United States Government Accountability Office

Testimony before the Subcommittees on Counterterrorism and Intelligence, and Oversight and Management Efficiency, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Thursday, July 12, 2018

INFORMATION SECURITY

Supply Chain Risks Affecting Federal Agencies

Accessible Version

Statement of Gregory C. Wilshusen
Director, Information Security Issues

GAO-18-667T

July 12, 2018

INFORMATION SECURITY

Supply Chain Risks Affecting Federal Agencies

GAO Highlights

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

Why GAO Did This Study

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

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

What GAO Recommends

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

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

What GAO Found

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

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

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

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

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

Chairmen King and Perry, Ranking Members Rice and Correa, and Members of the Subcommittees:

Thank you for the opportunity to testify at today's hearing on keeping adversaries away from the homeland security supply chain. As you know, federal agencies and the owners and operators of our nation's critical infrastructure rely extensively on information technology (IT) and IT services to carry out their operations. Securing this technology, its supply chain, and the information it contains is essential to protecting national and economic security.

Since 1997, we have identified federal information security as a governmentwide high-risk area. In 2003, we expanded this high-risk area to include protecting systems supporting our nation's critical infrastructure.[1]

My statement provides an overview of the information security risks associated with the supply chains used by federal agencies to procure IT equipment, software, or services.[2] The statement also discusses our 2012 assessment of the extent to which four national security-related agencies—the Departments of Defense, Justice, Energy, and Homeland Security (DHS)—had addressed these risks.[3]

[1]See, most recently, GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others,* GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

[2]The National Institute of Standards and Technology (NIST) has defined the term "supply chain" as a set of organizations, people, activities, information, and resources that create and move a product or service from suppliers to an organization's customers. 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).

[3]GAO, *IT Supply Chain: National Security-Related Agencies Need to Better Address Risks*, GAO-12-361 (Washington, D.C.: Mar. 23, 2012).

In developing this testimony, we relied on our previous reports,[4] as well as information provided by the national security-related agencies on their actions in response to our previous recommendations. We also considered information contained in special publications issued by the National Institute of Standards and Technology (NIST) and a directive issued by DHS. A more detailed discussion of the objectives, scope, and methodology for this work is included in each of the reports that are cited throughout this statement.

The work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The design and development of information systems can be complex undertakings, consisting of a multitude of pieces of equipment and software products, and service providers. Each of the components of an information system may rely on one or more supply chains—that is, the set of organizations, people, activities, information, and resources that create and move a product or service from suppliers to an organization's customers.

Obtaining a full understanding of the sources of a given information system can also be extremely complex. According to the Software Engineering Institute, the identity of each product or service provider may not be visible to others in the supply chain. Typically, an acquirer, such as a federal agency, may only know about the participants to which it is directly connected in the supply chain. Further, the complexity of corporate structures, in which a parent company (or its subsidiaries) may own or control companies that conduct business under different names in multiple countries, presents additional challenges to fully understanding

[4]See GAO-12-361; *State Department Telecommunications: Information on Vendors and Cyber-Threat Nations*, GAO-17-688R (Washington, D.C.: July 27, 2017); and *Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment*, GAO-13-625T (Washington, D.C.: May 21, 2013).

the sources of an information system. As a result, the acquirer may have little visibility into the supply chains of its suppliers.

Federal procurement law and policies promote the acquisition of commercial products when they meet the government's needs. Commercial providers of IT use a global supply chain to design, develop, manufacture, and distribute hardware and software products throughout the world. Consequently, the federal government relies heavily on IT equipment manufactured in foreign nations.

Federal information and communications systems can include a multitude of IT equipment, products, and services, each of which may rely on one or more supply chains. These supply chains can be long, complex, and globally distributed and can consist of multiple tiers of outsourcing. As a result, agencies may have little visibility into, understanding of, or control over how the technology that they acquire is developed, integrated, and deployed, as well as the processes, procedures, and practices used to ensure the integrity, security, resilience, and quality of the products and services. Table 1 highlights possible manufacturing locations of typical components of a computer or information systems network.

