



5 September 2008

Hon. Carlos M. Gutierrez, Secretary of Commerce  
U.S. Department of Commerce  
1401 Constitution Ave., NW  
Washington, DC 20230

Dear Secretary Gutierrez:

We write to you, on behalf of the Public Interest Registry (PIR), regarding an extraordinary matter of protection against threats to the security and stability of the Internet and the integrity of data in the Domain Name System.

We urge you to take the steps necessary to authorize the application of a digital signature to the root of the Internet. This single step by the United States Department of Commerce will enable domain name holders (now numbering in excess of 150 million worldwide) to implement the protocols known as Domain Name System Security Extensions (DNSSEC).

The Public Interest Registry, the not-for-profit corporation that manages the .ORG registry, is responsible for over 7 million registrants in the .ORG domain. PIR is dedicated to providing an open, responsible, and truly global approach for the .ORG community. PIR was created by the Internet Society (ISOC), a professional membership society that provides leadership in addressing issues that confront the future of the Internet. ISOC is the organizational home for the groups responsible for Internet infrastructure standards. Together PIR and ISOC are working to promote the continued growth and development of the Internet.

Attacks on the security of the Internet have been much in the news lately, and there is an increased urgency to take the technical steps to combat these attacks. The .ORG registry is the first generic top level domain authorized by ICANN to implement DNSSEC, and .ORG has undertaken a process to implement it. Using DNSSEC, domain name holders can protect the integrity of data in the Domain Name System by digitally signing their domains. In order to make DNSSEC effective, there is one additional step that is needed - "signing the root". If a digital signature is applied to the root of the Domain Name System, end-to-end assurance of the data is possible. Without a signature on the root, it is impossible to assure the validity of any of the other signatures in the system.

.ORG believes that the time has come to separate the technical matter of signing the root from any political issues that may exist regarding control of the content of the root zone file and the nature of the Department of Commerce's oversight of the Internet Corporation for Assigned Names and Numbers (ICANN).

There is at this time an urgent need to deal with threats to the security and stability of the Internet. The so-called "Kaminsky attack" is very dangerous; it is an attack against the integrity of the DNS data itself. The best chance to fight against this kind of attacks is the implementation of DNSSEC. The danger that is presented by the "Kaminsky attack" and similar variants against the content of the DNS-cache is



undetectable by the user. DNSSEC makes sure that this kind of brute force attack as well as some other untraceable man-in-the-middle attacks and the whole range of phishing schemes based on them do not have a chance of success.

Before this kind of attack, an Internet user would be at risk if he or she clicked on a link with a URL that was cleverly crafted to be similar to a legitimate web site. The user would then be directed to a phony web-site. Now, after a Kaminsky attack, by contrast, a user could do everything right, typing in an exactly correct bank URL, but still wind up handing the user's life savings to a cyber-criminal. These attacks take advantage of a systemic vulnerability in the Internet protocol itself, which cannot be changed without a change to the protocol. All other proposals on the table, and the ones implemented during the last weeks when the attack was known but not made public, only make it harder for the attack to succeed. These proposals make an attack take much longer in order to be successful, but they don't make it impossible.

DNSSEC is the change in protocol that is really needed. The technology is available to us, but it has to have widespread implementation and adoption. Using DNSSEC, domain name holders can protect the integrity of their domain-data in the Domain Name System by digitally signing their domains. But, in order to make DNSSEC effective, there is one additional step that is needed, namely, "signing the root". If a digital signature is applied to the root of the Domain Name System, the top level domains could sign their zones and make the keys available via the signed root zone. When this chain of signed trust exists unbroken from top to the domain holder's zone, it is easy to use DNSSEC. Without a signature on the root, it is much more complicated and needs additional methods and measures, like setting up and configuring a central repository of keys to assure the validity of any of the other signatures in the system.

The near unanimous opinions of the best technical minds working in the field of Internet security are that the technical solution, signing the root now and a quick deployment of DNSSEC, is a fundamental next step in improving the security of the Internet, and it is readily available.

We appreciate your consideration of our views and ask that you direct the Department and accelerate the process needed to sign the root.

Respectfully Submitted,  
PUBLIC INTEREST REGISTRY

**/s/ Alexa A.S. Raad**  
President and CEO

cc: Meredith Baxter, Acting Assistant Secretary for Communications and Information, NTIA  
Paul Twomey, CEO, ICANN  
Paul Levins, Executive Officer and Vice President - Corporate Affairs, ICANN  
Kurt Pritz, Senior Vice President, Services, ICANN  
Doug Brent, COO, ICANN  
David Conrad, Vice President of Research and IANA Strategy