Testimony of Fiona M. Alexander
Associate Administrator, Office of International Affairs
National Telecommunications and Information Administration
United States Department of Commerce

Before the

Committee on Energy and Commerce
Subcommittee on Communications and Technology
United States House of Representatives

Hearing on
"Cybersecurity: Threats to Communications Networks and Public-Sector Responses"
March 28, 2012

Introduction

Good morning Chairman Walden, Ranking Member Eshoo, and Members of the Committee. Thank you for this opportunity to testify on behalf of the Department of Commerce's National Telecommunications and Information Administration (NTIA) regarding cybersecurity. NTIA is the President's principal advisor on telecommunications and information policy matters, and is the Executive Branch expert on issues relating to the Internet's domain name system (DNS) - a critical component of the cyber infrastructure. NTIA supports a multi-stakeholder approach to the coordination of the DNS to ensure the long-term viability of the Internet as a force for innovation and economic growth. Working with other stakeholders, NTIA develops policies and takes actions to preserve an open, interconnected global Internet that supports continued innovation and economic growth, investment, and the trust of its users. This multi-stakeholder model of Internet policymaking – convening the private sector, civil society, as well as governments to address issues in a timely and flexible manner – has been responsible for the past success of the Internet and is critical to its future.

The Internet plays an increasingly vital role in daily life, from helping businesses expand to improving education and health care. Every day, millions of Americans shop, sell, bank, learn, talk, and work online. At the turn of the century, online retail sales totaled approximately $20 billion in the United States, now they are nearing $200 billion. The growth of the Internet is due in part to the trust of its users – trust, for example, that when users type a website address, they will be directed to their intended destination. Given the Internet's importance to the Nation's economic and social advancement, it is essential that the Internet - and its underlying infrastructure - remain stable and secure. This is a primary objective motivating NTIA's efforts to secure the DNS and what I specifically will address today.

DNS Vulnerabilities and Efforts to Enhance Security through DNSSEC

The DNS is a critical component of the Internet infrastructure. It works like a telephone directory, allowing users to reach websites using easy-to-understand domain names (e.g., http://www.commerce.gov) rather than the numeric network server addresses (e.g., http://170.110.225.194) necessary to retrieve information on the Internet. The authenticity of the DNS data is essential to the security of the Internet – it is vital that users reach their intended destinations on the Internet and are not unknowingly redirected to fraudulent and malicious websites.

The early DNS, while exceptional in many ways, lacked strong security mechanisms. Over time, hackers and others have found more and more ways to exploit vulnerabilities in the DNS protocol that put the integrity of DNS data at risk. These vulnerabilities increase the likelihood of certain DNS-related cyber attacks, such as man-in-the-middle attacks, which could lead to identity theft and other security compromises.

In response to these risks, the Internet Engineering Task Force (IETF), a multi-stakeholder body that develops and promotes Internet standards, developed Domain Name System Security Extensions (DNSSEC), a suite of specifications for securing information provided by the DNS. DNSSEC provides an additional layer of security to the DNS by authenticating the origin of DNS data and verifying its integrity while it moves across the Internet.

NTIA's Efforts to Promote DNSSEC

In 2008, NTIA undertook a multi-stakeholder public consultation process regarding whether and how DNSSEC should be deployed at the authoritative root of the DNS – the top-level zone of the DNS hierarchy for which NTIA has historical oversight.[1] In response to the public notice, NTIA received an overwhelming response from the global multi-stakeholder Internet community supporting efforts to implement DNSSEC at the authoritative root as soon as possible. Over the next year and a half, NTIA worked closely with the Department of Commerce's National Institute of Standards and Technology (NIST), as well as its root zone management partners – VeriSign and the Internet Corporation for Assigned Names and Numbers (ICANN) – to fully deploy DNSSEC at the root in July 2010. This effort enjoyed the support of the multi-stakeholder Internet community and drew upon the input and expertise of technical experts from around the world.

DNSSEC deployment at the authoritative root was an important step toward protecting the integrity of DNS data and mitigating attacks such as cache poisoning, which allows an attacker to redirect traffic to fraudulent sites, and other data modification threats. This effort marked significant progress in making the Internet more robust and secure. DNSSEC essentially gives a "tamper proof seal" to the address book of the Internet, and in so doing, gives Internet users greater confidence in their online experience. As a result, Internet users will have greater confidence that when they visit a particular website – whether it be their bank, retailer, or doctor – they are not seeing a spoofed copy that cybercriminals can use to perpetuate identity theft or other crimes using the DNS.

In helping to deploy DNSSEC at the root zone, NTIA sought to facilitate greater DNSSEC deployment throughout the rest of the global DNS hierarchy. To realize the greatest benefits of DNSSEC, there needs to be broad deployment, support, and participation of actors throughout the Internet landscape, including, for example, domain name registrars, top-level domain registry operators, ISPs, software vendors, and others. Since the deployment of DNSSEC at the root, adoption of DNSSEC has increased throughout the Internet ecosystem. While these efforts are encouraging, NTIA is committed to increasing adoption further.

If we are to maintain trust in the Internet, we must support further DNSSEC deployment. Governments, as well as other stakeholders, must continue to support the deployment and development of DNSSEC-related software, tools, and other products and services. As we explore issues affecting the Internet space, we should take all appropriate steps to ensure that DNSSEC use and adoption continues to grow and to maintain the security and stability of the DNS. In the coming months, NTIA, working as a part of the Department's Internet Policy Task Force, will be looking for opportunities to launch further multistakeholder processes aimed at enhancing security and stability of the DNS as well as broader cybersecurity efforts.

Conclusion

Thank you again for the opportunity to testify. NTIA looks forward to working with Congress, U.S. business, individuals, and other stakeholders to preserve and enhance the security and stability of the Internet DNS. NTIA will continue its efforts to support the broader deployment of DNSSEC and welcomes the opportunity to continue this discussion in the future.

I will be happy to answer any questions.

---

[1] For more information, see http://www.ntia.doc.gov/legacy/DNS/noi_10092008.html.