

March 2012

IT SUPPLY CHAIN

National Security- Related Agencies Need to Better Address Risks



G A O

Accountability * Integrity * Reliability

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.

IT SUPPLY CHAIN

National Security-Related Agencies Need to Better Address Risks

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.

Contents

Letter		1
	Background	3
	IT Supply Chain Presents Numerous Information Security Risks to Federal Agencies	11
	Three National Security-Related Agencies Have Not Fully Addressed IT Supply Chain Risk	17
	Agencies Have Not Determined the Extent of Foreign-Developed IT Telecommunications Equipment, Software, or Services	27
	Conclusions	28
	Recommendations for Executive Action	28
	Agency Comments and Our Evaluation	30
Appendix I	Objectives, Scope, and Methodology	33
Appendix II	Comments from the Department of Energy	36
Appendix III	Comments from the Department of Homeland Security	38
Appendix IV	GAO Contact and Staff Acknowledgments	40
Tables		
	Table 1: Threats to the IT Supply Chain	12
	Table 2: Examples of Supply Chain Vulnerabilities	16
Figure		
	Figure 1: Potential Origins of Common Suppliers for Laptop Components	5

Abbreviations

CISO	chief information security officer
CNCI	Comprehensive National Cybersecurity Initiative
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SEI	Software Engineering Institute
SP	special publication
US-CERT	U.S. Computer Emergency Readiness Team

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



G A O

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

March 23, 2012

Congressional Requesters

Information systems, as well as the products and services that support their function, are essential for government operations. Federal agencies rely extensively on computerized information systems and electronic data to carry out their operations. The security of these systems and data is essential to protecting national and economic security.

The exploitation of information technology (IT) products and services through the supply chain is an emerging threat.¹ In January 2012, the Director of National Intelligence identified the vulnerabilities associated with the IT supply chain for the nation's networks as one of the greatest strategic cyber threat challenges the country faces.² IT supply chain-related threats can be introduced in the manufacturing, assembly, and distribution of hardware, software, and services. Moreover, these threats can appear at each phase of the system development life cycle, when an agency initiates, develops, implements, maintains, and disposes of an information system. As a result, the compromise of an agency's IT supply chain can degrade the confidentiality, integrity, and availability of its critical and sensitive networks, IT-enabled equipment, and data.

Safeguarding federal computer systems is a continuing challenge. We have consistently identified significant weaknesses in the security controls for federal systems and networks and in the associated agencies' information security programs that have jeopardized the confidentiality, integrity, and availability of government information. Because of the persistent nature of these vulnerabilities and associated risks, we have

¹The National Institute of Standards and Technology (NIST) has defined the term "supply chain" to mean a set of organizations, people, activities, information, and resources for creating and moving a product or service from suppliers through to an organization's customers. Also, NIST defines "information technology" as any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes, among other things, computers, software, firmware, and services (including support services).

²Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community*, unclassified statement for the record, Senate Select Committee on Intelligence (Washington, D.C.: Jan. 31, 2012).

designated information security as a governmentwide high-risk issue since 1997 in our biennial reports to Congress.³ In addition, challenges associated with the acquisition of information systems have contributed to other high-risk designations. For example, we have identified the Department of Defense (Defense) business systems modernization and the implementation and transformation of the Department of Homeland Security (DHS) as high-risk issues, which include challenges associated with their respective systems acquisitions.⁴

Our objectives were to identify (1) the key risks associated with the supply chains used by federal agencies to procure IT equipment, software, or services;⁵ (2) the extent to which selected national security-related agencies have addressed IT supply chain risks; and (3) the extent to which national security-related federal agencies have determined that their telecommunications networks contain foreign-developed equipment, software, or services. To identify key risks, we analyzed government and nongovernment reports on IT supply chain risks. We also validated identified threats with experts from the Office of the Director of National Intelligence, the National Security Agency, the Central Intelligence Agency, and the Defense Intelligence Agency. To identify department efforts to address IT supply chain risks, we analyzed department information security policies and procedures and interviewed senior information security

³GAO's biennial high-risk list identifies government programs that have greater vulnerability to fraud, waste, abuse, and mismanagement or need transformation to address economy, efficiency, or effectiveness challenges. We have designated federal information security as a high-risk area since 1997; in 2003, we expanded this high-risk area to include protecting systems supporting our nation's critical infrastructure. See, most recently, GAO, *High-Risk Series: An Update*, [GAO-11-278](#) (Washington, D.C.: February 2011).

⁴GAO first designated Department of Defense business systems modernization as high risk in 1995 and designated implementing and transforming the Department of Homeland Security as a high-risk area in 2003.

⁵According to NIST, risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of (1) the adverse impacts that would arise if the circumstance or event occurs, and (2) the likelihood of occurrence, which is based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability. NIST defines "threat" as any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial or disruption of service. NIST also defines "vulnerability" as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat.

program officials at the Department of Energy (Energy), the Department of Justice (Justice), DHS, and Defense. These departments were selected because of their national security-related duties. To identify the extent to which the departments have identified foreign-developed equipment, software, and services, we analyzed federal statutes, regulations, and policies to determine whether any tracking requirements exist. We also interviewed agency officials regarding their current efforts to determine and track country-of-origin information for their IT equipment, software, and services. Further, we interviewed federal officials from four components of the national security community to identify potential costs and benefits associated with tracking the country of origin of IT equipment, software, or services. Additional details of our objectives, scope, and methodology are included in appendix I.

We conducted this performance audit from November 2010 to March 2012 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Information systems can be complex undertakings consisting of a multitude of pieces of equipment, software products, and service providers. Each of these components may rely on one or more supply chains. Obtaining a full understanding of the sources of a given information system during initiation and development can also be extremely complex. According to the Software Engineering Institute (SEI), the identity of each product or service provider may not be visible to others in the supply chain.⁶ Typically, an acquirer (such as a federal agency) will only know about the participants directly connected to it in the supply chain. As a result, an acquirer will have little visibility into the supply chains of its suppliers.⁷ For example, a program office at a federal

⁶Carnegie Mellon University, Software Engineering Institute, *Evaluating and Mitigating Software Supply Chain Security Risks*, CMU/SEI-2010-TN-016 (Pittsburgh, Pa.: May 2010).

⁷A supplier of information technology elements or services is also an acquirer of subelements that make up the products. Each subelement may have its own supply chain.

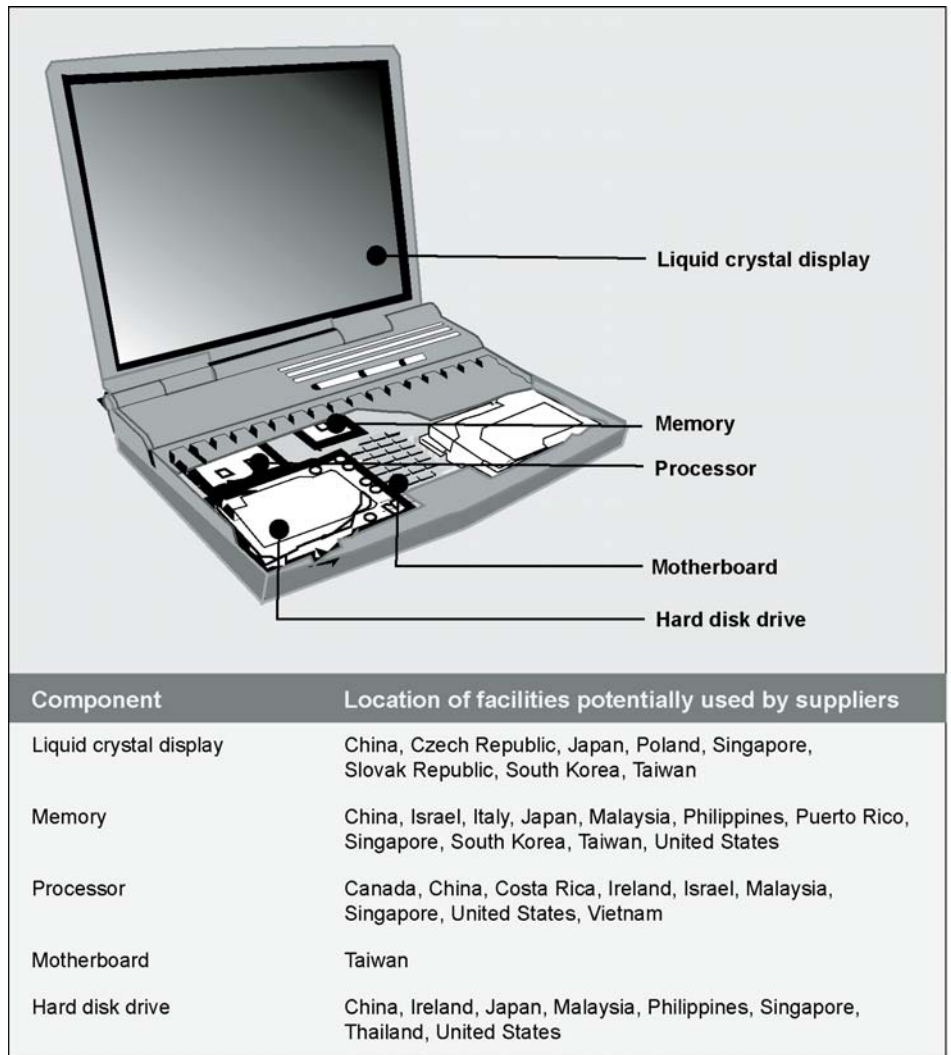
agency may rely on a prime contractor to acquire, develop, and maintain an information system. In turn, the prime contractor may obtain the equipment, software, and services that constitute the system through various means, including the

