Packet Clearing House
572B Ruger Street, Box 29920
The Presidio of San Francisco
San Francisco, California
94129-0920 USA
+1 415 831 3100 main
+1 415 831 3101 fax

Meredith Attwell Baker
Acting Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W., Room 4701
Washington, DC 20230
USA

Monday, November 24, 2008

Re: Docket Number: 0810021307-81308-01
Enhancing the Security and Stability of the Domain Name and Addressing System

Mrs. Baker:

As the DNS server infrastructure operator for one of the publicly-signed TLDs, one of the testbed signed roots, three of the other major signed TLD trials, and more than fourteen million authoritative TLD resource records, PCH respectfully submits the following response to the NTIA's public inquiry.

We believe that a DNSSEC signed root is an immediate imperative. Increasingly sophisticated DNS data integrity attacks have made DNSSEC essential to the continued security and stability of the Internet. Signature of the root is unfortunately prerequisite to effective protection for the rest of the DNS hierarchy, and thus PCH has continuously supported the Internet community's public requests for DNSSEC signing of the root which have come with increasing frequency and urgency over the past few years.

Furthermore, we believe that the only responsible implementations of a root-signing scheme are those which adhere rigorously to established security best-practices. This rules out any scheme involving inter-organizational transfer of keys, and rules out any scheme that places responsibility for applying signatures in different hands than the knowledge of the veracity of the data to which the signature is being applied. These are insupportable political half-measures that endanger the safety and security of all the world's Internet users.

> *In terms of addressing cache poisoning and similar attacks on the DNS, are there alternatives to DNSSEC that should be considered prior to or in conjunction with consideration of signing the root?*

No. Over the past fifteen years, countless alternatives have been explored in detail, and the Internet technical community has converged on DNSSEC as the best and only standardized solution to protect the integrity of DNS data. The time for experimentation was more than a decade ago. Now is the time for implementation.

What are the advantages and/or disadvantages of DNSSEC relative to other possible security measures that may be available?

DNSSEC is the only appropriate solution to the problem of DNS data integrity. It solves the entire class of both security and accidentally-introduced problems. It's standardized, and there are many available implementations, both commercial and open-source. The security model it implements has been published and scrutinized and subjected to several generations of improvement and refinement. None of these qualities are true of any alternative technologies.

What factors impede widespread deployment of DNSSEC?

The fact that the root remains unsigned means that, regardless of how diligent security professionals may be in attempting to protect the zones they're responsible for, their efforts can have no effect. The root must be signed to achieve any meaningful protection for domain holders and Internet users.

What end user education may be required to ensure that end users possess the ability to utilize and benefit from DNSSEC?

Anything that depends upon action by, or education of, individual end users will never reach fruition. Instead, it's critical that operating system and application software vendors come together within the context of the IETF, and standardize the behavior of their software in the presence of inauthentic DNS data. Uniform application behavior will allow end-users to operate in an informed manner.

What is a viable time frame for implementation at the root zone level?

The existing ICANN test-bed has proven the technical viability of their approach over the past year and a half. It's likely that the security processes could be made ready for external security audit in a matter of a couple of weeks, and the signed root zone could be made available to the full Internet-using public in January of 2009.

What are the risks and/or benefits of implementing DNSSEC at the root zone level?

There are no significant risks of implementing signatures in the root zone. The slight increase in the complexity of the IANA's task, could be much more than made up for by a simplification of the remainder of the process, which is presently needlessly baroque, fragile, and vulnerable to attack. DNSSEC signature data is transparent to legacy DNS implementations, so it poses no risk to those who choose not to implement or use it.

The risk of failing to sign the root, on the other hand, is the certain continued increase in virtually undetectable DNS data integrity attacks, which will further erode and ultimately destroy public confidence in the Internet, and render it too risky for the online commerce and banking that have become commonplace drivers of economic growth.

Is additional testing necessary to assure that deployment of DNSSEC at the root will not adversely impact the security and stability of the DNS?

No. The existing ICANN implementation has been thoroughly tested over the past eighteen months, and as soon as its operational practices have undergone a thorough external security review it should be ready for production use.

What entities (e.g., root server operators, registrars, registries, TLD operators, ISPs, end users) should be involved in such testing?

Each of the above constituencies have participated in the many preexisting testbeds. Everyone is ready for progress.

