UNITED STATES COUNCIL FOR INTERNATIONAL BUSINESS

November 24, 2008

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

**Re: NTIA Notice of Inquiry, Enhancing the Security and Stability of the Internet's Domain Name and Addressing System: DNSSEC Implementation at the Root Zone**

Dear Ms. Alexander:

The United States Council for International Business (USCIB) appreciates the opportunity to submit this response to the U.S. Department of Commerce Notice of Inquiry on "Enhancing the Security and Stability of the Internet's Domain Name and Addressing System."

USCIB is a business association whose membership includes some 300 leading U.S. companies, professional services firms and associations, representing a wide array of Internet stakeholders, including general business users, ISPs, IP Rights Holders, registries, and registrars. The secure and stable functioning of the Internet is of critical importance to all of our members given the amount of their business that is conducted over it.

As such, USCIB supports efforts to improve the security and stability of the Domain Name System (DNS), the Internet's hierarchical naming system that translates human-friendly domain names into numerical Internet Protocol addresses. We believe increased security is necessary in light of ongoing threats to the Internet's infrastructure. These threats include the DNS vulnerability publicized by Dan Kaminsky and other Internet security researchers in the summer of 2008. As these experts noted, unpatched computer servers are particularly vulnerable to a DNS attack called "cache-poisoning" that redirects unsuspecting Internet users to malicious sites or hijacks their email.

USCIB believes that DNS security could be further improved by the deployment of DNS Security Extensions (DNSSEC), a suite of software specifications for digitally signing certain DNS information. At present, DNSSEC offers unmatched data origin authentication and data integrity features that can thwart cache poisoning attacks. While the DNS community is exploring other security options, no other solution has been fully developed nor would any of the proposed possible solutions provide the same protections offered by DNSSEC in response to this particular vulnerability.

1212 Avenue of the Americas
New York, NY 10036-1689
212.354.4480 tel
212.575.0327 fax
www.uscib.org

It must be noted that DNSSEC will only live up to its promise if all DNS zones are digitally signed. While this "chain of trust" will need to include the root zone, a signed root alone will not improve DNS security nor spur the widespread DNSSEC implementation. Several economic and political issues surrounding the signing of the root likely will be as critical to the success of this initiative as the technical aspects documented in the proposals before the U.S. Department of Commerce.

Thus USCIB supports deployment of DNSSEC in a manner that recognizes both the significant benefits and potential challenges inherent in the deployment of any technology. Particular issues to be considered for DNSSEC include the impact of the protocol on the size and speed of Internet traffic, what entities will bear the burden for deployment, and what entity or entities will ensure and be accountable for implementation.

As part of this process on the technical side, USCIB suggests that creating and analyzing data from a signed-root test bed could facilitate the adoption of DNSSEC. We recognize that appropriate live testing and safeguards in real-world, end-to-end environments that include the root can help ensure the continued security and stability of the DNS. Other test-beds exist and it may be helpful to synthesize data from these as well in order to leverage work already done.

With regards to process flows of deployment, USCIB favors those options that reduce cost and complexity while enhancing security and preserving stability. Furthermore, it is vital that every stage of DNSSEC deployment, as well as management and invalidation of key-signing keys, be fully transparent.

While USCIB supports a role for DNSSEC, we recognize that its deployment will not solve every security issue on the Internet; it only addresses the issue of DNS data integrity. The business community, as well as other stakeholders, must remain vigilant in the face of persistent and emerging threats to the DNS. DNSSEC deployment will help resolve one critical issue, but continued work towards increasing security and stability overall must remain a top priority as the Internet grows in size and complexity.

USCIB commends the U.S. Department of Commerce for its ongoing interest in providing for the security and stability of the DNS. We believe that DNSSEC is the best tool to address a widely publicized vulnerability in the DNS. We support DNSSEC deployment, with encouragement for the U.S. Department of Commerce to carefully consider the aforementioned issues in order to foster solutions that will be acceptable to all interested parties.