- reuse of existing equipment or legacy software;
- outsourcing of system development to an additional supplier;
- development of the capability in-house; or
- acquisition of the capability directly from a supplier or commercial off-the-shelf-vendor, or through open-source means.

In addition, the complexity of corporate structures, in which a parent company (or its subsidiaries) may own or control IT companies that conduct business under different names in multiple countries, presents additional challenges to obtaining a full understanding of the source of an information system. According to NIST, today's complex global economy and manufacturing practices make corporate ownership and control more ambiguous when assessing supply chain vulnerabilities. For example, foreign-based companies sometimes manufacture and assemble products and components in the United States, and U.S.-based companies sometimes manufacture products and components overseas, or domestically employ foreign workers.

Commercial providers of IT use a global supply chain to design, develop, manufacture, and distribute hardware and software products throughout the world. Many of the manufacturing inputs required for those products—whether physical materials or knowledge—are acquired from various sources around the globe. Figure 1 depicts the potential countries of origin of the common suppliers for various components within a commercially available computer.

Figure 1: Potential Origins of Common Suppliers for Laptop Components



Source: GAO analysis of public information.

Federal Policy Promotes the Use of Commercial IT

Federal procurement law and policies promote the acquisition of commercial products when they meet the government's needs. For example, provisions of the Federal Acquisition Streamlining Act of 1994 are designed to encourage the government to buy commercial items by (1) requiring a preference for commercial items where feasible, and (2) making exceptions to certain government requirements that previously discouraged commercial vendors from offering their products and services to the government. In addition, Office of Management and

Budget (OMB) Circular A-130 requires that agencies select investments in information technology (such as computers, software, firmware,⁸ and support services) that, among other things, make maximum use of commercial, off-the-shelf technology.⁹ OMB Circular A-130 also requires that agencies acquire off-the-shelf software from commercial sources unless developing custom software has been documented as more cost-effective.

The Comprehensive National Cybersecurity Initiative Recognizes Supply Chain Risk to Federal IT

In 2008, the Bush administration began to implement a series of initiatives, referred to as the Comprehensive National Cybersecurity Initiative (CNCI), aimed primarily at improving cybersecurity within the federal government. Specifically, CNCI is composed of a set of 12 initiatives with the objective of safeguarding federal executive branch information systems by reducing potential vulnerabilities; protecting against intrusion attempts; and anticipating future threats through defensive, offensive, educational, research and development, and counterintelligence efforts.

One of the CNCI initiatives focused on developing a multipronged approach for addressing global supply chain risk management. Specifically, the initiative stated that risks stemming from both the domestic and global supply chains must be managed in a strategic and comprehensive way over the entire life cycle of products, systems, and services. It further states that managing this risk will require

- a greater awareness of the threats, vulnerabilities, and consequences associated with acquisition decisions;
- the development and employment of tools and resources to technically and operationally mitigate risk across the life cycle of products (from design through retirement);
- the development of new acquisition policies and practices that reflect the complex global marketplace; and

⁸Firmware is defined as the combination of a hardware device and computer instructions and data that reside as read-only software on that device.

⁹OMB, *Management of Federal Information Resources*, Circular A-130 (Washington, D.C.: November 28, 2000).

-
- partnership with industry to develop and adopt supply chain risk management standards and best practices.

In March 2010, we reported on the actions that had been taken to develop interagency mechanisms to plan and coordinate CNCI activities and the challenges the CNCI faced in achieving its objectives related to securing federal information systems.¹⁰ We determined that the White House and federal agencies had taken steps to plan and coordinate CNCI activities by establishing several interagency work groups. We also determined that the CNCI faced several challenges in meeting its objectives, including defining roles and responsibilities, establishing measures of effectiveness, and establishing an appropriate level of transparency (including for supply chain risk management activities). We made six recommendations to OMB to address the identified challenges. OMB concurred with five of our six recommendations and has since taken steps to address most of these challenges, including clarifying cybersecurity responsibilities and activities among federal entities.

Federal Law Requires Agencies to Establish Information Security Programs, and Implementing Standards and Guidelines Provide for Management of Supply Chain-Related Risk

The Federal Information Security Management Act of 2002 (FISMA) establishes federal agency information security program requirements that support the effectiveness of information security controls over information resources that support federal operations and assets.¹¹ Its framework creates a cycle of risk management activities necessary for an effective security program. FISMA requires every federal agency to establish an information security program. Additionally, the act assigns responsibility to NIST to provide standards and guidelines to agencies on information security.¹²

FISMA directed NIST to promulgate federal standards for (1) the security categorization of federal information and information systems based on the objective of providing appropriate levels of information security

¹⁰GAO, *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, [GAO-10-338](#) (Washington, D.C.: Mar. 5, 2010).

¹¹Title III of the E-Government Act of 2002, Pub. L. No. 107-347, Dec. 17, 2002.

¹²FISMA requires that federal agencies comply with NIST information security standards, and agencies may not waive their use. In addition, FISMA requires agencies to develop, document, and implement agencywide programs to provide security for the information systems that support their operations and assets.

according to a range of risk levels, and (2) minimum security requirements for information and information systems in each such category. NIST subsequently issued two Federal Information Processing Standards (FIPS):

- FIPS 199 is to be used to categorize information and information systems, thereby providing a common framework for expressing security.¹³ Under this standard, a system is categorized (high, moderate, or low¹⁴) based on the type of impact that would result from a loss of confidentiality, integrity, or availability.
- FIPS 200 addresses the specification of minimum security requirements for federal information and information systems.¹⁵ In particular, FIPS 200 directs federal agencies to meet the minimum security requirements through the use of the security controls in accordance with NIST Special Publication 800-53 (SP 800-53).¹⁶

NIST issued SP 800-53 to provide a catalog of security controls and technical guidelines that federal agencies use to protect federal information and information systems. After conducting the security categorization process established by FIPS 199, organizations are required to select an appropriately tailored set of initial security controls consistent with the baselines in SP 800-53. In August 2009, NIST published SP 800-53, Revision 3, which, for the first time, included a security control for supply chain protection (SA-12).¹⁷ As part of SA-12,

¹³NIST, *Federal Information Processing Standards (FIPS) Publication 199: Standards for Security Categorization of Federal Information and Information Systems* (Gaithersburg, Md.: February 2004).

¹⁴NIST defines “high,” “moderate,” and “low impact” with respect to consequences of loss of confidentiality, integrity or availability. Thus, high, moderate, and low impact correspond, respectively; to catastrophic, serious, or limited adverse effect on organizational operations, organizational assets, or individuals.

¹⁵NIST, *FIPS Publication 200: Minimum Security Requirements for Federal Information and Information Systems* (Gaithersburg, Md.: March 2006).

¹⁶NIST, *Recommended Security Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 3 (Gaithersburg, Md.: May 2010).

¹⁷SA-12 states that an organization should define and employ a list of measures to protect against supply chain threats as part of a comprehensive, defense-in-breadth information security strategy. According to SP 800-53, Revision 3, SA-12 should be selected for the initial control baseline of all agency information systems categorized as high impact.