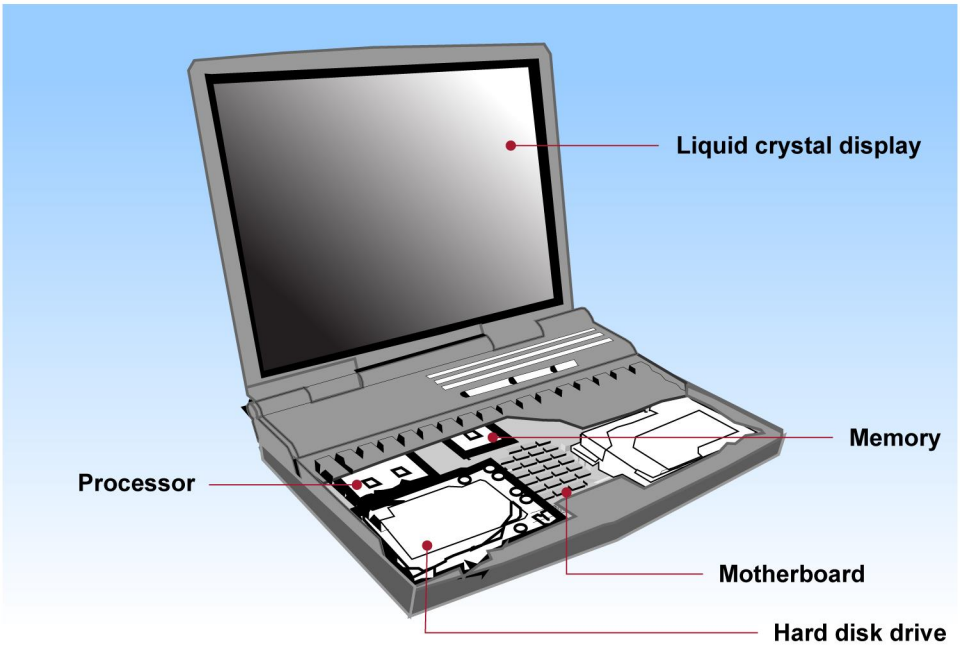
Table 1: Possible Manufacturing Locations of Typical Network Components

Component	Possible manufacturing locations
Workstations	United States, Israel, Spain, China, Malaysia, Singapore, United Kingdom
Notebook computers	United States, Israel, Spain, China, Malaysia, Singapore, United Kingdom
Routing and switching	United States, India, Belgium, Canada, China, Germany, Israel, Japan, Netherlands, Poland, United Kingdom
Fiber optic cabling	China, Malaysia, Vietnam, Japan, Thailand, Indonesia
Servers	Brazil, Canada, United States, India, Japan, France, Germany, United Kingdom, Israel, Singapore
Printers	Japan, United States, Germany, France, Netherlands, Taiwan, China, Malaysia, Thailand, Vietnam, Philippines

Source: GAO analysis of public information | GAO-18-667T

Moreover, many of the manufacturing inputs required for these components—whether physical materials or knowledge—are acquired from various sources around the globe. Figure 1 depicts the potential countries of origin of common suppliers of various components in a commercially available laptop computer.

Figure 1: Potential Origins of Common Suppliers of Laptop Components



Component	Location of facilities potentially used by suppliers
Liquid crystal display	China, Czech Republic, Japan, Poland, Singapore, Slovak Republic, South Korea, Taiwan
Memory	China, Israel, Italy, Japan, Malaysia, Philippines, Puerto Rico, Singapore, South Korea, Taiwan, United States
Processor	Canada, China, Costa Rica, Ireland, Israel, Malaysia, Singapore, United States, Vietnam
Motherboard	Taiwan
Hard disk drive	China, Ireland, Japan, Malaysia, Philippines, Singapore, Thailand, United States

Source: GAO analysis of public information. | GAO-18-667T

Federal Laws and Guidelines Require the Establishment of Information Security Programs and Provide for Managing Supply Chain Risk

The *Federal Information Security Modernization Act* (FISMA) of 2014 requires federal agencies to develop, document, and implement an agency-wide information security program to provide information security

for the information systems and information that support the operations and assets of the agency.[5] The act also requires that agencies ensure that information security is addressed throughout the life cycle of each agency information system. FISMA assigns NIST the responsibility for providing standards and guidelines on information security to agencies. In addition, the act authorizes DHS to develop and issue binding operational directives to agencies, including directives that specify requirements for the mitigation of exigent risks to information systems.

