



The Committee on Energy and Commerce

Internal Memorandum

March 23, 2012

TO: Members, Subcommittee on Oversight and Investigations

FROM: Subcommittee on Oversight and Investigations Staff

RE: Hearing on “IT Supply Chain Security: Review of Government and Industry Efforts”

On Tuesday, March 27, 2012, at 10:00 a.m. in room 2123 of the Rayburn House Office Building, the Subcommittee on Oversight and Investigations will hold a hearing entitled “IT Supply Chain Security: Review of Government and Industry Efforts.”

This hearing is the third in a series of hearings that focuses on the cybersecurity threats related to federal information technology (IT), infrastructure, and industries within the jurisdiction of the Energy and Commerce Committee. The hearing will provide an overview of the supply chain risks to federal IT and the federal government’s efforts to recognize these risks and mitigate the impacts they pose. The hearing will also examine the Government Accountability Office’s (GAO) report entitled “IT Supply Chain: National Security-related Agencies Need to Better Address Risks.” In particular, the Subcommittee will examine the challenges the national security agencies and industry face as they work to identify and address risks to Federal IT systems.

I. WITNESSES

Two panels of witnesses will testify at the hearing:

Panel I

Mr. Gregory C. Wilshusen
Director of Information Security Issues
Government Accountability Office (GAO)

Mr. Mitchell Komaroff
Director, Trusted Mission Systems Networks
U.S. Department of Defense

Mr. Gil Vega
Associate CIO for Cybersecurity & Chief Information Security Officer
U.S. Department of Energy

Panel II¹

Mr. Larry Castro
Managing Director
The Chertoff Group

Mr. Dave Lounsbury,
Vice President
Government Program & Managing Director, U.S. Research & Technology
The Open Group

II. BACKGROUND

A supply chain is a system of organizations, people, technology, activities, information and resources involved in producing a good or service from supplier to customer. Our nation has a highly connected global IT market which creates highly sophisticated challenges to ensure the integrity of supply chains. To protect the integrity of these manufacturing processes, cybersecurity criteria for information technology systems, software and networks are necessary. Developing criteria for cybersecurity requires an assessment of network threats such as cyberterrorism, malware, data theft and the Advanced Persistent Threat (APT). No two supply chains are the same and neither are the solutions.

Securing our vast IT systems is critical to our national and economic security. The federal government is one of the largest purchasers of IT systems and must ensure that the products and services it acquires are protected. In January 2012, the Director of National Intelligence identified the vulnerabilities associated with the IT supply chain as one of the greatest strategic cyber threat challenges.² IT supply chain-related threats can be introduced at any point in the development or distribution process. IT products and services are so prevalent today that a vulnerability in a supply chain threatens an agency's confidentiality, integrity, and availability of its critical and sensitive networks, IT-enabled equipment, and data.

The Comprehensive National Cybersecurity Initiative (CNCI) aims to guide cybersecurity within the federal government.³ The CNCI recommends developing a multi-pronged approach for addressing global supply chain risk management due to the globalization of the commercial information and communications technology marketplace. According to the

¹ Both Mr. Castro and Mr. Lounsbury do not represent government agencies and will be providing a private industry perspective on supply chain risk management best practices.

² Director of National Intelligence, Worldwide Threat Assessment of the US Intelligence Community, unclassified statement for the record, Senate Select Committee on Intelligence (Washington, D.C.: January 31, 2012).

³ See The White House, The Comprehensive National Cybersecurity Initiative (Washington, DC: March 2010), <http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf>.

CNCI initiatives, risks originating from both the domestic and global supply chains must be managed in a strategic and comprehensive way over the entire lifecycle of products, systems and services.⁴ The reality of the global marketplace today underscores the importance threat assessments and risk mitigation in the procurement of federal IT.

To pinpoint departmental efforts to identify IT supply chain risks and analyze information security policies, GAO conducted an audit from November 2010 to February 2012 of the following agencies: Department of Energy (Energy), the Department of Justice (Justice), Department of Homeland Security (DHS), and Department of Defense (Defense). GAO concluded that, while these agencies have made strides to identify and address IT supply chain threats and risks, more comprehensive policies, procedures and monitoring capabilities are needed to manage emergent IT supply chain risks.

The report is attached to this memorandum.

III. ISSUES

The following issues will be examined at the hearing:

- The key risks associated with the supply chains used by federal agencies to procure IT equipment, software, or services;
- The extent to which selected national security-related agencies have addressed IT supply chain risks;
- The extent to which national security-related federal agencies have determined that their telecommunications networks contain foreign-developed equipment, software, or services; and,
- The extent to which private industry has addressed IT supply chain risks.

IV. CONTACTS

If you have any questions about this hearing, please contact Carl Anderson or Karen Christian at (202) 225-2927.

Attachment

⁴ See Ibid, CNCI Initiative #11.