NIST identified several specific measures that organizations could use to provide additional supply chain protections. These include, but are not limited to,

- conducting a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services;
- using trusted shipping and warehousing for information systems, information system components, and information technology products; and
- employing independent analysis and penetration testing against delivered information systems, information system components, and information technology products.¹⁸

SP 800-53, Revision 3, also includes a security control for system and services acquisition policy and procedures (SA-1).¹⁹ Thus, for systems where both controls are selected, agencies should develop, disseminate, and review acquisition policy and implementing procedures that help protect against supply chain threats throughout the system development life cycle.

Other policy requires SP 800-53 controls to be selected for both non-national security and national security systems. Specifically, OMB Circular A-130 states that federal agencies are required to use SP 800-53 in selecting and specifying controls for non-national security programs. Also, in October 2009, the Committee on National Security Systems published Instruction 1253,²⁰ which establishes SP 800-53 as a common

¹⁸NIST defines “penetration testing” as security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network.

¹⁹SA-1 states that organizations should develop formal, documented procedures to facilitate the implementation of system and services acquisition policy and associated system and services acquisition family of controls, which includes SA-12. According to SP 800-53, Revision 3, SA-1 should be selected for the initial control baseline regardless of categorization.

²⁰The Committee on National Security Systems was established by National Security Directive 42 to, among other things, issue policy directives and instructions that provide mandatory information security requirements for national security systems. The committee is chaired by the Department of Defense.

foundation for information security controls for national security systems.²¹ Under this instruction, all national security systems are directed to select SA-1 as part of their initial control baselines. Further, all national security systems that are categorized as high or moderate impact for integrity are directed to select SA-12 as part of their initial control baselines.²²

In March 2011, NIST published SP 800-39, which provides an approach for organizationwide management of information security risk, including those related to supply chains.²³ Among other things, the publication states that risk management requires organizations to monitor risk on an ongoing basis as part of a comprehensive risk management program. Monitoring programs can aid agency officials in oversight of currently implemented security controls. To support risk monitoring, organizations are expected to describe how compliance with security requirements is verified and how the organization will determine the effectiveness of risk response activities.

In addition, the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 included provisions related to supply chain security. Specifically, Section 806 authorizes the Secretaries of Defense, the Army, the Navy, and the Air Force to exclude a contractor from specified types of procurements on the basis of a determination of significant supply chain risk to a covered system.²⁴ Section 806 also establishes requirements for limiting disclosure of the basis of such procurement action.

²¹The Committee on National Security Systems Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, October 2009.

²²The impact level for a national security system is determined using the Committee on National Security Systems Instruction 1253 instead of FIPS 199. The instruction uses a more granular structure in which the potential impact levels of loss of confidentiality, integrity, and availability are individually used to select categorization.

²³NIST, *Managing Information Security Risk: Organization, Mission, and Information System View*, SP 800-39 (Gaithersburg, Md.: March 2011).

²⁴The act defines “supply chain risk” as “risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.”

NIST Plans to Issue Further Guidance on IT Supply Chain Practices

In June 2010, NIST released a draft interagency report, *Piloting Supply Chain Risk Management Practices for Federal Information Systems*,²⁵ which, when finalized and published, is intended to provide agencies with supply chain risk mitigation strategies integrated with the information systems development life cycle. Its methodology for handling supply chain risk included, among other things, determining which procurements should consider supply chain risk, working with agency stakeholders to help mitigate supply chain risk, and describing roles and responsibilities within the agency. NIST plans to release the final version of the report by the end of fiscal year 2012.

In February 2012, NIST released for comment the initial public draft of SP 800-53, Revision 4, which, when finalized and published, is intended to provide, among other things, additional supply chain-related guidance and protection measures.²⁶ The draft revised SA-12 guidance and incorporated supply chain considerations into, among other things, security measures related to incident handling and reporting. NIST anticipates the publication of the final document in July 2012.

IT Supply Chain Presents Numerous Information Security Risks to Federal Agencies

Reliance on a global supply chain introduces multiple risks to federal information systems and underscores the importance of threat assessments and risk mitigation. These risks include threats posed by actors—such as foreign intelligence services or counterfeiters—who may exploit vulnerabilities in the supply chain, thus compromising the confidentiality, integrity, or availability of the end-system and the information it contains.²⁷ This in turn can adversely affect an agency's ability to carry out its mission.

The IT Supply Chain Faces Threats

Supply chain-related threats are present at various phases of the system development life cycle. Each of the key threats presented in table 1 could create an unacceptable risk to federal agencies.

²⁵NIST, *Piloting Supply Chain Risk Management Practices for Federal Information Systems*, Draft NISTIR 7622 (Gaithersburg, Md.: June 2010).

²⁶NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, Draft SP 800-53, Revision 4 (Gaithersburg, Md.: February 2012).

²⁷Supply chain-related threat actors include corporate spies, corrupt government officials, cyber vandals, disgruntled employees, foreign military, government agents or spies, radical activists, purveyors of counterfeit goods, or criminals.

Installation of Hardware or Software Containing Malicious Logic

Table 1: Threats to the IT Supply Chain

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

Source: GAO analysis of unclassified governmental and nongovernmental data.

Threat actors can use the supply chain to insert hardware or software containing malicious logic through tampering during the development and implementation of an information system. Malicious logic is hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. For example, viruses and Trojan horses are two forms of malicious logic that could be included in a system via the supply chain. A virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user. A Trojan horse is a computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Malicious logic can cause significant damage by allowing attackers to take control of entire systems and thereby read, modify, or delete sensitive information; disrupt operations; launch attacks against other organizations' systems; or destroy systems.²⁸ For example, it was reported in 2008 that hardware similar to flash memory drives that was released by a major U.S. electronics manufacturer contained malicious code that could allow an attacker to take over an infected system.²⁹ Additionally, recent information reported by DHS indicates that malicious

²⁸GAO, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, [GAO-08-588](#) (Washington, D.C.: July 31, 2008).

²⁹Hewlett-Packard (HP) Company, HP Software Security Response Team, *HP Support Document: Support Communications—Security Bulletin, HP USB Floppy Drive Key (Option) for ProLiant Servers, Local Virus Infection*, April 3, 2008, <http://bizsupport1.austin.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01404119>, accessed March 21, 2012; and Liam Tung, "HP Ships USB Sticks with Malware," *CNET News*, April 9, 2008. http://news.cnet.com/HP-ships-USB-sticks-with-malware/2100-7349_3-6236976.html, accessed January 3, 2012.

Installation of Counterfeit Hardware or Software

code attacks are prevalent in the federal environment. Specifically, according to the United States Computer Emergency Readiness Team (US-CERT), approximately 27 percent of the 42,854 agency-reported security incidents during fiscal year 2011 involved malicious code.³⁰ Although not necessarily the result of an IT supply chain attack, these incidents highlight the impact that such attacks could have on agency operations.

Counterfeit information technology is hardware or software that contains nongenuine component parts or code. A component is not genuine if it (1) is an unauthorized copy; (2) does not conform to the design, model, or performance standards as prescribed by the original component manufacturer; (3) is not produced by the original component manufacturer or is produced by an unauthorized contractor; (4) is an off-specification, defective, or used original component manufacturer product sold as “new” or working; or (5) has incorrect or false markings or documentation.

The Defense Department’s Information Assurance Technology Analysis Center has reported that counterfeit information technology threatens the integrity, trustworthiness, and reliability of information systems for several reasons, including the facts that (1) counterfeits are usually less reliable and therefore fail more often and more quickly than genuine parts, and (2) counterfeiting presents an opportunity for the counterfeiter to insert malicious logic or backdoors³¹ into the replicas or copies that would be far more difficult in more secure manufacturing facilities.³² Federal agencies have unintentionally purchased counterfeit IT products. For example, according to a Cisco report about the counterfeiting of its products, one case involved the illegal modification of routers with fake seals and Cisco

³⁰The United States Computer Emergency Readiness Team (US-CERT) is the operational arm of the National Cyber Security Division at DHS and is tasked with protecting the nation’s information infrastructure by coordinating defense against and response to cyber attacks.

³¹A “backdoor” is a general term for a malicious program that can potentially give an intruder remote access to an infected computer. At a minimum, most backdoors allow an attacker to perform a certain set of actions on a system, such as transferring files or acquiring passwords.

³²Information Assurance Technology Analysis Center, *Security Risk Management for the Off-the-Shelf (OTS) Information and Communications Technology (ICT) Supply Chain An Information Assurance Technology Analysis Center (IATAC) State-of-the-Art Report*, DO 380 (Herndon, Va.: August 2010).

