November 24, 2008

Fiona Alexander
Associate Administrator, Office of International Affairs
National Telecommunications and Information Administration
Department of Commerce
1401 Constitution Avenue NW, Room 4701
Washington, DC 20230

Re: NTIA Notice of Inquiry requesting comments on the Deployment of DNSSEC
(File Format: Adobe PDF, submitted via electronic mail to DNSSEC@ntia.doc.gov)

Dear Ms. Alexander:

Please include this submission in the collected responses to the NTIA's Notice of Inquiry requesting comments on the Deployment of DNSSEC in the DNS hierarchy and signing of the DNS Root.

Background
Since gaining its first ICANN-accreditation in 2000, The Go Daddy Group ("Go Daddy") has grown to become the world's largest group of domain name Registrars, with more than 6 million customers, and over 32 million domain name registrations under management. In addition to registration services, we also provide our customers with authoritative DNS hosting for over 19 million domain names.

Position Summary
It is Go Daddy's position that any successful implementation of DNSSEC must include signing the DNS root. Doing so should be considered part of a larger, comprehensive implementation that is developed cooperatively by stakeholder groups, and includes end-user education and training for IT professionals. However, many challenges remain unaddressed, including building consensus for a phased implementation timeframe, and a cost analysis of the infrastructure investment required at all levels.

At this time, Go Daddy offers no formal opinion on any of the six proposed Process Flow Models. Each of these models must be thoroughly analyzed in terms of risks, costs, and benefits.

Response to Inquiry Questions

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 signing the root?

We believe that additional non-technical initiatives can have a significant positive impact on the issue of cache poisoning and similar attacks. These include:

- Additional training for DNS server operators on the proper configuration of DNS systems.
- Integrated support from software vendors providing DNS servers, security tools, and web-browsers.
- Education efforts for the entire community of Internet users on general online security and protection.

At present, there is no alternative to DNSSEC that provides equivalent capabilities. In addition to DNSSEC deployment and non-technical education and cooperation efforts, there are discussions ongoing within the Internet Engineering Task Force (IETF) regarding possible enhancements to DNS. Two of these proposed ideas, known as "EDNS PING"[1] and "0x20"[2], could be deployed much faster than DNSSEC and with significantly less burden placed on registrars and other service providers. While neither will eliminate cache-poisoning incidents, they would make conducting such an attack on the DNS more difficult and resource intensive.

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

DNSSEC successfully achieves its specific objective, namely providing an authoritative response to DNS queries. As a result, DNSSEC is an effective countermeasure against cache-poisoning or other spoofing-styled attacks.

Some challenges remain with DNSSEC deployment, however, including:

- DNSSEC is difficult to deploy and represents a significant investment of resources on the part of TLD registry operators, domain name registrars, ISPs, and hosting services.
- Deploying DNSSEC in the absence of a signed root diminishes protection against DNS cache poisoning and similar attacks.
- DNSSEC adds complexity to a system that is intrinsically simple. There is a potential for lack of backward compatibility with some non-DNSSEC systems, which also creates concern.
- While most DNS functions are transparent to most users, the increased complexity of DNSSEC may introduce frequent lookup errors or diminished performance, negatively impacting their overall Internet experience.

What additional steps are required to facilitate broader DNSSEC deployment and use? What end user education may be required to ensure that end users possess the ability to utilize and benefit from DNSSEC?

Once the root is signed, the immediate next step will be the signing of individual TLDs by registry operators. Next, domain name registrars must implement the necessary systems and tools to allow domain name registrants the ability to sign domain name and manage keys. ISPs and hosting providers must implement DNSSEC-capable resolvers, and make these available to their subscribers.

DNSSEC training should be included in all professional training curricula offered by IT software vendors, such as Microsoft, ISC BIND, and others.

To ensure success, DNSSEC deployment will require cooperation from a variety of providers and industries. This will necessitate a comprehensive implementation plan, developed cooperatively by all stakeholder groups, and effectively managed by diverse governing entities, including IETF, ICANN, IGF and NTIA.

Should DNSSEC be implemented at the root zone level? Why or why not? What is a viable timeframe for implementation at the root zone level?

A signed root will expedite the release and adoption of DNSSEC-capable resolvers, and support a wider variety of DNSSEC and key-management tools for service providers and Enterprise IT system administrators. In the absence of a signed root, vulnerabilities to cache poisoning and similar attacks will remain within localized DNSSEC implementations. Additionally, products and tools from software vendors may be delayed in their development and release.

Currently, we are unconvinced that potential risks and benefits have been satisfactorily answered. It is our opinion that a comprehensive analysis be conducted to review the capital and operational expenses involved in implementing and operating DNSSEC at the root level. Additionally, major stakeholders affected by DNSSEC implementation should be surveyed as to their assessment of the demand for DNSSEC services.

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

Any initiative that includes modifications to the operation of the DNS root can present significant risk, and must be undertaken with an understanding of all potentials for disruption. Furthermore, the interaction between legacy systems and a DNSSEC root should be comprehensively tested and fully understood.

Is additional testing necessary to assure the deployment of DNSSEC at the root will not adversely impact the security and stability of the DNS? If so, what type of operational testing should be required, and under what conditions and parameters should such testing occur? What entities (e.g., root server operators, registrars, registries, TLD operators, ISPs, end users) should be involved in such testing?

DNSSEC technology has been extensively tested over a period of years, but several concerns about introducing it into the DNS root must be addressed. To do this, adoption should include defined trial periods, including a roll-back procedure to re-establish the non-DNSSEC root. This will allow service providers and TLD operators to

gauge the effect on system performance, and make any required modifications prior to any global implementation program.

All stakeholder entities should participate in testing, including TLD operators, registrars, and large ISP and Hosting providers. Additionally, vendors of operating systems, web browsers, email servers, and other enterprise software systems should participate in testing.

How would the different entities (e.g., root operators, registrars, registries, registrants, ISPs, software vendors, and users) be affected by deployment of DNSSEC at the root level? Are these different entities prepared for DNSSEC at the root level and/or are each considering deployment in their respective zones?
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?

Some TLD operators have adopted implementation plans to implement DNSSEC within their respective zones. A coordinated DNSSEC adoption plan should recognize the pioneering efforts of these entities, and analyze their experiences to better anticipate potential challenges.

It is noteworthy that the infrastructure investment to successfully test and deploy DNSSEC is not equitably spread amongst entities up and down the DNS chain. As an example, consider that for Go Daddy the implementation of DNSSEC and development of key management tools for registrants could exceed several million dollars. It is not clear if the value perception of DNSSEC in the general community will support offering DNSSEC as a premium service to domain registrants. Similar concerns are likely shared by TLD operators / registries, ISPs, and hosting providers.

Tim Ruiz
Vice President
Corp. Development & Policy
The Go Daddy Group, Inc.

With:
J. Bladel
M. Donahue
G. Kearns
J. Miller
G. Schwimer

1. "EDNS Option for performing a data PING." http://www.ietf.org/internet-drafts/draft-hubert-ulevitch-edns-ping-00.txt
2. "Use of Bit 0x20 in DNS Labels to Improve Transaction Identity." http://tools.ietf.org/html/draft-vixie-dnsext-dns0x20-00