NEUSTAR®
46000 Center Oak Plaza, Sterling, VA, USA 20166 +1 571 434 5400 +1 571 434 5786 www.neustar.biz

November 24, 2008

Ms. Fiona Alexander
Associate Administrator
Office of International Affairs
National Telecommunications and Information Administration
U.S. Department of Commerce
Washington, DC 20230

RE: Docket Number: 0810021307-81308-01
Enhancing the Security and Stability of the Internet's Domain Name and Addressing System

Dear Ms. Alexander,

NeuStar, Inc. ("NeuStar") is pleased to submit the attached response to the National Telecommunications and Information Administration's Notice of Inquiry on Enhancing the Security and Stability of the Internet's Domain Name and Addressing System.

NeuStar provides the North American communications industry with essential clearinghouse services and operates the authoritative directories that manage virtually all telephone area codes and numbers in the region. NeuStar enables the dynamic routing of calls among thousands of competing communications service providers in the United States and Canada. We also provide clearinghouse services to Internet service providers, cable television operators, and voice over Internet protocol (VoIP) service providers.

NeuStar also has several diverse lines of Internet Protocol business, including Internet domains, infrastructure DNS, managed enterprise DNS, ENUM, and other IP-related services. NeuStar currently operates the authoritative registries for the .biz gTLD and .us ccTLD, and provides back-end technical registry services for several other TLDs including .travel, and .tel. NeuStar operates a world-class global DNS network that supports several TLDs and thousands of enterprise customers, including many of the Fortune 500 companies – all customers that demand security and trust in the Domain Name System.

We look forward to further assisting the U.S. Department of Commerce in its deliberations on this important issue impacting the security and stability of the Domain Name System. If there are any questions regarding NeuStar's response, please contact me immediately at (480) 804-8250 or via email at rodney.joffe@neustar.biz.

Sincerely,

Rodney Joffe
Senior Vice President and Senior Technologist
NeuStar, Inc.

NEUSTAR®

NEUSTAR®
46000 Center Oak Plaza, Sterling, VA, USA 20166 +1 571 434 5400 +1 571 434 5786 www.neustar.biz

NeuStar Response to NTIA Notice of Inquiry on DNSSEC

DNSSEC and signing of the Root Zone is currently a high-priority topic of discussion within the Internet community. Following the July 2008 announcement of a critical DNS security vulnerability, urgency surrounding DNSSEC has increased significantly. NeuStar applauds the U.S. Department of Commerce's ongoing consultations with the community to identify the most appropriate and responsible path forward.

- NeuStar supports deployment of DNSSEC at the root zone level and encourages a responsible and expeditious move towards a signed root zone to ensure improved stability and security of the Domain Name System.

- While a signed root zone does not by itself secure the DNS it is an appropriate and necessary step towards bringing increased security to the entire DNS. Signing the root zone will simplify the work of TLDs as well as ISPs in deploying and managing DNSSEC. Signing the root zone will send an important signal to the entire Internet community (registries, registrars, ISPs, hardware manufacturers, software vendors, and Internet consumers) that DNSSEC is coming.

- While DNSSEC at the TLD zone level is technically feasible, without a signed root zone it is a piecemeal solution to a systemic challenge. A collection of signed TLD zones without a signed root zone is neither as efficient nor comprehensive as signed TLD zones operating under a signed root zone.

- Because the process of signing the root zone will take time to implement, NeuStar has developed an interim DNS security solution, but we believe the most effective and efficient response for securing the DNS is the signing of the root zone by a trusted entity or entities.

As a leading DNS provider to TLD and Enterprise customers, NeuStar is committed to ensuring security, stability and trust in the Domain Name System, for this reason taking the steps to deploy DNSSEC is a high/top priority.) Our customers demand the most secure and dependable DNS possible and NeuStar is very active in continually delivering the highest levels of service. NeuStar has a stake in protecting the investment that our customers and their customers have made to date in the DNS. As such, we believe the most appropriate, efficient, and universal solution to mitigate the recently identified DNS vulnerability is to implement DNSSEC at the root zone level. However, we have not been idle while waiting for those complex decisions to be made. Specifically, NeuStar has implemented the following security upgrades:

DNSSEC Support for NeuStar's TLD and Enterprise DNS Customers: By December 1, NeuStar will support DNSSEC for our TLD customers. That is, where we provide primary or secondary DNS to a TLD customer, they will be able to implement TLD-level DNSSEC while utilizing our DNS services. We will support DNSSEC for our second-level TLD and Enterprise customers in 2009.

Cache Defender – NeuStar has developed a proprietary solution to secure our DNS and the DNS of our customers until such time the root zone is signed and DNSSEC is fully implemented, operational, and supported throughout the chain of responsibility (root zone, registries, registrars, ISP, and end user software).

The following is NeuStar's response to the specific questions posed in the Notice of Inquiry:

Questions on DNSSEC Deployment Generally

- *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?*

    - Yes, there are alternate interim solutions to DNSSEC that should be considered in conjunction with the move toward signing the root zone. Pending the signing of the root zone and full support for DNSSEC throughout the DNS community (including registries, registrars, ISPs, hardware manufacturers and software developers), NeuStar has developed a proprietary solution for securing our DNS. We believe DNSSEC at the root zone level is the ultimate solution for securing the DNS, but we are unable to wait to deliver enhanced DNS security to our customers.