Failure or Disruption in the
Production or Distribution of
Critical Products

tape to appear as if they contained security protections of a model valued at twice as much as a standard version. These routers were then purchased by a reseller and sold to the federal government through an official government solicitation for purchase. Additionally, according to the United States Attorney's Office for the Southern District of Texas, the Marine Corps, Air Force, Federal Aviation Administration, and Federal Bureau of Investigation (FBI) allegedly purchased counterfeit Cisco products that had originated in China.³³ As a result, these agencies were at increased risk of installing products that were less reliable or secure than authentic IT equipment.

Failure or disruption in the production or distribution of a critical product could affect the availability of information technology equipment that is used to support federal information systems. Both man-made (e.g., disruptions caused by labor or political disputes) and natural causes (e.g., earthquakes, fires, floods, or hurricanes) could disrupt the supply of IT products critical to the operations of federal agencies. For example, following a severe Japanese earthquake in March 2011, it was reported that damage to Japan's semiconductor industry could affect the availability of computer memory on the global market, because approximately 40 percent of certain types of computer memory is manufactured in Japan.³⁴ In addition, according to the U.S.-China Economic and Security Commission, rare earth elements are a collection of 17 elements that are critical to commercial and military high-technology applications.³⁵ These elements are distributed globally, with China reportedly producing approximately 97 percent of the current world supply. As a result, a disruption in the supply chain for rare earth

³³The United States Attorney's Office, Southern District of Texas. *Two Charged with Selling Counterfeit Computer Products*, January 4, 2008. www.cybercrime.gov/edmanCharge.pdf, accessed January 31, 2012. The defendants in this investigation pleaded guilty to selling counterfeit Cisco products to the Federal Bureau of Prisons.

³⁴Jim Handy, "Significant Potential Problems in Semiconductors," *Objective Analysis* (March 11, 2011), http://www.objective-analysis.com/uploads/2011-03-11_Major_Earthquake_Hits_Japan.pdf, accessed January 4, 2012.

³⁵Rare earth elements can be used in a variety of commercial information technology equipment, such as cell phones and computer hard drives. Further, these elements are also critical to the development of sophisticated military applications, such as guidance and control systems and advanced communications systems.

Reliance on a Malicious or Unqualified Service Provider for the Performance of Technical Services

elements could reduce the availability of material necessary for the U.S. government to develop systems.

Contractors and other service providers may, by virtue of their position, have access to federal data and systems. As we have previously reported, service providers could attempt to use their access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.³⁶ We have also reported that the FBI has identified multiple sources of threats, such as foreign entities engaged in intelligence gathering and information warfare, criminals, and disgruntled employees or contractors working within an organization.³⁷ As an example of this type of threat, according to a United States Attorney's Office press release, a contract programmer was charged with stealing software code from the Federal Reserve Bank of New York.³⁸ Further, an FBI official alleged that this individual took advantage of the access associated with his position in order to steal highly sensitive source code.

Installation of Hardware or Software That Contains Unintentional Vulnerabilities

Unintentional vulnerabilities are hardware, software, or firmware that are included or inserted in a system and that inadvertently present opportunities for compromise. It has been reported that attackers focus their efforts on, among other things, finding and exploiting existing defects—such as buffer overflows—in the code, which are usually the result of unintentional coding errors.³⁹ For example, DHS recently released an alert that identified vulnerabilities in certain firmware used by

³⁶GAO, *Information Security: IRS Needs to Enhance Internal Control over Financial Reporting and Taxpayer Data*, [GAO-11-308](#) (Washington, D.C.: Mar. 15, 2011).

³⁷GAO, *Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk*, [GAO-09-661T](#) (Washington, D.C.: May 5, 2009).

³⁸Department of Justice, *Manhattan U.S. Attorney and FBI Assistant Director-In-Charge Announce Arrest of Computer Programmer For Stealing Proprietary Code From the Federal Reserve Bank of New York* (January 18, 2012), <http://www.justice.gov/usao/nys/pressreleases/January12/zhangboarrestpr.pdf>, accessed February 6, 2012.

³⁹Stacey Simpson, ed., *Software Assurance Forum for Excellence in Code (SAFECode), Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain* (June 14, 2010).

industrial control systems.⁴⁰ The vulnerabilities identified could allow remote attackers to, among other things, cause a denial of service.⁴¹

Vulnerabilities in Acquisition or Information Security Controls Are Exploitable

The threats described above can pose risk to federal information systems. Specifically, threat actors can introduce the above-mentioned threats by exploiting vulnerabilities that could exist at multiple points in the global supply chain. In addition, supply chain vulnerabilities can include weaknesses in agency acquisition or information security procedures, controls, or implementation related to a federal information system. If a threat actor exploits an existing vulnerability, it could lead to the loss of confidentiality, integrity, or availability of the end-system and associated information. Table 2 describes examples of the types of vulnerabilities that could be exploited.

Table 2: Examples of Supply Chain Vulnerabilities

Vulnerability	Description	Threat example
Acquisition of information technology products or parts from independent distributors, brokers, or the gray market	Purchasing from a source other than an original component manufacturer or authorized reseller may increase an agency's risk of encountering substandard, subverted, and counterfeit products. Independent distributors purchase new parts with the intention to sell and redistribute them back into the market, without having a contractual agreement with the original component manufacturer. Brokers are a type of independent distributor that work in a just-in-time inventory environment and search the industry and locate parts for customers as requested. The gray market refers to the trade of parts through distribution channels that, while legal, are unofficial, unauthorized, or unintended by the original component manufacturer.	Installation of counterfeit hardware or software

⁴⁰DHS, Industrial Control Systems Alert 11-346-01, "Schneider Electric Quantum Ethernet Module Multiple Vulnerabilities," December 12, 2011, https://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-346-01.pdf, accessed February 6, 2012. Control systems are computer-based systems that monitor and control sensitive processes and physical functions and perform vital functions in many of our nation's critical infrastructures, including electric power, oil and gas, water treatment, and chemical production.

⁴¹A denial of service is a method of attack from a single source that denies system access to legitimate users by overwhelming the target computer with messages and blocking legitimate traffic. It can prevent a system from being able to exchange data with other systems or use the Internet.

Vulnerability	Description	Threat example
Lack of adequate testing for software updates and patches	Applying untested updates and patches to information system components may increase an agency's risk that an attacker could insert malicious code of its choosing into a system. For example, if an agency or contractor fails to validate the authenticity of patches with suppliers, an attacker could write a fake patch that might allow unauthorized access to information in the system.	Installation of hardware or software containing malicious logic
Incomplete information on IT suppliers	Acquiring IT equipment, software, or services from suppliers without understanding the supplier's past performance or corporate structure may increase the risk of (1) encountering substandard, subverted, and counterfeit products, or (2) providing adversaries of the United States with access to sensitive agency systems or information. For example, lacking information concerning an IT service provider's corporate structure could reduce an agency's ability to assess whether or not the service provider or its employees are subject to undue foreign control or influence.	<p>Installation of hardware or software containing malicious logic</p> <p>Installation of hardware or software that contains unintentional vulnerabilities</p> <p>Installation of counterfeit hardware or software</p> <p>Failure or disruption in the production or distribution of critical products</p> <p>Reliance on a malicious or unqualified service provider for the performance of technical services</p>
Use of supply chain delivery and storage mechanisms that are not secure	Using delivery or storage mechanisms that are not secure may increase the risk that an IT product is intercepted or subverted while it is in transit to the agency or while it is in storage before installation. This vulnerability may allow a threat actor to gain unauthorized access to the IT product, thereby facilitating unauthorized modification, substitution, or diversion. Unsecured delivery and storage mechanisms may also lead to the exposure of sensitive information to unauthorized parties, such as the identity of the agency purchasing the IT product or how the IT product will be used.	<p>Installation of hardware or software containing malicious logic</p> <p>Failure or disruption in the production or distribution of critical products</p> <p>Installation of counterfeit hardware or software</p>

Source: GAO analysis of unclassified governmental and nongovernmental data.

Three National Security-Related Agencies Have Not Fully Addressed IT Supply Chain Risk

Although the four agencies in our review have acknowledged the risks presented by supply chain vulnerabilities, two of the agencies—Energy and DHS—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 the effectiveness of these measures. In contrast, Defense has made greater progress through its incremental approach to supply chain risk management. Specifically, it has defined supply chain protection measures and implementing procedures, and plans to develop outcome-based performance measures as the agency's supply chain risk management capabilities mature.

