From: "Steve Goodbarn" <steve.goodbarn@secure64.com>
To: <DNSSEC@ntia.doc.gov>
Date: Fri, Nov 21, 2008 5:01 PM
Subject: Enhancing the Security and Stability of the Internet's Domain Name and Addressing System

To:
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

From: Steve Goodbarn, on behalf of Secure64 Software Corporation

Thank you for the opportunity to comment on the proposed signing of the DNS root. ["Enhancing the Security and Stability of the Internet's Domain Name and Addressing System" Federal Register (October 9, 2008 (Volume 73, Number 197), Page 59608-59612, docket Number: 0810021307-81308-01)]

Topic 1: The root must be signed as soon as possible

DNSSEC provides an essential trust anchor that enables an order of magnitude improvement in internet security. It is an enabling infrastructure for new applications that further security of the web. It also makes existing applications, for example SSL, fully trustworthy. It will enable web applications, such as those that involve private data like health care records, to be secure and more cost beneficial. DNSSEC is essential to achieving the level of trust required for cloud computing.

The commercial potential of such applications and their positive impact on the world's economy should not be underestimated. In every case where user confidence is enhanced there is an economic benefit. No one wants to travel a highway known for its hijackings.

For this reason many individual country code and generic top level domains have been or will be signing their domains (adopting DNSSEC) in the near future. Signing the root makes the implementation and operation of DNSSEC considerably less complex than having multiple trust anchors. The longer we wait for the root to be signed the more complex and costly things will become.

Topic 2: What are the estimated costs that the various entities may incur to implement DNSSEC?

Deployment of DNSSEC in the root zone does not impose any costs on registrars, registries, registrants, ISPs and users because their adoption of DNSSEC is voluntary. Secure64 has developed a DNSSEC signer that reduces the administrative and training complexity and cost to operate DNSSEC to a trivial level in comparison to operating DNS servers without DNSSEC. An open source DNSSEC signer is expected within a year. With these tools there are simply no administrative or cost barriers of any consequence to implementing DNSSEC. Signing the root will encourage competition from other commercial and open source developers that will further reduce costs and complexity.

To summarize, signing the root as soon as possible will bring many benefits to internet users and will avoid needless waste resulting from having numerous trust anchors. There are no significant costs or technical barriers to widespread adoption of DNSSEC.

Sincerely,

Steven R. Goodbarn, CEO
Secure64 Software Corp
5600 South Quebec Street, Suite 320D
Greenwood Village, CO 80111-2228

DISCLOSURE: Steve Goodbarn is the CEO of Secure64 Software Corporation, a commercial enterprise which has developed and markets a DNSSEC signer that was developed with partial funding from the US Government.