November 24, 2008

Via E-mail

Fiona Alexander
Associate Administrator, Office of International Affairs
National Telecommunication and Information Administration
U.S. Department of Commerce

Re: *Enhancing the Security and Stability of the Internet's Domain Name and Addressing System,* Docket Number: 0810021307–81308–01

Dear Ms. Alexander:

Comcast Corporation hereby submits its comments in response to NTIA's Notice of Inquiry ("NOI") seeking comment on various proposals for the deployment of Domain Name and Addressing System Security Extensions (DNSSEC) at the root zone level. 73 FR 59608 (Oct. 9, 2008).

Comcast Corporation is the leading provider of entertainment, information and communication products and services in the United States. With over 24 million cable customers, over 14 million high-speed Internet customers, and over 5 million Comcast Digital Voice customers, Comcast is principally involved in the development, management, and operation of broadband systems and in the delivery of programming content.

As one of the largest ISPs in America, we believe that DNSSEC is important to all Internet users. The success of the Internet depends upon the ability of users to trust the information that the Internet's DNS infrastructure provides them in their day-to-day use. Without such trust, innovation on the Internet, and commerce and communications conducted over the Internet, would be jeopardized.

Comcast is strongly in favor of the global adoption of DNSSEC, starting with the signing of the root. Until the root is signed, signatures for a Top Level Domain (TLD), such as .net or .com, and signatures in domains like comcast.net, are of limited utility. The first step, therefore, should be to sign the root. In addition, we believe that the organization asked to implement root signing should have international participation, as well as open, transparent rules and procedures. Once the root is edited and signed, we believe that the TLD operators could then move to sign their respective TLDs.

While these activities have been under discussion in the Internet community, Comcast started a DNSSEC technical trial to understand and document the steps that ISPs and other implementers must undertake to implement DNSSEC-capable resolvers widely across large-scale networks. More information regarding this trial is available at http://www.dnssec.comcast.net.

The following is our response to the specific questions that have been posed by NTIA in the NOI.

I. Specific comments on the six NTIA proposals:

We believe that the fourth proposal is the most advantageous proposal from a technical perspective, and we believe with some modifications it would have the immediate and widespread support from the broader Internet community. While the initial implementation for signing the root should be simple and undertaken rapidly, the sixth proposal included the interesting concept of M of N key splitting. We believe that the fourth proposal could be enhanced by specifying such a mechanism, either initially or in the near future. Moreover, since the entities involved in the process could be from various countries and regions around the world, this could increase the international trust in the key signing process. It is also important that the organization(s) selected to perform these DNSSEC-related functions specify the security employed, in order to create confidence in how keys are generated, stored, and distributed.

The advantages of the fourth proposal are that it provides strong security and it is operationally less complex, combing both editing and signing of the root zone. In addition, the fourth proposal appears to offer the shortest time to deployment. (With respect to timing, we have observed that ICANN's signed root zone test bed appears to be more mature than existing alternatives).

Finally, we encourage the NTIA to put in place careful, documented, and transparent oversight in order to build trust in the DNSSEC root signing process.

II. From the Notice of Inquiry, questions on DNSSEC deployment generally:

a. **Question**: 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?

   Response: Some recursive servers have additional protections against cache poisoning that mitigate risks in the short term. However, other than DNSSEC, we are not aware of any similarly strategic and viable solutions to secure the DNS that have wide consensus and support in the Internet community, at the Internet Engineering Task Force (IETF), and in other industry forums.

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

   Response: DNSSEC has been in development for a long time, and there was sufficient Internet community consensus at the IETF to standardize DNSSEC. The technology has reached a point where many potential implementers understand what deployment would entail, various trials have been performed, and several countries and other entities have begun deploying DNSSEC. The remaining area of work is primarily in the development and/or deployment of operational tools for implementers to manage DNSSEC zones and keys.

c. **Question**: What factors impede widespread deployment of DNSSEC?