According to the NIST SP 800-53 control for supply chain protection, agencies should define which security measures, if any, should be employed to protect against supply chain threats. In addition, the NIST SP 800-53 control for system and service acquisition calls for agencies to develop, document, and disseminate procedures to ensure the effective implementation of these measures. These procedures can be developed for the agency's security program in general, or for a particular information system when required. Finally, according to NIST SP 800-39, agencies should also implement monitoring mechanisms to verify compliance with, and determine the effectiveness of, established security controls and associated supply chain protection measures.

Energy Lacks IT Supply Chain Measures, Documented Procedures, and Monitoring Capabilities

Energy has not defined security measures that information system owners should employ to protect against supply chain threats. In May 2011, the department revised its information security program, which sets forth requirements and responsibilities to protect departmental information and information systems. The program document requires Energy components to implement its provisions based on requirements and guidance defined by NIST and the Committee on National Security Systems, which includes the IT supply chain protection control. According to Energy's chief information security officer (CISO), the department is in the process of implementing the program, and a large percentage of the department will be covered by the end of fiscal year 2012. However, the department was unable to provide details on implementation progress, milestones for completion, or how supply chain protection measures would be defined.

Additionally, without defined supply chain security measures, Energy is not in a position to develop, document, and disseminate procedures to ensure the effective implementation of supply chain protection. The development of implementation procedures relies on the department defining its supply chain security measures.

Further, Energy is not in a position to implement a monitoring capability to verify compliance with, and determine the effectiveness of, any such protections. The department's information security program does describe high-level efforts to monitor risks to Energy information systems. However, it does not specify any monitoring or compliance efforts related to IT supply chain measures because Energy has not yet defined what supply chain measures will be employed by system owners.

Until Energy ensures that IT supply chain protection measures and implementing procedures are developed, documented, and disseminated, officials will be without essential guidance that facilitates the effective and consistent implementation of supply chain protection on departmental information systems. Further, senior Energy leadership will not have an effective monitoring capability to provide them with the information necessary to make informed decisions on supply chain protection activities. Implementing a monitoring capability for any supply chain security measures can help ensure that measures are adequate in the face of changes in threats, departmental operations, or level of compliance.

DHS Lacks IT Supply Chain Measures, Documented Procedures, and Monitoring Capabilities

Although its information security guidance mentions the SP 800-53 control related to supply chain protection, DHS has not defined the measures that system owners should employ. Under DHS's information security program, the department's CISO is responsible for issuing departmentwide information security policy that incorporates NIST guidelines and applicable OMB memorandums and circulars for all DHS systems and networks. The department's information security policy manager stated that DHS had not addressed IT supply chain security through its policy. The official stated that DHS is currently in the process of developing such policy, but provided no details on when it would be completed.

Additionally, in the absence of defined supply chain security measures, DHS is not in a position to develop, document, or disseminate procedures to ensure the effective implementation of supply chain protection. DHS issued a handbook to provide specific techniques and procedures for implementing the department's information security policy; however, it does not include any supply chain-related implementation guidance. This is due to the fact that the department has not yet defined what supply chain measures will be employed by system owners.

The department also is not in a position to implement a monitoring mechanism to assess the compliance with and effectiveness of IT supply chain security measures. DHS's information security policy does describe high-level monitoring for compliance and effectiveness of its information security program, including its components performing assessments against the controls identified in NIST SP 800-53. However, the policy does not specify any monitoring or compliance efforts related to IT supply chain measures, because the department has not yet defined what supply chain measures will be employed by system owners.

Until DHS updates its information security policy to ensure that IT supply chain protection measures and implementing procedures are developed and documented, officials will be without essential guidance that is required to effectively implement supply chain protection on departmental information systems. Further, senior DHS leadership will not have an effective monitoring capability that provides the information that is necessary to make informed decisions on supply chain protection activities. Implementing a monitoring capability for any supply chain security measures can help ensure that measures are adequate in the face of changes in threats, departmental operations, or level of compliance.

Justice Has Defined Supply Chain Measures, but Lacks Documented Procedures and Monitoring Capabilities

Justice has defined specific security measures that information system owners should employ to protect against supply chain threats. The department's minimum security control requirements specify that supply chain protection for high-impact systems is to be provided through the use of vendor acquisition contracts and agreements. In particular, Justice officials identified two generic contract provisions that could be used to address supply chain threats: (1) a citizenship and residency requirement and (2) a national security risk questionnaire (including a Foreign Ownership Control and Influence review).

However, Justice has not developed, documented, and disseminated procedures to ensure the effective implementation of these supply chain protection measures. Specifically, Justice officials were not able to identify which acquisitions would need to have the provisions inserted. Although the Justice CISO stated that the agency would require a national security risk questionnaire based on a national security and departmental mission impact determination, Justice officials could not identify documented criteria that would help security officers and other officials make this determination.

Further, Justice has not implemented a monitoring mechanism to verify compliance with, and determine the effectiveness of, its supply chain security measures. Justice's CISO stated that the department did not have a system to track the use and effectiveness of the contract provisions across all components. As a result, departmental officials were not able to identify the frequency with which the provisions had been inserted into contracts for IT equipment, software, or services. In addition, Justice officials stated that the results of the Foreign Ownership Control and Influence reviews conducted under the provisions were generally kept with the program offices and acquisitions officials. Justice's CISO

stated that one reason for not monitoring is that the department is waiting for CNCI initiative 11 and the Committee on National Security Systems to produce guidance related to monitoring supply chain risk.

Until the department develops, documents, and disseminates procedures to implement its policy on IT supply chain protection, and implements a process to monitor that policy, Justice officials have limited assurance that departmental information systems are being adequately protected against supply chain threats.

Defense Has Issued, and Monitors Compliance with, Supply Chain Measures and Implementation Procedures

Defense's supply chain risk management efforts began in 2003 and include multiple policies that specify measures to be employed for supply chain protection.⁴² For example, in February 2009, the department issued policy that requires that supply chain risk be addressed early and across the entire system life cycle.⁴³ This policy applies to those systems that handle information that the agency determines is critical—in terms of both content and timeliness—to the readiness or effectiveness of the armed forces. The policy calls for the incremental implementation of supply chain risk management through a series of pilot projects. According to the policy, the target date for achieving full operational capability for supply chain risk management is fiscal year 2016. An official from Trusted Mission Systems and Networks, an office within the Defense Office of the Chief Information Officer, stated that lessons learned from the pilots should aid in the implementation of supply chain protection throughout the system development life cycle in a manner that enables systems to meet departmental cost, schedule, and performance requirements.⁴⁴

⁴²FISMA permits an agency to use more stringent information security standards if it certifies that its standards are at least as stringent as the NIST standards and are otherwise consistent with policies and guidelines issued under FISMA.

⁴³Defense subsequently reissued the policy and extended it through March 2012. Directive-Type Memorandum 09-016, *Supply Chain Risk Management to Improve the Integrity of Components Used in DoD Systems* (March 10, 2010).

⁴⁴Trusted Mission Systems and Networks is the Defense organization that is responsible for, among other things, leading the department's supply chain risk management pilot effort, providing required quarterly and final reports for CNCI Initiative 11, and developing and updating the supply chain risk management Pilot Program Key Practices and Implementation Guide and Concept of Operations.

In addition, the 2009 policy states that the supply chain pilots shall include, among other things,

- processes to assess threats from potential suppliers providing critical components to applicable systems;
- processes to detect the occurrence, reduce the likelihood of occurrence, and mitigate the consequences of products containing counterfeit components or malicious functions; and
- enhanced developmental and operational test and evaluation capabilities, including software vulnerability detection methods and automated tools.

In addition, a July 2011 memorandum, which was issued by the Principal Deputy Under Secretary of Defense for Acquisition, Technology, and Logistics, requires every acquisition program to submit and update a “program protection plan” at each milestone of Defense’s system acquisition process. Among other things, program protection is intended to be the integrating process for managing risks to advanced technology and mission-critical system functionality from supply chain exploits or design vulnerabilities throughout the acquisition life cycle.

Defense has developed, documented, and disseminated procedures to facilitate the effective incremental implementation of supply chain protection measures. In February 2010, the department released a supply chain risk management *Key Practices and Implementation Guide*, which describes 32 specific measures that an organization could take to enhance supply chain protection. Examples of these measures include

- maximizing visibility into suppliers;
- choosing programming languages, subsets, and tools that counter weaknesses; and
- reducing supply chain risks during software updates and patch management.⁴⁵

⁴⁵Defense released a previous version of the guide in 2009.

