

The Committee on Energy and Commerce

MEMORANDUM



March 26, 2012

To: Members and Staff, Subcommittee on Communications and Technology

From: Majority Committee Staff

Subject: Hearing on “Cybersecurity: Threats to Communications Networks and Public-Sector Responses”

The subcommittee will hold a hearing Wednesday, March 28, 2012, at 10:00 a.m. in 2322 Rayburn House Office Building on “Cybersecurity: Threats to Communications Networks and Public-Sector Responses.” This is the third hearing in the Subcommittee’s cybersecurity series.

I. **WITNESSES**

One panel of witnesses will testify:

Ms. Fiona Alexander
Associate Administrator
Office of International Affairs
National Telecommunications and Information
Administration (NTIA)
U.S. Department of Commerce

Admiral Jamie Barnett (ret.)
Chief
Public Safety & Homeland Security Bureau
Federal Communications Commission (FCC)

Mr. Bob Hutchinson
Senior Manager for Information Security
Sciences
Sandia National Laboratories

Mr. Greg Shannon
Chief Scientist
Computer Emergency Readiness Team
Software Engineering Institute
Carnegie Mellon University

Ms. Roberta Stempfley
Acting Assistant Secretary for Cyber Security
and Communications
Department of Homeland Security

II. BACKGROUND

Americans are more interconnected today than ever before. Communications networks empower our citizens to share information across the country in the blink of an eye. The Internet has become an essential component of our economy and now also supports vital infrastructure and services. Major disruptions in our communications networks could have crippling consequences for the country.

The private sector and communications industry witnesses at the Subcommittee's prior two hearings, however, urged that the federal government move cautiously when considering federal intervention in the cybersecurity arena. Stakeholders have expressed similar sentiments when meeting with the Subcommittee's bipartisan cybersecurity working group. Collectively they argued that one-size solutions don't fit all; that there are few technical solutions that legislation could advance that industry is not already working on; that by the time the government were to legislate standards and solutions, both industry and bad actors would likely have moved beyond them; that when Congress passes cyber-laws it increases regulatory obligations that bad actors ignore but that industry must confront, diverting resources; that regulated solutions offer bad actors a roadmap for evasion and mischief; and that any legislation must remain cognizant of privacy and civil liberties issues. They recommended, therefore, that the federal government focus on education, information sharing, advancing voluntary best practices, and eliminating regulatory obstacles to collaboration between and among the private and public sectors.

This hearing will examine threats to America's communications networks, what the public sector is doing to address those threats, how it is working with the private sector, and what role the federal government should play in securing communications networks. The Subcommittee will hear from witnesses representing the FCC, the NTIA, the DHS, Carnegie Mellon's Computer Emergency Readiness Team, and Sandia Laboratories.

The FCC. The FCC is actively involved in cybersecurity issues as a host of the Communications Security, Reliability and Interoperability Council (CSRIC). Council members include individuals from federal agencies, state and local governments and law enforcement agencies, and private companies. CSRIC provides recommendations to the FCC to ensure security and reliability of communications networks. The CSRIC's Cybersecurity Working Group released a best practices report March 22, 2012, to address botnet attacks, domain name fraud, and IP route hijacking. The report appears to advocate a similar approach to the well received voluntary code of conduct Australia adopted, which was discussed at a prior hearing. To be successful, this type of approach should likely remain voluntary and nimble so it can evolve over time, and should involve all stakeholders, not just Internet service providers (ISPs).

The NTIA. The NTIA serves as the principal advisor to the President on telecommunications policy and how it pertains to the economy. It has been involved in cybersecurity issues through its oversight of the Internet Corporation for Assigned Names and Numbers and efforts to implement Domain Name Server Security Extensions, a topic discussed at previous hearings.

DHS. The Department of Homeland Security (DHS) has several divisions that are involved with cybersecurity.

The Office of Emergency Communications (OEC) works to ensure that emergency responders and government officials are able to communicate during natural disasters, terrorist attacks, and other emergencies. OEC is also tasked with establishing and maintaining interoperable emergency communications nationwide. The office was created by Congress in response to the inability of emergency responders to communicate with each other during Hurricane Katrina.

The National Cybersecurity Division (NCSD) works with public, private, and international entities to build and maintain an effective cyberspace response system and to implement a risk management program for protecting critical infrastructure. Within the NCSD are several programs that work to achieve these goals. One such program is the United States Computer Emergency Readiness Team (US-CERT). US-CERT works with private companies to analyze cyber threats and vulnerabilities and coordinates responses to Internet disruptions. US-CERT utilizes the National Cyber Alert System to send email notifications to subscribers in an effort to help citizens protect their own computers from cyber attacks.

The National Cybersecurity and Communications Integration Center (NCCIC) was created to consolidate and coordinate all DHS cyber and communications operation centers. It works with all levels of government and the private sector to enhance DHS's ability to mitigate risks and respond to threats and disruptions to the nation's communications networks. The NCCIC combines the operations of US-CERT and the National Coordinating Center for Telecommunications, which coordinates information sharing between agencies to restore communications networks during national emergencies.

Sandia National Laboratories. The Sandia National Laboratories are two Department of Energy research and development labs operated by the Sandia Corporation, a wholly owned subsidiary of the Lockheed Corporation. One of Sandia's main tasks is to ensure the reliability of the nation's nuclear weapon systems and critical infrastructure from all types of attacks and has for some time concentrated on cyberthreats. Out of necessity, Sandia has developed some of the most sophisticated techniques to detect and thwart cyberattacks. Sandia's Supervisory Control and Data Acquisition (SCADA) test bed has developed engineering best practices, industry standards, and vulnerability assessments for America's energy control systems. Sandia also runs the Center for Cyberdefenders Program, which familiarizes computer science students with computer systems, network operations, and information security. Many of these students go on to work for Sandia or other government and private-sector entities in the field of cybersecurity.

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