The Committee on Energy and Commerce

Internal Memorandum

March 5, 2012

MEMORANDUM

To: Members and Staff, Subcommittee on Communications and Technology

From: Majority Committee Staff

Subject: Hearing on "Cybersecurity and the Pivotal Role of Communications Networks"

The Subcommittee will hold a hearing Wednesday, March 7, 2012, at 10:00 a.m. in 2123 Rayburn House Office Building on "Cybersecurity and the Pivotal Role of Communications Networks." This hearing will continue our examination of cybersecurity and our communications infrastructure with a focus on what Internet Service Providers (ISPs) are doing to address cybersecurity, whether there are statutory or regulatory obstacles hampering their efforts, how we can encourage public-private partnerships, and how we can facilitate information sharing among private industry and between the private and public sectors.

I. WITNESSES

One panel of witnesses will testify:

Dr. Edward Amoroso
Chief Security Officer
AT&T Services, Inc.

Mr. David Mahon
Chief Security Officer
CenturyLink

Mr. Jason Livingood
Vice President, Internet Systems Engineering
Comcast Corporation

Mr. John Olsen
Senior Vice President & Chief Information Officer
MetroPCS Communications Inc.

Additional witnesses may be added.

II. BACKGROUND

DNSSEC. An issue raised in our February 8, 2012, cybersecurity hearing was the ability of bad actors to spoof the Domain Name System (DNS), the system that translates domain names (*e.g.*, www.house.gov) into machine-readable IP addresses (*e.g.*, 172.228.181.132). By exploiting vulnerability in the DNS, a bad actor can perform a "man-in-the-middle" attack on consumers. In such an attack, consumers think their username, password, or other personal information is being securely transmitted to their bank, email service, or other trusted partner. In fact, because the bad actor has inserted itself between the consumer and the website, the bad

actor is able to see all the information transmitted between the two. To prevent such attacks, the Internet Engineering Task Force created DNS Security Extensions (DNSSEC), which are designed to certify that the IP address provided by the DNS is in fact the IP address of the website the consumer is trying to access. However, for DNSSEC to be effective, three different groups must adopt the framework: (1) ISPs need to make their DNS servers DNSSEC compatible; (2) domain owners need to enable their websites to send back authenticating information, and (3) browsers need to be able to request and process the authentications.

DNSSEC has been implemented to varying degrees across the Internet. More than 50 top-level domains—including .com, .net. .gov, and .edu—have taken the steps necessary to participate in DNSSEC. However, because DNSSEC requires all intermediate DNS servers to participate, ISPs must also implement it for consumers to realize the benefits.

Code of Conduct/Best Practices. Industry adoption of a voluntary code of conduct and best practices could also improve cybersecurity and promote consumer practices that help combat cyberthreats like malware and botnets. Australia has implemented a voluntary code of conduct, called iCode, that has greatly reduced botnets, malware, and spam in the country's communications networks. For a code of conduct or best practices to be effective, there must be widespread adoption.

Supply Chain Risk Management. While established networks face a number of cybersecurity challenges, a network is only as secure as the elements that comprise the network. As service providers acquire the software, servers, switches, and other equipment that deliver services to consumers, just one link in the chain with questionable provenance can introduce vulnerability into an otherwise secure network. Bad actors have a number of ways to potentially corrupt the communications supply chain, from malicious code in the components that could compromise the integrity of the communications on the network to attempts to remotely cause network elements to fail.

Information Sharing. ISPs and other network operators may discover cyberthreats as they use traffic analysis to manage their networks. They may be reluctant to publicize or share this information, however, because of concerns over liability, public confidence, or the sharing of competitively sensitive information. Sharing cyberthreat information with other companies may also violate current laws and regulations. While federal government agencies also collect their own data on potential cyberthreats, current law or custom may similarly hinder their ability or willingness to share information.

Trusted Routing. As consumers increasingly adopt services that move information through "the cloud," it is important to know that data is arriving at its intended destination and that the systems the data transits are secure. Trusted routing efforts are aimed at ensuring the security of data throughout its network transit.

Educating Consumers. Consumer education is key to securing communications networks. It is sometimes stated that the weakest part of a data network sits between the chair and the keyboard. Because the Internet and technology landscape are constantly changing, it is

difficult for the average consumer to keep up with new cyberthreats. As the panel of experts discussed at the February 8, 2012, hearing on this topic, there is an ever changing variety of ways that cyberthreats can enter a customer's daily life. Network providers have a unique relationship with their customers to easily distribute cyberthreat information. Streamlining the ability of network providers to equip consumers with this information and the tools to secure their online lives will secure all networks from evolving cyberthreats.

If you need more information, please call Neil Fried or David Redl at (202) 225-2927.