GAO

Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-361, a report to congressional requesters

March 2012

IT SUPPLY CHAIN

National Security-Related Agencies Need to Better Address Risks

Why GAO Did This Study

Federal agencies rely extensively on computerized information systems and electronic data to carry out their operations. The exploitation of information technology (IT) products and services through the global supply chain is an emerging threat that could degrade the confidentiality, integrity, and availability of critical and sensitive agency networks and data.

GAO was asked to identify (1) the key risks associated with the IT supply chains used by federal agencies; (2) the extent to which selected national security-related departments have addressed such risks; and (3) the extent to which those departments have determined that their telecommunication networks contain foreign-developed equipment, software, or services. To do this, GAO analyzed federal acquisition and information security laws, regulations, standards, and guidelines; examined departmental policies and procedures; and interviewed officials from four national security-related departments, the intelligence community, and nonfederal entities.

What GAO Recommends

GAO is recommending that the Departments of Energy, Homeland Security, and Justice take steps, as needed, to develop and document policies, procedures, and monitoring capabilities that address IT supply chain risk. These departments generally concurred with GAO's recommendations.

View GAO-12-361. 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. These risks include threats posed by actors—such as foreign intelligence services or counterfeiters—who may exploit vulnerabilities in the supply chain and thus compromise the confidentiality, integrity, or availability of an end system and the information it contains. This in turn can adversely affect an agency's ability to effectively carry out its mission. Each of the key threats presented in the table below could create an unacceptable risk to federal agencies.

Threats to the IT Supply Chain

Installation of malicious logic on hardware or software
Installation of counterfeit hardware or software
Failure or disruption in the production or distribution of a critical product or service
Reliance upon a malicious or unqualified service-provider for the performance of technical services
Installation of unintentional vulnerabilities on hardware or software

Source: GAO analysis of unclassified governmental and nongovernmental data.

Although four national security-related departments—the Departments of Energy, Homeland Security, Justice, and Defense—have acknowledged these threats, two of the departments—Energy and Homeland Security—have not yet defined supply chain protection measures for department information systems and are not in a position to have implementing procedures or monitoring capabilities to verify compliance with and effectiveness of any such measures. Justice has identified supply chain protection measures, but has not developed procedures for implementing or monitoring compliance with and effectiveness of these measures. Until comprehensive policies, procedures, and monitoring capabilities are developed, documented, and implemented, it is more likely that these national security-related departments will rely on security measures that are inadequate, ineffective, or inefficient to manage emergent information technology supply chain risks. In contrast, Defense has made greater progress through its incremental approach to supply chain risk management. The department has defined supply chain protection measures and procedures for implementing and monitoring these measures. The four national security-related departments also participate in governmentwide efforts to address supply chain security, including the development of technical and policy tools and collaboration with the intelligence community.

Officials at the four departments stated that their respective agencies have not determined or tracked the extent to which their telecommunications networks contain foreign-developed equipment, software, or services. Federal agencies are not required to track this information, and officials from four components of the U.S. national security community believe that doing so would provide minimal security value relative to cost.