How would implementation of DNSSEC at the root zone impact DNSSEC deployment throughout the DNS hierarchy?

It would make it possible.

How would the different entities (e.g., root operators, registrars, registries, registrants, ISPs, software vendors, end users) be affected by deployment of DNSSEC at the root level?

Root server operators are unaffected by this change, since their function is at a different level. The content of the root zone is transparent to the function of the root server operators. Each of the other mentioned constituents is either enabled to provide more secure and trustworthy services, or is the beneficiary of such services.

Are these different entities prepared for DNSSEC at the root zone level and /or are each considering deployment in their respective zones?

Yes. Most who are aware of the issues are either awaiting root zone signature so that they may proceed in protecting themselves and their customers, or are proceeding on the assumption that the root zone will be signed soon. End users have no active role to take, but will benefit as deployment progresses.

What are the estimated costs that various entities may incur to implement DNSSEC? In particular, what are the estimated costs for those entities that would be involved in deployment of DNSSEC at the root zone level?

We've signed quite a few zones, and incurred very little cost. Typically a couple of days of work for one or two people, including testing. However, the root is more sensitive than TLDs, and will be subjected to far more vigorous attack. ICANN has already expended considerable effort on their root zone signature implementation, to good effect. We would like to see the benefit of that investment made available to the Internet-using public.

Of the six process flow models or others not presented, which provides the greatest benefits with the fewest risks for signing the root and why? Specifically, how should key management (public and private key sets) be distributed and why? What other factors related to key management (e.g., key roll over, security, key signing) need to be considered and how best should they be approached?

Of the six models presented, only model four comes near an acceptable level of security best-practices compliance. From an operational-reliability standpoint, the extraneous feature of the separate Root Zone Distributor should be eliminated. As long as all DNSSEC key operations are contained within the IANA function operator, there can be no further threat to the integrity of the root zone data, but the artificial extra step of sending data out to a separate Root Zone Operator before it's published to the rest of the root server operators is an unfortunate and unproductive added single-point-of-failure which should be eliminated for the stability of the system.

Any responsibly-designed system will keep all routine key operations within a closely-bounded security regime, which does not span multiple organizations, multiple locations, or multiple areas

of administrative responsibility. It should be transparent, accountable, publicly scrutinized, and expertly audited. But ultimately, stewardship of the Zone Signing Keys and the use of the Key Signing Keys to create new Zone Signing Keys is technical plumbing. The only significant matter of policy associated with this entire issue is the method by which Key Signing Keys are invalidated or rolled over. Since there will necessarily be a very small number of KSKs, the rollover of a KSK depletes a scarce resource. Invalidation of a KSK should require the joint agreement of the IANA operator, the governmental overseer, and the IAB.

> *We invite comment with respect to what technical capabilities and facilities or other attributes are necessary to be a Root Key Operator.*

Two properties are necessary.

First, the Root Key Operator who applies a DNSSEC signature to the root zone must be the selfsame entity that has firsthand knowledge of the veracity of the data to which they are affixing their signature. Only one party has that knowledge, and that is ICANN, by dint of their direct relationship with each and every Top Level Domain administrator.

Second, the Root Key Operator must be verifiably compliant with RFC4641, *DNSSEC Operational Practices*. It is the responsibility of the governmental overseer to ensure that this compliance is achieved and maintained, and that public confidence in the Root Key Operator is upheld by enforcing the transparency and accountability of the Root Key Operator.

> *What specific security considerations for key handling need to be taken into account? What are the best practices, if any, for secure key handling?*

These practices are standardized and defined in RFC4641.

> *Should a multi-signature technique, as represented in the M of N approach discussed in the appendix, be utilized in implementation of DNSSEC at the root zone level?*

As we have suggested above, multiple signatures would hamstring day-to-day operation of the Zone Signing Key and the use of the Key Signing Key to create new Zone Signing Keys. Any such additional complexity would make an otherwise simple system more fragile, and would add no new security.

On the other hand, the invalidation and rollover of the Key Signing Keys is a crucial matter of both policy and technical operation, and has grave global consequences. Any one organization is subject to subversion, but it is extremely unlikely that all three of the relevant bodies, ICANN, the Department of Commerce, and the Internet Architecture Board, could be simultaneously compromised.

Thank you for your time and attention to this urgent and consequential matter,

Ross Stapleton-Gray
Chief Security Officer
Packet Clearing House