   Response: The main factor impeding widespread deployment of DNSSEC is the lack of a signed root. Other factors, which are relatively minor in comparison to the lack of a signed root, include the lack of management infrastructure for administering the signing of zones and maintaining zone keys. This is an area of focus in our current technical trial, and we anticipate sharing our experiences with the Internet community.

d. **Question**: 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?

   Response: Large organizations such as enterprises, universities, and Internet Service Providers (ISPs) that have a direct impact on how the Internet is accessed by various types of users need to be leaders in the deployment process. ISPs and other infrastructure providers that operate domain name services should push to deploy DNSSEC-capable resolvers as soon as possible. Other key Internet companies, web portals, and software tools, should become DNSSEC-aware. Operating system (OS) vendors should provide stub resolvers that are DNSSEC-capable. Registrars and Registries should also begin to provide support for and publish signed zones. Finally, tools and processes are needed to address key signature errors.

III. From the Notice of Inquiry, questions concerning signing of the root zone:

a. **Question**: Should DNSSEC be implemented at the root zone level? Why or why not? What is a viable time frame for implementation at the root zone level?

   Response: Yes, DNSSEC should definitely be implemented at the root zone level. This will eliminate the need for all of the trust anchor repositories and other key authentication tools that have been developed or are in development, assuming TLDs begin signing shortly after the root is signed. We believe the root should be signed as soon as feasible, but no later than 2009.

b. **Question**: What are the risks and/or benefits of implementing DNSSEC at the root zone level?

   Response: Implementation of DNSSEC is overwhelmingly positive for all of the reasons cited previously. The main risk to ISPs is in the potential for infrastructure scalability concerns with DNS resolvers, since DNSSEC will require additional processing of DNS lookups. However, this can be solved with both software efficiency improvements and incremental hardware investments. It is also important to note that simply signing the root will not require ISPs to immediately deploy DNSSEC support in their networks, nor will it require domain owners to immediately sign their zones.

c. **Question**: Is additional testing necessary to assure that 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?

   Response: In order to make the Internet secure, every organization has to do its part. Test beds have been used in the past, and several nations and organizations have performed DNSSEC trials and deployments. Clearly, however, there should be a rigorous process to test signing the root prior to public introduction.

d. **Question**: How would implementation of DNSSEC at the root zone impact DNSSEC deployment throughout the DNS hierarchy?

   Response: This should help with the deployment process, as a precedent would be set, encouraging Registries to begin signing the TLDs for which they are authoritative. Also, having a single trust anchor at the root and in each TLD will make it easier for ISPs to support DNSSEC-capable resolvers, as they will not need to check multiple trust anchor repositories. As this will make operating DNSSEC-capable resolvers less burdensome, we expect that it would encourage more ISPs to deploy DNSSEC in their networks.

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

   Response: We believe that many major TLD operators are preparing for

DNSSEC deployment in their zones. However, TLD operators are clearly in the best position to answer this question. As noted above, having a single trust anchor at the root and in each TLD will make it easier for ISPs to support DNSSEC-capable resolvers, as they will not need to check multiple trust anchor repositories. As this will make operating DNSSEC-capable resolvers less burdensome, we expect that it would encourage more ISPs to deploy DNSSEC in their networks.

f. **Question**: 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?

Response: The benefit of securing the Internet's DNS from caching poisoning sorts of attacks, and from a potential loss in trust of critical Internet infrastructure outweighs the modest costs involved in implementing DNSSEC at the root zone level. We believe DNSSEC deployment will benefit our customers, as well as other Internet users.

Respectfully submitted,

Kathryn Zachem
Vice President,
Regulatory & State Legislative Affairs
COMCAST CORPORATION
Suite 500
2001 Pennsylvania Ave.
Washington, DC 20006
(202) 379-7134

Jason Livingood
Executive Director, Internet Systems Engineering
National Engineering & Technical Operations
COMCAST CABLE COMMUNICATIONS
One Comcast Center
Philadelphia, PA 19103