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

    - Advantages of DNSSEC at the Root Zone Level

        - Based in standard protocols
        - One key signs all
        - Minimizes one-off solutions

    - Disadvantages of DNSSEC at the Root Zone Level

        - Time to implement
        - Marketplace awareness
        - Operational support among registries, registrars, ISPs, hardware/software providers

- *What factors impede widespread deployment of DNSSEC?*

    - Until the Kaminsky vulnerability was identified, most TLD registries and registrars did not see DNSSEC as necessary or commercially feasible. Since Kaminsky, malicious exploitation of the vulnerability has been seen and community awareness is growing regarding the importance of securing the DNS, but many entities have not yet been

convinced DNSSEC is a priority deserving of their focus and resources. Once the root zone is signed, momentum will build quickly for supporting DNSSEC at an operational level.

- *What additional steps are required to facilitate broader DNSSEC deployment and use?*
    - The root zone needs to be signed and the standard EPP extensions for registry-registrar-reseller-registrant transactions need to be supported, operationalized, and the benefits communicated to the marketplace.

- *What end-user education may be required to ensure that end users possess the ability to utilize and benefit from DNSSEC?*
    - Most users of the Internet have little or no interest in DNSSEC. They expect Internet experts to take all necessary and appropriate steps to ensure that their user experience is safe and secure.
    - Once the root zone is signed and the solution path for securing the DNS is clear, consumer-friendly documents should be prepared and publicized to help educate those with an interest.
    - The best end-user education will come from software and hardware providers that incorporate DNSSEC trust-verification into their products.

General Questions Concerning Signing of the Root Zone

- *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?*
    - Yes, DNSSEC should be implemented at the root zone level.
    - DNSSEC should be implemented at the root zone level because it is the most simple, efficient and universal method of improving and enhancing DNS security.
    - DNSSEC should be implemented at the root zone level to link all DNSSEC-enabled TLDs to one place. Having one point of trust available to all relying parties will simplify the security of the DNS. Having hundreds of points of trust will increase the chance that one rogue point can be used to hide malicious activity.
    - Any delay in signing the root zone adds risk, but signing the root zone without necessary structural safeguards would add greater risk.

- The root zone should be signed as soon as a trusted party (or parties) has been identified and all appropriate structures are in place to secure, distribute, and manage rollover of the Root Signing Keys and Key Signing Keys.

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

  - The risks of implementing DNSSEC at the root zone level lie with the selection of Root Zone Operator and key signing authorities. If the entity or entities selected are not viewed as neutral guarantors of the process, that lack of trust would likely become a perceived risk to the security and stability of the Internet.

  - The benefit of implementing DNSSEC at the root zone level is the simplicity and efficiency of a single set of keys that would anchor and validate the DNS, thereby reducing the volume of key rollover among hundreds or thousands of individual zones.

- *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 should be involved in such testing?*

  - We believe additional production testing would be desirable, particularly among registries, registrars and ISPs.

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

  - Implementation of DNSSEC at the root zone level would likely accelerate adoption throughout the DNS hierarchy.

- *How would different entities be affected by deployment of DNSSEC at the root zone level? Are these different entities prepared for DNSSEC at the root zone level and/or are each considering deployment in their respective zones?*

  - Because DNSSEC adoption would be an opt-in decision, different entities can choose to operationally support DNSSEC when they are able.

  - Once the root zone is signed and momentum builds in the community for securing and validating DNS traffic, the commercial cost of not supporting DNSSEC will far outweigh the cost of doing so.

- Each TLD operator could sign its own zone, but would be unlikely to do so if the root zone were signed. TLD operators are signing their zones today because they perceive a lack of resolve or movement toward signing the root zone.

- *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 the deployment of DNSSEC at the root zone level?*

  - Following the identification of the Kaminsky vulnerability, the cost of not implementing and supporting DNSSEC is much higher than doing so.

Operational Questions Concerning Signing of the Root Zone

- The Department recognizes that the six process flow models discussed in the appendix may not represent all of the possibilities available. The Department invites comment on these process flow models as well as whether other process flow models may exist that would implement deployment of DNSSEC at the root zone more efficiently or effectively.

- Of the six process flow models or others not presented, which provides the greatest benefit with the fewest risks for signing the root and why? Specifically, how should the 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?

  - NeuStar believes that Process Flows #4 or #6 in the NOI Appendix are the most appropriate alternatives for management of DNSSEC at the root zone level.

  - In the near term, we believe that either the IANA Functions Operator or Multiple Root Key Operators (M of N) are best able to provide the level of trust required for this important function.

  - A key factor in any decision concerning the signing of the root zone must be a clear process for the future transition of that responsibility. The Internet community must have confidence that, if a future change in operator or operators is deemed necessary, that a clear process exists to do so. Any contract or agreement governing this important function should have clauses covering cooperation in transition to a subsequent operator.

- The Department invites comment with respect to what technical capabilities and facilities or other attributes are necessary to be a Root Key Operator.

  - The Root Key Operator must have experience in operating a registry while also demonstrating its capability to secure, distribute and rollover the keys.

46000 Center Oak Plaza, Sterling, VA, USA 20166 +1 571 434 5400 +1 571 434 5786 www.neustar.biz

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

    - The value of the key is related to the value of publicizing the key to all relying parties. The key is not any more valuable than the database driving the zone. Exposure of an old key is harmless once all relying parties delete it. That is - old keys do not protect documents encrypted for long periods of time.

- 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? Why or why not? If so, would additional testing of the technique be required in advance of implementation?

    - NeuStar believes that a multi-signature technique, as represented in the 'M of N' approach (Proposed Process Flow #6) could be utilized if the IANA Functions Operator is not determined to be the better choice.

    - Given the public nature of any change to the root zone, no entity will be reasonably able to abuse the power of legitimately having the private key. The critical reason to protect the root-zone key signing key is that the expense of rolling from one KSK to the next KSK during a panic. Concern over who has legitimate control of the key is a red herring. The real problem is someone learning the key, slipping in changes to caches using it, and leaving the legitimate root zone signer to clean up the mess.