The Committee on Energy and Commerce

Memorandum

May 17, 2013

To: Members and Staff, Subcommittee on Communications and Technology

From: Majority Committee Staff

Subject: Communications Supply Chain Hearing

The Subcommittee will hold a hearing Tuesday, May 21, 2013, at 2:00 p.m. in 2123 Rayburn House Office Building entitled “Cybersecurity: An Examination of the Communications Supply Chain.”

I. Witnesses

Jennifer Bisceglie
President and CEO
Interos Solutions, Inc.

Robert B. Dix, Jr.
Vice President, Government Affairs and Critical Infrastructure Protection
Juniper Networks, Inc.

Mark L. Goldstein
Director, Physical Infrastructure Issues
Government Accountability Office (GAO)

John Lindquist
President and CEO
Electronic Warfare Associates

David Rothenstein
Senior Vice President, General Counsel and Secretary
Ciena

Stewart A. Baker
Partner, Steptoe & Johnson LLP
Former Assistant Secretary for Policy, Department of Homeland Security (DHS)

Dean Garfield
President and CEO
Information Technology Industry Council

II. Background

The features of modern communications networks that make them so useful are also what make them vulnerable: their decentralized, interconnected nature and their international scope. The more the world relies on communications networks for business, entertainment, and emergency response the more, too, it risks if those networks are compromised. This hearing will look at challenges in securing the communications supply chain, what steps industry is taking, and what role standards organizations, public-private partnerships, and the government might play.

The Potential Threat. The complex, interdependent, and myriad software and hardware components that make up the communications infrastructure present multiple points of attack for those that seek to do harm. Bad actors can plant vulnerabilities in the supply chain or take advantage of vulnerabilities that creep in inadvertently. They can insert malicious or insecure hardware or software into a communications network or alter legitimate software operating on legitimate equipment. And, because communications networks are interconnected, someone else's vulnerability can be everyone's vulnerability. Just as there is a strong decentralized component to the networks so, too, must there be a strong decentralized component to the defenses. Moreover, just as there is no one-size-fits-all network, there cannot be a one-size-fits-all response. Since the technology underlying both the U.S. infrastructure and cyber-attacks can change rapidly, protective measures must evolve rapidly, as well.

How vulnerable is the supply chain? What are the main vulnerabilities? How much of the vulnerability comes from malicious activity and how much comes from poor design? How can the supply chain be secured in the various stages of manufacture, shipment, installation, and operation? What are the different challenges in protecting the software and hardware supply chains? Is one more vulnerable than the other? How can the networks be defended without losing the benefits that come from the interconnected nature of our communications architecture? Would better information sharing between and among government and the private sector help? What kinds of cost-benefit and risk analyses should go into securing the communications supply chain?

Standards Organizations. Various organizations in the U.S. and abroad—such as the International Standards Organization and the American National Standards Institute—develop best practices and standards for securing the supply chain. What types of best practices and standards have organizations such as these promulgated? Have they been successful in ameliorating supply chain risks? What additional challenges do open standards present? Are proprietary processes more or less secure than open standards? Can standardization itself ironically make vulnerabilities more widespread? Where are best practices and standards most effective? Are voluntary approaches sufficient or are some mandatory measures necessary?

CFIUS and Team Telecom. The Committee on Foreign Investment in the United States (CFIUS) and Team Telecom are two organizations that review significant communications transactions. While not their sole focus, they sometimes examine supply chain issues.

The CFIUS examines purchases of U.S. businesses by foreign entities. An inter-agency group headed by the U.S. Department of Treasury, the CFIUS includes representatives from the Departments of Justice, Homeland Security, Commerce, Defense, State and Energy, as well as the Office of the U.S. Trade Representative and the White House Office of Science and Technology Policy. Additionally, the Office of Management and Budget, the Council of Economic Advisors, the National Security Council, the National Economic Council, the Homeland Security Council, the Director of National Intelligence, and the Secretary of Labor participate as observers or *ex officio* members. French company Alcatel's acquisition of Lucent Technologies, U.K. company Vodafone's acquisition of AirTouch, and German company Deutsche Telekom's acquisition of VoiceStream were all subject to CFIUS review.

