in Vilnius. It seems to me that transparency will be served to have such a summary in hand and that credit should be given to all the parties, including VeriSign, NIST, the USG among others, who have cooperated to achieve this milestone. To those who newly seek to assume responsibility in these areas, these summaries would reinforce the readiness and ability of the existing organizations to carry out these tasks without uncalled for interventions.

This is just a first step into increasing the resistance of the Internet infrastructure to various threats. More secure routing and the accelerated implementation of IPv6 are also high on my agenda, as are much less vulnerable operating systems and  browsers.

I hope you share this sense of accomplishment and take pride in the leadership shown by the main proponents of DNSSEC and its implementation.

Sincerely,

Vint Cerf