May 21, 2013

TELECOMMUNICATIONS NETWORKS

Addressing Potential Security Risks of Foreign-Manufactured Equipment

GAO Highlights

Highlights of GAO-13-652T, a testimony before the Subcommittee on Communications and Technology, Committee on Energy and Commerce, House of Representatives

Why GAO Did This Study

The United States is increasingly reliant on commercial communications networks for matters of national and economic security. These networks, which are primarily owned by the private sector, are highly dependent on equipment manufactured in foreign countries. Certain entities in the federal government view this dependence as an emerging threat that introduces risks to the networks. GAO was requested to review actions taken to respond to security risks from foreign-manufactured equipment.

This testimony addresses (1) how network providers and equipment manufacturers help ensure the security of foreign-manufactured equipment used in commercial communications networks, (2) how the federal government is addressing the risks of such equipment, and (3) other approaches for addressing these risks and issues related to these approaches.

This is a public version of a sensitive report that GAO issued in May 2013. Information deemed sensitive has been omitted. For the May 2013 report, GAO reviewed laws and regulations and interviewed officials from federal entities with a role in addressing cybersecurity or international trade, the five wireless and five wireline network providers with the highest revenue, and the eight manufacturers of routers and switches with the highest U.S. market shares. GAO obtained documentary and testimonial evidence from governmental entities in Australia, India, and the United Kingdom, because of their actions to protect their networks from supply chain attacks.

View GAO-13-652T. For more information, contact Mark Goldstein at (202) 512-2834 or goldsteinm@gao.gov.

What GAO Found

The network providers and equipment manufacturers GAO spoke with reported taking steps in their security plans and procurement processes to ensure the integrity of parts and equipment obtained from foreign sources. Although these companies do not consider foreign-manufactured equipment to be their most pressing security threat, their brand image and profitability depend on providing secure, reliable service. In the absence of industry or government standards on the use of this equipment, companies have adopted a range of voluntary risk-management practices. These practices span the life cycle of equipment and cover areas such as selecting vendors, establishing vendor security requirements, and testing and monitoring equipment. Equipment that is considered critical to the functioning of the network is likely to be subject to more stringent security requirements, according to these companies. In addition to these efforts, companies are collaborating on the development of industry security standards and best practices and participating in information-sharing efforts within industry and with the federal government.

The federal government has begun efforts to address the security of the supply chain for commercial networks. In 2013, the President issued an Executive Order to create a framework to reduce cyber risks to critical infrastructure. The National Institute of Standards and Technology (NIST)—a component within the Department of Commerce—is responsible for leading the development of the cybersecurity framework, which is to provide technology-neutral guidance to critical infrastructure owners and operators. NIST published a request for information in which NIST stated it is conducting a comprehensive review to obtain stakeholder input and develop the framework. NIST officials said the extent to which supply chain security of commercial communications networks will be incorporated into the framework is dependent in part on the input it receives from stakeholders. GAO identified other federal efforts that could impact communications supply chain security, but the results of those efforts were considered sensitive.

There are a variety of other approaches for addressing the potential risks posed by foreign-manufactured equipment in commercial communications networks, including those approaches taken by foreign governments. For example, the Australian government is considering a proposal to establish a risk-based regulatory framework that requires network providers to be able to demonstrate competent supervision and effective controls over their networks. The government would also have the authority to use enforcement measures to address noncompliance. In the United Kingdom, the government requires network and service providers to manage risks to network security and can impose financial penalties for serious security breaches. While these approaches are intended to improve supply chain security of communications networks, they may also create the potential for trade barriers, additional costs, and constraints on competition, which the federal government would have to take into account if it chose to pursue such approaches.