The NetChoice Coalition
Promoting Convenience, Choice, and Commerce on The Net
Steve DelBianco, Executive Director
1401 K St NW, Suite 502
Washington, DC 20005
202-420-7482
www.netchoice.org

November 24, 2008

Comment in response to NTIA Notice of Inquiry (NOI) regarding
Domain Name and Addressing System Security Extensions (DNSSEC)

DNSSEC is necessary—but not sufficient—to improve the integrity and security of the Internet.

For businesses that rely on e-commerce, Internet security vulnerabilities translate into direct and indirect financial harm. Direct harms include actual losses, plus the substantial investments made in security software, hardware, and services.   Indirect harm is felt whenever a current or potential consumer declines to do business online, which is understandable given the frightening headlines about online crime. For these reasons, e-commerce leaders have consistently promoted a policy and technical environment that supports a stable and secure Internet.

In our recent report, "*Hardening the Security Stack*" (http://www.netchoice.org/library/netchoice-security-stack-paper.pdf), NetChoice described how DNSSEC will play a role in the broader effort to improve security of the DNS. Our report maintains that DNSSEC addresses only one of the many security challenges facing the Internet, but is vital to thwart cache poisoning attacks. In essence, we conclude that DNSSEC is necessary--but not sufficient—to solve Internet security vulnerabilities.

DNSSEC implementation will be extremely challenging.

Implementing DNSSEC presents many serious technological challenges. Mistakes in implementation could destabilize the DNS and disrupt the end-user experience, possibly causing more harm than good. Still there appears to be growing consensus among technologists that it is time to move forward with implementing DNSSEC, initially for the root-zone and eventually for all zones.

As indicated in the NOI, this consensus creates more questions than it answers, triggering a larger discussion about how DNSSEC should be implemented. One major question is what entity or combination of entities should manage root signing and hold the keys.   Determining the right answer to these questions may mean the difference between success and failure in this critical initial experience with DNSSEC.

ICANN has too much on its plate to take on the additional complexities and responsibilities of DNSSEC

We leave the technical questions of this NOI to technical experts who have worked with DNSSEC for the past decade. Instead, what concerns NetChoice is the ambitious attempt by ICANN (Internet

Corporation for Assigned Names and Numbers) to choose this point in its history to take on the serious challenges associated with implementing and managing DNSSEC.

At least one of the proposed DNSSEC models envisions ICANN taking the technical and administrative lead in implementing DNSSEC at the root level. This would mark a new and complex challenge for ICANN, which is already struggling to meet self-imposed deadlines on a number of key challenges facing the global DNS.

Even a partial list reveals the astonishing scope and complexity of what's on ICANN's plate today. In the year ahead, ICANN plans to:

- Accept and review several hundred application from entities around the world seeking to operate new top-level domains;

- Implement internationalized domain names in top-level domains – for the first time;

- Restructure itself to be more independent, accountable, transparent; and

- Declare independence from its legacy relationship with the U.S. Commerce Department.

Meanwhile, ICANN continues to feel pressure from long-standing challenges. Over the past year ICANN has witnessed:

- Increasing cyber-crime and online fraud that exploits weaknesses in DNS oversight;

- A schism over restructuring plans for the GNSO, the most significant supporting organization in ICANN.   Non-contracted parties are understandably concerned that "reform for the sake of reform" has diminished the role of the private-sector in ICANN's bottom-up, consensus process; and

- the Secretary General of the International Telecommunications Union declared earlier this month that ICANN must give governments a more direct role in setting Internet technical policies.

As active participants in ICANN since 2004, we have directly witnessed the strain caused by these challenges. We readily acknowledge that ICANN's tasks are made more difficult by its commitment to a bottom-up, consensus-driven process for policy development.

Yet, even with a massive growth in staff and consulting resources, ICANN is struggling to meet deadlines and address its growing portfolio of issues. Key deadlines have slipped, critical documentation is provided late, or at the last minute, and constituency leaders are growing increasingly restive about process problems and uncontrollable outcomes.

NetChoice supports the ICANN model, and will continue working to help ICANN weather the significant challenges it faces in the coming years. In fact, the executive director of NetChoice and its member companies are among the most reliable participants in policy working groups and at ICANN meetings.

But anyone close to ICANN can see that this is not an organization that should actively seek complex new challenges at this time – particularly when there are other viable options available.

If we have learned anything DNSSEC in the past decade, it is this: *implementation in the real world is much harder than implementation in the lab*.   Global implementation of DNSSEC for the root-zone will be the greatest test yet of this critical technology. It will require the full attention and skills of whatever entity takes on the challenge.

ICANN is entering the single most challenging and potentially destabilizing period of its decade-long existence. We are deeply skeptical of any decision that would increase the serious challenges facing this critically important entity.

Sincerely,

Steve DelBianco
Executive Director, NetChoice

About NetChoice

NetChoice is coalition of trade associations and e-commerce companies, including more than 10,000 small businesses that rely on e-commerce. NetChoice members care deeply about upholding and improving the security and stability of the global Internet, beginning with the Domain Name System. NetChoice is an active participant in the Internet governance process through its involvement with the Internet Corporation for Assigned Names and Numbers (ICANN) and in other arenas such as the annual Internet Governance Forum.

See www.netchoice.org and http://blog.netchoice.org