July 12, 2018

INFORMATION SECURITY

Supply Chain Risks Affecting Federal Agencies

Highlights of GAO-18-667T, a testimony before the Subcommittees on Counterterrorism and Intelligence, and Oversight and Management Efficiency, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

IT systems are essential to the operations of the federal government. The supply chain—the set of organizations, people, activities, and resources that create and move a product from suppliers to end users—for IT systems is complex and global in scope. The exploitation of vulnerabilities in the IT supply chain is a continuing threat. Federal security guidelines provide for managing the risks to the supply chain.

This testimony statement highlights information security risks associated with the supply chains used by federal agencies to procure IT systems. The statement also summarizes GAO's 2012 report that assessed the extent to which four national security-related agencies had addressed such risks. To develop this statement, GAO relied on its previous reports, as well as information provided by the national security-related agencies on their actions in response to GAO's previous recommendations. GAO also reviewed federal information security guidelines and directives.

What GAO Recommends

In its 2012 report, GAO recommended that Justice, Energy, and DHS take eight actions, as needed, to develop and document policies, procedures, and monitoring capabilities that address IT supply chain risk. The departments generally concurred with the recommendations and subsequently implemented seven recommendations and partially implemented the eighth recommendation.

View GAO-18-667T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Reliance on a global supply chain introduces multiple risks to federal information systems. Supply chain threats are present during the various phases of an information system's development life cycle and could create an unacceptable risk to federal agencies. Information technology (IT) supply chain-related threats are varied and can include:

- installation of intentionally harmful hardware or software (i.e., containing "malicious logic");
- installation of counterfeit hardware or software;
- failure or disruption in the production or distribution of critical products;
- reliance on malicious or unqualified service providers for the performance of technical services; and
- installation of hardware or software containing unintentional vulnerabilities, such as defective code.

These threats can have a range of impacts, including allowing adversaries to take control of systems or decreasing the availability of materials needed to develop systems. These threats can be introduced by exploiting vulnerabilities that could exist at multiple points in the supply chain. Examples of such vulnerabilities include the acquisition of products or parts from unauthorized distributors; inadequate testing of software updates and patches; and incomplete information on IT suppliers. Malicious actors could exploit these vulnerabilities, leading to the loss of the confidentiality, integrity, or availability of federal systems and the information they contain.

GAO reported in 2012 that the four national security-related agencies in its review—the Departments of Defense, Justice, Energy, Homeland Security (DHS)—varied in the extent to which they had addressed supply chain risks. Of the four agencies, Defense had made the most progress addressing the risks. It had defined and implemented supply chain protection controls, and initiated efforts to monitor the effectiveness of the controls. Conversely, Energy and DHS had not developed or documented policies and procedures that defined security measures for protecting against IT supply chain threats and had not developed capabilities for monitoring the implementation and effectiveness of the measures. Although Justice had defined supply chain protection measures, it also had not developed or documented procedures for implementing or monitoring the measures.

Energy and Justice fully implemented the recommendations that GAO made in its 2012 report and resolved the deficiencies that GAO had identified with their supply chain risk management efforts by 2016. DHS also fully implemented two recommendations to document policies and procedures for defining and implementing security measures to protect against supply chain threats by 2015, but could not demonstrate that it had fully implemented the recommendation to develop and implement a monitoring capability to assess the effectiveness of the security measures.