Defense has also developed, documented, and disseminated procedures related to program protection plans. According to these procedures, program protection plans should guide a program office's security measures, and should be updated as threats and vulnerabilities change or are better understood. The procedures identify at least four ways in which Defense programs should manage supply chain risk. Specifically, the procedures recommend that program officials

- identify critical program information, critical functions, and components;⁴⁶
- document how supply chain threat assessments will be used to influence system design, development environment, and procurement practices;
- assess the need for trusted suppliers for integrated circuits; and
- identify specific counterfeit protection measures.

Defense has also implemented a monitoring mechanism to determine the status and effectiveness of its supply chain protection pilots. Trusted Mission Systems and Networks is responsible for collecting supply chain risk management data and metrics on pilot efforts and reporting the results of the pilots conducted between 2009 and 2010. For example, this office issued a limited release report, dated April 2011, that described the findings and lessons learned related to supply chain protection. According to the report, this information was based on data collected from the 2010 supply chain pilots conducted in fiscal years 2009 and 2010. An official within Trusted Mission Systems and Networks stated that the office has continued to provide quarterly reports on the status and lessons learned from ongoing pilot activities.

In addition, Defense has monitored compliance with, and the effectiveness of, program protection policy and procedures for several acquisition programs. According to the Deputy Director for Program Protection, Office

⁴⁶Defense defines "critical program information" as elements or components of a research, development, and acquisition program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability.

of the Under Secretary of Defense for Acquisition, Technology, and Logistics, the office has conducted six milestone reviews since July 2011.⁴⁷ We observed evidence that, for four of the milestone reviews, appropriate Defense officials had verified whether or not the acquisition program had complied with the July 2011 memo and procedures related to program protection planning. For example, the documentation associated with one review conditioned approval on program officials completing an analysis to identify critical components and information within 180 days of the milestone review decision. Regarding the two remaining programs, Defense Systems Engineering officials documented deficiencies in the program protection plan for one of the programs, and, according to the Deputy Director for Program Protection, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, these deficiencies were communicated to senior officials prior to the milestone review decision. The remaining program was not approved for continued development.

According to Trusted Mission Systems and Networks officials, the department is collecting metrics to assess the effectiveness of the supply chain risk management aspects of protection planning. Specifically, officials stated that the department is currently collecting data concerning the extent to which the department has engaged with program managers to understand supply chain threats, conducted criticality analyses to identify critical functions, and developed appropriate countermeasures and mitigations. According to an official within Trusted Mission Systems and Networks, the department had conducted 63 such engagements during fiscal year 2011.

National Security-Related Agencies Participate in Governmentwide Efforts to Address Supply Chain Security

The four national security-related agencies also participate in interagency efforts to address supply chain security. These include participation in the CNCI, development of technical and policy tools, and collaboration with the intelligence community.

In support of the CNCI, Defense and DHS jointly lead an interagency initiative on supply chain risk management to address issues of globalization affecting the federal government's IT. Defense's pilot program is intended to provide a basis for supply chain risk management

⁴⁷A milestone decision can be defined as a point at which a recommendation is made and approval is sought regarding starting or continuing an acquisition program (i.e., proceeding to the next phase).

policy recommendations to other federal agencies. In April 2011, Defense reported conducting supply chain risk management pilots and developed findings related to the need for (1) effective staffing and funding of supply chain risk management activities, (2) enterprise governance of supply chain risk management issues and mitigations, (3) processes and procedures to enhance trust and reduce risk in IT, (4) legal and contractual methods—including new legislation—to avoid using those suppliers determined to present elevated supply chain risk, and (5) revised agency policy to address supply chain risk management.

Additionally, DHS has developed a comprehensive portfolio of technical and policy-based product offerings for federal civilian departments and agencies. These services are incorporated into the set of capabilities offered by DHS's National Cyber Security Division's Supply Chain Risk Management Program, including technical assessment capabilities, acquisition support, and incident response capabilities. These services include the following:

- **Technical risk assessments:** A comprehensive set of technical risk assessment capabilities that includes destructive and nondestructive analysis, code review and assessment, development of attack graphs, vulnerability assessments, and mitigation recommendations.
- **Acquisition threat and risk assessments:** Department and agency program managers can submit system acquisition requirements for review and comment and will receive vendor risk assessment reports on vendors competing for the acquisition and potential mitigations for any identified risk.
- **Incident response and supply chain risk management analysis:** The Supply Chain Risk Management Program has been working in cooperation with US-CERT to develop integrated analysis and response capabilities for supply chain incidents into its existing missions.
- **DHS supply chain risk management product offerings:** Operational activities to support federal civilian department and agency efforts to manage information technology supply chain risk. These include assessment of agencies' supply chain risk management capabilities and support of ongoing or future acquisitions, as well as technical analysis of hardware and software.

Additionally, in March 2012, the Committee on National Security Systems issued a directive that directs agencies with national security systems to implement a supply chain risk management program.⁴⁸ The directive lists available best practices, tools, and resources, including those developed under CNCI efforts and Defense's supply chain pilots. According to Defense and DHS officials, departments and agencies from Defense, the intelligence community, and the civilian agencies collaborated in developing this directive.

Further, Energy, DHS, Defense, and a component of Justice—the FBI—have contributed, to varying degrees, to the development of a common methodology for conducting threat assessments on entities that do business with the national security community. Under this initiative, which is led by the Office of the National Counterintelligence Executive,⁴⁹ agencies are requested to provide copies of threat assessments to a centrally maintained database where they are stored for future use by components of the national security community. In addition, officials from Energy, DHS, Defense, and the FBI stated that they have, or have had, agency officials assigned to the office to facilitate threat information sharing. According to National Counterintelligence Executive officials, the four national security-related agencies have contributed 40 percent of the threat assessments available since 2009. Specifically, Energy has contributed 1 percent, DHS has contributed 4 percent, FBI has contributed 9 percent, and Defense or its components have contributed 26 percent of the threat assessments. Officials further stated that the vast majority of these assessments relate to firms within the IT industry, and the remainder relate to Defense weapons systems.

⁴⁸Committee on National Security Systems, Directive 505, *Supply Chain Risk Management* (Mar. 7, 2012).

⁴⁹Formerly an independent agency, the Office of the National Counterintelligence Executive is now a component of the Office of the Director of National Intelligence. The duties of the National Counterintelligence Executive are set forth in part in the Counterintelligence Enhancement Act of 2002. One of these duties is to act in coordination with other agencies to assess the vulnerabilities of the U.S. government, as well as the private sector, to intelligence threats in order to identify the areas, programs, and activities that require protection from such threats.

Agencies Have Not Determined the Extent of Foreign-Developed IT Telecommunications Equipment, Software, or Services

Officials within the offices of the chief information officer at the Departments of Energy, Homeland Security, and Defense, and the Justice Management Division stated that their respective agencies have not determined and do not currently track the extent to which their telecommunications networks contain foreign-developed equipment, software, or services.

Federal law and regulation do not require federal agencies to track the country of origin of the telecommunications equipment, software, and services that they procure. Although a number of federal laws authorize a preference for American supplies or end products, these laws are of limited use for enhancing information assurance. For example, the Buy American Act, which is designed to promote national commerce and industry, generally (1) restricts federal agencies' purchase of nondomestic ("foreign") manufactured products, and (2) requires that each federal agency report to Congress annually for fiscal years 2009-2011 on the amount of acquisitions it made from entities that manufactured end products outside the United States. Under the act, however, an end product can be considered domestic even if it contains foreign components. Moreover, as implemented, the act does not apply to the acquisition of commercial IT products, which means that the government may purchase commercial IT without regard to the Buy American Act and its reporting requirements. Similarly, the Berry Amendment, which requires domestic sourcing by Defense of specialty metals, also has limited value for IT assurance. Specifically, the Berry Amendment does not apply to either electronic components or commercially available off-the-shelf items containing specialty metals.⁵⁰

In addition, federal officials from four components of the national security community provided reasons why the cost of tracking IT equipment's country of origin outweighs the potential benefits. First, officials from the Director of National Intelligence and the National Security Agency stated that the relationship between a company and a foreign military or intelligence service is a more reliable indicator of a potential security risk than whether a product was manufactured outside the United States. Second, officials from the Director of National Intelligence, Defense

⁵⁰The Berry Amendment could apply where the Secretary of Defense, upon the recommendation of the Strategic Materials Protection Board pursuant to 10 U.S.C. 187, determines that the domestic availability of a particular electronic component is critical to national security.