NIST has issued several special publications (SP) that provide guidelines to federal agencies on controls and activities relevant to managing supply chain risk. For example,

- NIST SP 800-39 provides an approach to organization-wide management of information security risk, which states that organizations should monitor risk on an ongoing basis as part of a comprehensive risk management program.[6]
- NIST SP 800-53 (Revision 4) provides a catalogue of controls from which agencies are to select controls for their information systems. It also specifies several control activities that organizations could use to provide additional supply chain protections, such as conducting due diligence reviews of suppliers and developing acquisition policy, and implementing procedures that help protect against supply chain threats throughout the system development life cycle.[7]
- NIST SP 800-161 provides guidance to federal agencies on identifying, assessing, selecting, and implementing risk management processes and mitigating controls throughout their organizations to help manage information and communications technology supply chain risks.[8]

[5]FISMA 2014 (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as *Title III, E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this statement, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

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

[7]NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

[8]NIST, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, SP-800-161 (Gaithersburg, Md.: April 2015).

In addition, as of June 2018, DHS has issued one binding operational directive related to an IT supply chain-related threat. Specifically, in September 2017, DHS issued a directive to all federal executive branch departments and agencies to remove and discontinue present and future use of Kaspersky-branded products on all federal information systems.[9] In consultation with interagency partners, DHS determined that the risks presented by these products justified their removal.

Beyond these guidelines and requirements, the *Ike Skelton National Defense Authorization Act for Fiscal Year 2011* also 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 specific types of procurements on the basis of a determination of significant supply chain risk to a covered system.[10] Section 806 also establishes requirements for limiting disclosure of the basis of such procurement action.

IT Supply Chains Introduce Numerous Information Security Risks to Federal Agencies

In several reports issued since 2012,[11] we have pointed out that the reliance on complex, global IT supply chains introduces multiple risks to federal information and telecommunications systems. This includes the risk of these systems being manipulated or damaged by leading foreign cyber-threat nations such as Russia, China, Iran, and North Korea.[12] Threats and vulnerabilities created by these cyber-threat nations, vendors

[9]DHS, *Removal of Kaspersky-Branded Products*, BOD-17-01 (Washington, D.C.: Sept. 13, 2017).

[10]The 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."

[11]GAO-12-361, GAO-13-652T, and GAO-17-688R.

[12]The Office of the Director of National Intelligence has identified Russia, China, Iran, and North Korea as leading cyber-threat nations in its *Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington, D.C.: Feb. 9, 2016 and Feb. 13, 2018).

or suppliers closely linked to cyber-threat nations,[13] and other malicious actors can be sophisticated and difficult to detect and, thus, pose a significant risk to organizations and federal agencies.

As we reported in March 2012,[14] supply chain threats are present at various phases of a system's development life cycle. Key threats that could create an unacceptable risk to federal agencies include the following.

- **Installation of hardware or software containing malicious logic**, which is hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. 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.
- **Installation of counterfeit hardware or software**, which is hardware or software containing non-genuine component parts or code. According to the Defense Department's Information Assurance Technology Analysis Center, counterfeit IT threatens the integrity, trustworthiness, and reliability of information systems for several reasons, including the facts that (1) counterfeits are usually less reliable and, therefore, may fail more often and more quickly than genuine parts; and (2) counterfeiting presents an opportunity for the

[13]The Department of State Authorities Act, Fiscal Year 2017, defines "closely-linked" as, with respect to a foreign supplier, contactor, or subcontractor and a cyber-threat nation, (1) incorporated or headquartered in the territory; (2) having ties to the military forces; (3) having ties to the intelligence services; or (4) the beneficiary of significant low-interest or no-interest loans, loan forgiveness, or other support of a leading cyber-threat nation. The Act also included a provision for GAO to review the Department of State's (State) critical telecommunications equipment or services obtained from manufacturers or suppliers that are closely linked to the leading cyber-threat nations. Based on GAO's open source review of generalizable samples of 52 telecommunications device manufacturers and software developers supporting the State's critical telecommunications capabilities and 100 of State's telecommunications contractors, GAO identified 16 companies--12 equipment manufacturers and software developers and 4 telecommunications contractors--with suppliers reported to be headquartered in cyber-threat nations. All of these suppliers were reported to be headquartered in China or, in one case, Russia. The data did not establish whether State's telecommunications capabilities were supported by equipment or software originating from suppliers linked to companies in GAO's samples. GAO did not identify any reported military ties, intelligence ties, or low-interest loans involving cyber-threat nations among any of the suppliers. See GAO-17-688R.