Team Telecom is an informal inter-agency group within the U.S. government that advises the Federal Communications Commission on the law enforcement and national security implications of significant transactions. It includes representatives from the Departments of Homeland Security, Justice (including the FBI), and Defense.

How well do the CFIUS and Team Telecom processes work? Should they be expanded to cover purchases of equipment or software by U.S. communications companies? If so, what types of purchases should they focus on? What impact would such review have on the operation of communications companies?

Trusted Delivery and Code Escrow. To secure the supply chain, some companies—and countries—arrange for trusted third-parties to take delivery of the hardware and software for communications networks. The third parties may serve a variety of functions, from inspecting manufacturing facilities to securing and testing products. They may be involved in the entire lifecycle of the equipment or software. In the case of software, the third party may hold a copy of the code in escrow. In such cases, the security company first receives and secures a copy of the software prior to its compilation. Experts then review the "raw" software for anomalous code, coding errors, and potential vulnerabilities. Next, the security company takes delivery of the compiled software, referred to as the binary code. To ensure the reviewed software is the same as what is being installed, the firm compares this binary code to the binary code that results from compiling the raw software it received in step one. Finally, the company may randomly test future shipments of the software or manage installation of the software on delivered hardware.

How well do trusted delivery and code escrow work? In what situations should they be used? The United Kingdom has used trusted delivery and code escrow to manage hardware and software purchased from companies such as China's Huawei. Is there greater reason to employ such measures in the purchase of foreign products than domestic ones?

Foreign Suppliers. The House Permanent Select Committee on Intelligence initiated an investigation in November 2011 into the level of security risk posed by telecommunications companies with potential ties to the Chinese government or military. The Intelligence Committee focused on Huawei and ZTE, the top two Chinese telecommunications equipment manufacturers. The Committee concluded in an October 2012 report that the companies had failed to quell concerns that relying on their equipment could pose security threats because of the possible influence of the Chinese government. The report recommended, therefore, that the companies be more transparent; that the Committee on Foreign Investment in the United States block acquisitions, takeovers, or mergers involving Huawei and ZTE; that the relevant congressional committees consider expanding the role of the CFIUS to cover purchasing agreements; that U.S. government systems not use Huawei or ZTE equipment, particularly if the systems are sensitive; that the private sector strongly consider using other vendors; and that congressional committees of jurisdiction consider whether legislation—including information sharing legislation—is needed to better address the risk posed by telecommunications companies with nation-state ties.

How do cost pressures on domestic communications companies in the competitive communications marketplace and the growing dependence on foreign suppliers impact supply chain security? How do the supply chain risks compare between the purchase of hardware and software from foreign companies and domestic companies? Are purchases from some countries riskier than others and, if so, how should that relative risk be assessed? Much of the equipment in U.S. communications networks are manufactured and assembled in China, or contain components that are manufactured and assembled there, even when the vendor itself is not a Chinese company. How should the risk in those scenarios be assessed?

Recent Federal Activity. The National Institute of Standards and Technology (NIST) released its "Notional Supply Chain Risk Management Practices for Federal Information Systems" in 2012. In the document, NIST details an approach for government agencies to determine the risk associated with elements of an information system to identify and secure each stage of the supply chain and to manage security mechanisms through the entire lifecycle of the purchased equipment. The Obama Administration released its *National Strategy for Global Supply Chain Security* in January 2013. The *National Strategy* seeks to harmonize supply chain practices across the Federal government and develop best practices for application to commercial networks. The Administration released its Executive Order on cybersecurity and Presidential Policy Directive 21 in February 2013, both aimed at improving U.S. cybersecurity, including supply chain integrity. The Executive Order and Presidential Policy Directive instruct Executive Branch agencies to review existing regulations and to propose new ones to improve cybersecurity if necessary. Executive Branch agencies are currently in the process of implementing these orders.

How well are each of these approaches expected to work? What role should the Federal government play in securing the supply chain? Can it set a positive example in the deployment of its own networks? What impact can it have as a large purchaser of private-sector hardware and software? Should the Federal government be establishing best practices or requirements for supply chain security? What role should the National Telecommunications and Information Administration play? What role should the Department of Homeland Security play? What role should the Federal Communications Commission and its Communications Security, Reliability and Interoperability Council play?

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