Intelligence Agency, and the National Security Agency stated that tracking the country of origin alone would not be helpful because the country of origin does not necessarily reveal the origin of component technology that a supplier integrates into the final product. Third, officials from the Central Intelligence Agency and the Director of National Intelligence stated that tracking the country of origin for every IT component used in the agency's telecommunications networks would be prohibitively expensive and infeasible, based on the mechanisms that are currently readily available.

Conclusions

IT supply chain risk management is an emerging and complex area. The organizations, people, activities, information, and resources used to create and distribute commercial IT to federal agencies introduce a myriad of security risks to federal information systems. If exploited, supply chain vulnerabilities—such as purchasing IT from gray markets or poor inspection and testing procedures—can introduce threats to the confidentiality, integrity, and availability of federal information systems. Should this occur on a critical information system, the potential exists for serious adverse impact on an agency's operations, assets, or employees.

Despite acknowledging these risks, the Departments of Energy and Homeland Security have not developed clear policies that define what security measures, if any, should be implemented to protect against supply chain threats. Further, the Departments of Energy, Justice, and Homeland Security have neither developed and documented procedures for implementing supply chain protection measures nor established monitoring capabilities that are necessary to verify compliance with, and the 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 agencies 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 by defining supply chain protection measures and implementing procedures.

Recommendations for Executive Action

To assist three national security-related agencies in better addressing IT supply chain-related security risks for their departmental information systems, we are making the following eight recommendations.

To assist the Department of Energy in protecting against IT supply chain threats, we recommend that the Secretary of Energy direct the appropriate agency officials to take the following three actions:

- develop and document departmental policy that defines which security measures should be employed to protect against supply chain threats;
- develop, document, and disseminate procedures to implement the supply chain protection security measures defined in departmental policy; and
- develop and implement a monitoring capability to verify compliance with, and assess the effectiveness of, supply chain protection measures.

To assist the Department of Homeland Security in protecting against IT supply chain threats, we recommend that the Secretary of Homeland Security direct the appropriate agency officials to take the following three actions:

- develop and document departmental policy that defines which security measures should be employed to protect against supply chain threats;
- develop, document, and disseminate procedures to implement the supply chain protection security measures defined in departmental policy; and
- develop and implement a monitoring capability to verify compliance with, and assess the effectiveness of, supply chain protection measures.

To assist the Department of Justice in protecting against IT supply chain threats, we recommend that the Attorney General direct the appropriate agency officials to take the following two actions:

- develop, document, and disseminate procedures to implement the supply chain protection security measures defined in departmental policy; and
- develop and implement a monitoring capability to verify compliance with, and assess the effectiveness of, supply chain protection measures.

Agency Comments and Our Evaluation

We provided a draft of this report to the Departments of Defense, Energy, Homeland Security, and Justice (including the FBI), the Office of the Director of National Intelligence, and the Department of Commerce's NIST for their review and comment.

Energy provided written comments on a draft of our report (see app. II), signed by the department's Chief Information Officer. In its comments, Energy stated that it concurred with the spirit of our recommendations. Energy also expressed concern that the recommendations are not fully aligned with the administration's initiatives and stated that it believes policies and standards to address IT supply chain risk management must be coordinated at the national level, not independently through individual agencies. We agree that national or federal policies and standards should be coordinated and promulgated at the national or federal level. We also believe, as intended by our recommendations, that federal departments are responsible for developing departmental policies and procedures that are consistent and aligned with federal guidance. Our recommendations to Energy are based on and consistent with federal guidance on supply chain risk management. Energy also stated that our report may significantly underestimate the deep complexities and interdependencies posed by the supply chain threat. Our report recognizes the unique characteristics related to understanding and mitigating the risks associated with the emerging IT supply chain threat. In particular, we identified potential threats to federal information systems that are beyond the failure or disruption in the production or distribution of critical IT products, including the introduction of hardware or software containing malicious logic at any point in a system's life cycle.

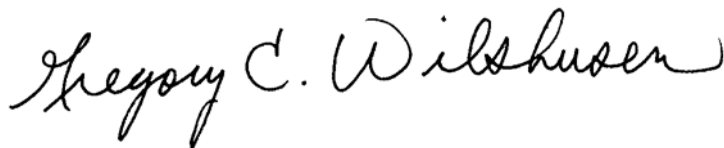
DHS also provided written comments on a draft of our report (see app. III), signed by DHS's Director of Departmental GAO-OIG Liaison Office. In its comments, DHS concurred with our recommendations and stated that the department's Chief Information Security Officer had begun coordinating with the appropriate program offices to develop departmental policy to define security measures to protect against supply chain threats, with an estimated completion date of October 31, 2012. DHS also indicated that the Chief Information Security Officer will (1) examine the best available risk management procedures and (2) explore viable options for verifying compliance with, and assessing the effectiveness of, IT supply chain protection measures, with estimated completion dates of June 30, 2013, and October 31, 2013, respectively. We also received technical comments via e-mail from DHS officials responsible for IT supply chain-related efforts that were incorporated, where appropriate.

In addition, Justice concurred with the recommendations via an e-mail from the Acting Assistant Director, Audit Liaison Group, Internal Review and Evaluation Office, Justice Management Division. We also received technical comments via e-mail from FBI's audit liaison that were incorporated, where appropriate.

We also received technical comments via e-mail from additional officials responsible for IT supply chain-related efforts at Defense, Commerce's NIST, and the Office of the Director of National Intelligence. These comments were incorporated, where appropriate.

We are sending copies of this report to interested congressional committees; the Secretaries of the Departments of Defense, Energy, and Homeland Security; the Attorney General; the Administrator of the General Services Administration; the Director of the Office of Management and Budget; and other interested parties. In addition, the report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions regarding this report, please contact me at (202) 512-6244 or at wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix IV.



Gregory C. Wilshusen
Director
Information Security Issues

List of Congressional Requesters

The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security
and Governmental Affairs
United States Senate

The Honorable Kay Bailey Hutchison
Ranking Member
Committee on Commerce, Science,
and Transportation
United States Senate

The Honorable Thomas R. Carper
Chairman
Subcommittee on Federal Financial
Management, Government Information,
Federal Services, and International Security
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Jon Kyl
Ranking Member
Subcommittee on Crime and Terrorism
Committee on the Judiciary
United States Senate

The Honorable Kirsten Gillibrand
United States Senate

The Honorable Fred Upton
Chairman
Committee on Energy and Commerce
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to identify (1) the key risks associated with the supply chains used by federal agencies to procure information technology (IT) equipment, software, or services; (2) the extent to which selected national security-related agencies have addressed information technology supply chain risks; and (3) the extent to which national security-related federal agencies have determined that their telecommunication networks contain foreign-developed equipment, software, or services.

To identify the key risks, we collected, reviewed, and analyzed relevant supply chain-related practices, guidance, reports, policies, articles, press releases, and other materials from the Departments of Commerce, Defense, Homeland Security (DHS), and Justice. We also collected, reviewed, and analyzed articles from organizations, such as the Information Assurance Technology Analysis Center, the Software Assurance Forum for Excellence in Code, and the Supply Chain Management Center at the University of Maryland's Robert H. Smith School of Business. Using these materials, we identified supply chain-related threats and vulnerabilities based on whether multiple source documents acknowledged the same or similar threats. On the basis of our analysis, we created common descriptions of the key threats and vulnerabilities related to the supply chain. We then validated our list of key threats by sharing them with, and soliciting feedback from, officials from the Office of the Director of National Intelligence, the Office of the National Counterintelligence Executive, the Defense Intelligence Agency, the Central Intelligence Agency, and the National Security Agency.

