AT&T Services, Inc.

November 24, 2008

Electronic Submission

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

Re: AT&T Comments on NTIA Notice of Inquiry, Docket number: 0810021307 – 81308-01; Enhancing the Security and Stability of the Internet's Domain Name and Addressing System.

AT&T Inc, on behalf of its affiliates ("AT&T"), appreciates the opportunity to submit this response to the National Telecommunications and Information Administration, U.S. Department of Commerce Notice of Inquiry ("NOI") on "Enhancing the Security and Stability of the Internet's Domain Name and Addressing System".

As a leading provider of global IP networking services and Internet connectivity, AT&T knows that the reliability, resiliency, and security of the Internet's Domain Name and Addressing System ("DNS") and its unique indicators is of critical importance. It has been recognized that the corruption of the DNS is one effective way to corrupt, damage and impede the integrity of Internet based applications and services. AT&T also is involved in identifying, addressing, and mediating against the full range of threats and attacks on Internet networks and applications.

AT&T supports the importance of enhancing the security of the DNS. The threats that were recently revealed regarding recursive servers demonstrated the importance of ensuring the security and stability of the Internet's underlying infrastructure. The U.S. Department of Commerce, through its NOI, has served to catalyze and deepen awareness of the importance and timeliness of the questions regarding the adoption of Domain Name and Addressing System Security Extensions ("DNSSEC") and the associated question of signing the root zone.

AT&T believes the deployment of DNSSEC can bring substantial benefits by limiting the vulnerability of the DNS to the threat of cache poisoning attacks. It is important to keep in mind, however, that DNSSEC is not a full answer to Internet security, resiliency and reliability. While the Internet community continues making progress on DNSSEC implement, we also must continue to focus on addressing other challenges and threats to Internet security and stability.

The U.S. Department of Commerce's NOI correctly identifies a number of technical and operational issues that must be resolved prior to DNSSEC implementation. AT&T is in the process of analyzing the options presented, as well as other mechanisms that could be utilized to handle DNS key management. We believe further investigation and analysis is needed to fully develop a DNSSEC implementation plan, which can build on the input that is provided in response to the NOI.

There are several steps that can be taken to further develop a DNSSEC implementation plan in a transparent process with input from the Internet community. For example, the use of test bed DNSSEC deployments should be helpful in identifying technical and operational problems that may arise in signing the root zone, as well as the solutions to any such problems. These test beds also help to identify the range of challenges faced by those who are key participants in the adoption of DNSSEC, and enable planning by the community for how to reach and embrace such additional players. The U.S. Department of Commerce also could elicit additional input by organizing in-person roundtable discussions and/or by issuing further questions that build on the information provided in response to the NOI.

DNSSEC implementation, however, cannot be viewed solely as a technical question. For example, it is important to consider the impact of DNSSEC implementation on the transmission of Internet traffic, service quality and the cost of providing service. In addition, economic and political considerations must be addressed in order to ensure the successful implementation of DNSSEC. Thus, AT&T suggests that further input from the broader Internet community is essential to assessing the impact of DNSSEC and developing an implementation plan.

Moreover, the full impact of DNSSEC on the other parties involved in the Internet needs to be understood. AT&T believes that DNSSEC can only be fully effective if all DNS zones are digitally signed, starting with the root zone. The role of signing the root in driving further implementation of DNSSEC at other layers of the Internet ecosystem – such as ISPs, software companies and Internet backbone providers – is not yet fully understood. In addition, further examination is needed regarding the roles and responsibilities of the present "registries" and 'registrars' in the implementation and support of DNSSEC, which will directly impact how and when the largest generic top level zones (i.e., ".com" and ".net") will be signed. Ultimately, successful DNSSEC implementation will require a coordinated approach that seeks to minimize complexity and avoid imposing excessive costs on Internet users.

AT&T appreciates the U.S. Department of Commerce, through the National Telecommunications and Information Agency, for its leadership in advancing the dialogue and examination of the issues related to the role of DNSSEC in the security and stability of the DNS. We look forward to participating as this dialogue continues, and in the examination of solutions that are broadly accepted by all affected stakeholders.

Respectfully submitted,