G A O
Accountability * Integrity * Reliability
Highlights

Highlights of GAO-12-579T, a testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

March 27, 2012

IT SUPPLY CHAIN

Additional Efforts Needed by National Security-Related Agencies to Address Risks

Why GAO Did This Study

Information technology (IT) systems and the products and services that support them are essential to the operations of the federal government. These products and services are delivered through a complex global supply chain, and the exploitation of vulnerabilities in the IT supply chain is an emerging threat. Federal law requires establishment of information security programs, and implementing standards and guidelines provide for managing supply chain risk.

GAO was asked to testify on its recently issued report that, among other things, identified key risks associated with the supply chains used by federal agencies to procure IT equipment, software, and services, and assessed the extent to which four national security-related agencies have addressed such risks. In producing that report, 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

In its report, GAO recommended 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. In commenting on a draft of the report, the departments generally concurred with the recommendations.

View GAO-12-579T. 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 and underscores the importance of threat assessments and mitigation. Supply chain threats are present at various phases of a system's development life cycle and could create an unacceptable risk to federal agencies. Key supply chain-related threats 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 attackers to take control of systems or decreasing the availability of critical 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 acquisition of products or parts from unauthorized distributors; application of untested updates and software patches; acquisition of equipment, software, or services from suppliers without knowledge of their past performance or corporate structure; and use of insecure delivery or storage mechanisms. These vulnerabilities could by exploited by malicious actors, leading to the loss of the confidentiality, integrity, or availability of federal systems and the information they contain.

The four national security-related agencies in GAO's review—the Departments of Energy, Homeland Security, Justice, and Defense—varied in the extent to which they have addressed supply chain risks. Specifically, Energy and Homeland Security had not yet defined supply chain protection measures for department information systems and are not in a position to develop implementing procedures and monitoring capabilities. Justice has defined supply chain protection measures but has not developed implementation procedures or monitoring capabilities. Until these agencies develop comprehensive policies, procedures, and monitoring capabilities, increased risk exists that they will be vulnerable to IT supply chain threats. By contrast, the Department of Defense has made greater progress: it has defined supply chain protection measures and implementing procedures and initiated efforts to monitor compliance and effectiveness. In addition, various interagency efforts are under way to address supply chain risks affecting federal IT.