To identify the extent to which selected national security-related agencies have addressed IT supply chain risks, we analyzed agency policies and procedures related to information security and system acquisition at the Departments of Energy, Justice, Homeland Security, and Defense. We selected these national security-related departments because each is authorized to perform duties connected to national security, law enforcement, intelligence, or homeland defense. In particular, we evaluated whether an agency had, consistent with National Institute of Standards and Technology (NIST) Special Publication 800-53 controls SA-1 and SA-12, defined measures and developed implementing procedures to protect against information technology supply chain threats. We did not assess the effectiveness or legality of any defined measures or developed implementing procedures. In addition, we interviewed officials at each of the four agencies. For Energy, we interviewed officials from the National Nuclear Security Administration Office of the Chief Information Officer; Department of Energy Office of the Chief Information Officer; the Office of Health, Safety, and Security; the

Office of Security Technology and Assistance; and the Office of Intelligence and Counterintelligence. For Justice, we interviewed officials from the Federal Bureau of Investigation and the Justice Management Division. For DHS, we interviewed officials from the National Cyber Security Division (Supply Chain Risk Management Group), the Office of the Chief Information Officer/Security Officer, and the Intelligence and Analysis Office. For Defense, we interviewed officials from the Defense Intelligence Agency, the Office of the Defense Chief Information Officer (Trusted Mission Systems and Networks), the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (Systems Engineering), the National Security Agency, the Defense Information Assurance Program, and the U.S. Army.

To identify the extent to which national security-related federal agencies have determined that their telecommunications networks contain foreign-developed equipment, software, or services, we conducted a legal analysis and interviewed agency officials. Specifically, to determine whether agencies were required to make determinations related to the presence of foreign-developed equipment, software, or services in their telecommunications networks, we analyzed federal statutes, regulations, and agency policies. Sources consulted include provisions of the United States Code such as the Buy American Act, as well as other public laws; the Federal Acquisition Regulation and relevant supplements, including the Defense Federal Acquisition Regulation Supplement; Defense Federal Acquisition Regulation Procedures, Guidance, and Information; Department of Homeland Security procurement regulations; Office of Management and Budget Circular A-130; selected Homeland Security Presidential Directives; selected Executive Orders; and related GAO products. To determine whether the selected national security-related federal agencies had made determinations related to the presence of foreign-developed equipment, software, or services on their telecommunications networks, we interviewed officials from Justice's Management Division and the Offices of the Chief Information Officer for the Departments of Energy, Homeland Security, and Defense. In order to identify potential costs and benefits associated with tracking the country of origin of IT equipment, software or services, we also interviewed officials from the Director of National Intelligence, the Defense Intelligence Agency, the National Security Agency, and the Central Intelligence Agency.

We conducted this performance audit from November 2010 through March 2012 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Energy



Department of Energy
Washington, DC 20585

March 13, 2012

Gregory C. Wilshusen
Director
Information Security Issues
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Wilshusen:

The Department of Energy (DOE) Office of the Chief Information Officer (OCIO) appreciates the opportunity to provide comments to the Government Accountability Office's (GAO) Draft Information Technology (IT) Supply Chain Report, *National Security-related Agencies Need to Better Address Risks* (GAO-12-361).

The Department supports the Administration's goal outlined its National Strategy for Global Supply Chain Security to "strengthen global supply chains in order to protect the welfare and interests of the American people and secure our Nation's economic prosperity." We share the GAO's concern for risks posed to DOE's mission by threats to the IT supply chain. We recognize this is an important issue not only for DOE and its agency partners with National Security missions, but also for the private sector industries that operate and maintain our Nation's critical infrastructure.

The Department and its National Laboratories have been at the forefront of identifying vulnerabilities in the IT supply chain, as well as in developing technologies to mitigate the risk to our National Security Systems¹ and assets. In protecting our mission against these sophisticated threats, the Department closely coordinates with the Intelligence Community to identify the most effective safeguards and overall risk-based approach to counter specific attack vectors which are likely to have the greatest impact to DOE's National Security mission.

Management Response

The draft GAO report identified three recommendations to help ensure the Department is protected against IT supply chain threats. Specifically it recommended that DOE—

- Develop and document Departmental policy that defines which security measures should be employed to protect against supply chain threats.
- Develop, document, and disseminate procedures to implement the supply chain protection security measures defined in departmental policy.
- Develop and implement a monitoring capability to verify compliance with, and assess the effectiveness of, supply chain protection measures.

The Department concurs with the spirit of the GAO's recommendations. The Department also supports the *National Strategy's* strategic goals which articulate the need to "promote the secure and efficient

¹ The term 'National Security System' has the meaning provided in Title III of the E-Government Act (Public Law 107-347).



Printed with soy ink on recycled paper

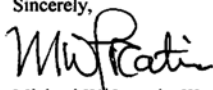
movement of goods” and to “foster a resilient supply chain.” To this end, the Administration has communicated that it seeks to align Federal activities across the United States Government including in our partnerships with industry.

There are many challenges and cost tradeoffs that must be considered in managing risk to the IT and related supply chains. In its report, the GAO recognized this concern noting that intelligence officials from the CIA, NSA, DIA, and the DNI warned that the cost of many existing approaches for IT supply chain risk management outweigh the security benefits. This is because sophisticated subversions inserted into IT hardware and software supply chains can be exceptionally difficult to detect. In the absence of improved technical means to identify and characterize these exploits, the value of focusing on compliance-driven administrative controls to mitigate supply chain risks at the individual agency level is questionable and likely counterproductive. We are therefore concerned that many of the GAO’s conclusions may significantly underestimate the deep complexities and interdependencies posed by this threat, and that the specific recommendations are not fully aligned with the Administration’s initiatives.

We believe that the unified approach described in the *National Strategy* is the right approach and that policies and standards to address IT supply chain risk management must be coordinated and implemented at the National level, not independently through individual agencies. In moving forward, the Department is working closely with the National Counterintelligence Executive and other elements of the Intelligence and National Security communities in defining mission-effective strategies to promote the development of advanced technologies to deliver the technological breakthroughs necessary to effectively and efficiently protect the IT supply chain for our National Security Infrastructure, our Nation’s critical infrastructure and more broadly for all IT environments in Government and Industry.

Again, we thank you for the opportunity to review this report. If you have any questions related to this letter, please feel free to contact me at (202) 586-0166.

Sincerely,



Michael W. Locatis, III

Appendix III: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

March 15, 2012

Gregory C. Wilshusen
Director, Information Security Issues
441 G Street, NW
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Wilshusen:

Re: Draft Report GAO-12-361, "IT SUPPLY CHAIN: National Security-related Agencies Need to Better Address Risks"

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government and Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's acknowledgement of DHS involvement in interagency efforts to address information technology (IT) supply chain security concerns, including our participation in the development of technical and policy tools, and collaboration with the intelligence community. DHS and the Department of Defense also jointly lead an effort on supply chain risk management to address issues of globalization affecting the federal government's IT. DHS is aware of the threats to the IT supply chain and moving forward to address those risks.

The Department is confident in being able to implement IT supply chain protection measures for software. However, the cost benefit of deploying these measures for hardware has proven problematic for the entire IT security community. As security measures are identified and where costs are commensurate with the risk, DHS will examine their feasibility for our risk environment and adopt them, as appropriate.

The draft report contained three recommendations directed at DHS, with which the Department concurs. Specifically, GAO recommended that the Secretary of Homeland Security direct the appropriate agency officials to:

Recommendation 1: Develop and document departmental policy that defines which security measures should be employed to protect against supply chain threats.

Response: Concur. The DHS Chief Information Security Officer (CISO) has begun coordinating with the appropriate program offices to develop departmental policy that will define which security measures should be employed to protect against supply chain threats. We are dependent upon the IT security community's innovation and advancement at this time.

The policy will require system owners to identify risks emanating from the IT supply chain, assess the impact to their program, and identify security measures, if any, that shall be employed to minimize those risks. Estimated Completion Date (ECD): October 31, 2012

Recommendation 2: Develop, document, and disseminate procedures to implement the supply chain protection security measures defined in departmental policy.

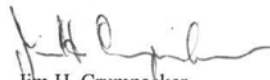
Response: Concur. The DHS CISO will examine the best available risk management procedures in the IT security community and adopt, document, and disseminate those procedures that are most appropriate to the Department's risk environment.
ECD: June 30, 2013

Recommendation 3: Develop and implement a monitoring capability to verify compliance with, and assess the effectiveness of, supply chain protection measures.

Response: Concur. The DHS CISO will explore the viable options within the Department for verifying compliance with, and assessing the effectiveness of, IT supply chain protection measures. A monitoring capability will be established based on those results.
ECD: October 31, 2013

Again, thank you for the opportunity to review and comment on this draft report. Technical comments on this report were previously provided under separate cover. We look forward to working with you on future Homeland Security issues.

Sincerely,



Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

GAO staff who made significant contributions to this report include Michael W. Gilmore, Assistant Director; Bradley W. Becker; Kami J. Corbett; Richard J. Hagerman; Kush K. Malhotra; Lee A. McCracken; Sylvia Shanks; and Adam Vodraska.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