[14]GAO-12-361.

counterfeiter to insert malicious logic or backdoors[15] into replicas or copies that would be far more difficult in more secure manufacturing facilities.[16]

- **Failure or disruption in the production or distribution of critical products.** Both man-made (e.g., disruptions caused by labor, trade, or political disputes) and natural (e.g., earthquakes, fires, floods, or hurricanes) causes could decrease the availability of material needed to develop systems or disrupt the supply of IT products critical to the operations of federal agencies.
- **Reliance on a malicious or unqualified service provider** for the performance of technical services. By virtue of their position, contractors and other service providers may have access to federal data and systems. 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.
- **Installation of hardware or software that contains unintentional vulnerabilities**, such as defects in code that can be exploited. Cyber attackers may focus their efforts on, among other things, finding and exploiting existing defects in software code. Such defects are usually the result of unintentional coding errors or misconfigurations, and can facilitate attempts by attackers to gain unauthorized access to an agency's information systems and data, or disrupt service.

We noted in the March 2012 report that threat actors[17] can introduce these threats into federal information systems 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 security procedures, controls, or implementation related to an information system. Examples of the types of vulnerabilities that could be exploited include

[15]A "backdoor" is a general term for a malicious program that can potentially give an intruder remote access to an infected computer.

[16]Information 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 State of the Art Repor*t, DO 380 (Herndon, Va.: August 2010).

[17]Supply chain-related threat actors include foreign intelligence services and militaries, corporate spies, corrupt government officials, cyber vandals, disgruntled employees, radical activists, purveyors of counterfeit goods, or criminals.

- acquisitions of IT products or parts from sources other than the original manufacturer or authorized reseller, such as independent distributors, brokers, or on the gray market;
- lack of adequate testing for software updates and patches; and
- incomplete information on IT suppliers.

If a threat actor exploits an existing vulnerability, it could lead to the loss of the confidentiality, integrity, or availability of the system and associated information. This, in turn, can adversely affect an agency's ability to carry out its mission.

Four National Security-Related Agencies Have Acted to Better Address IT Supply Chain Risks for Their Information Systems

In March 2012, we reported that the four national security-related agencies (i.e., Defense, Justice, Energy, and DHS) had acknowledged the risks presented by supply chain vulnerabilities.[18] However, the agencies varied in the extent to which they had addressed these risks by (1) defining supply chain protection measures for department information systems, (2) developing implementing procedures for these measures, and (3) establishing capabilities for monitoring compliance with, and the effectiveness of, such measures.

Of the four agencies, the Department of Defense had made the most progress addressing the risks. Specifically, the department's supply chain risk management efforts began in 2003 and included:

- a policy requiring supply chain risk to be addressed early and across a system's entire life cycle and calling for an incremental implementation of supply chain risk management through a series of pilot projects;
- a requirement that every acquisition program submit and update a "program protection plan" that was to, among other things, help manage risks from supply chain exploits or design vulnerabilities;
- procedures for implementing supply chain protection measures, such as an implementation guide describing 32 specific measures for

[18]GAO-12-361.

enhancing supply chain protection and procedures for program protection plans identifying ways in which programs should manage supply chain risk; and

- a monitoring mechanism to determine the status and effectiveness of supply chain protection pilot projects, as well as monitoring compliance with and effectiveness of program protection policies and procedures for several acquisition programs.

Conversely, our report noted that the other three agencies had made limited progress in addressing supply chain risks for their information systems. For example:

- The Department of Justice had defined specific security measures for protecting against supply chain threats through the use of provisions in vendor contracts and agreements. Officials identified (1) a citizenship and residency requirement and (2) a national security risk questionnaire as two provisions that addressed supply chain risk. However, Justice had not developed procedures for ensuring the effective implementation of these protection measures or a mechanism for verifying compliance with, and the effectiveness of these measures. We stressed that, without such procedures, Justice would have limited assurance that its departmental information systems were being adequately protected against supply chain threats.
- In May 2011, the Department of Energy revised its information security program, which required Energy components to implement provisions based on NIST and Committee on National Security Systems guidance. However, the department was unable to provide details on implementation progress, milestones for completion, or how supply chain protection measures would be defined. Because it had not defined these measures or associated implementing procedures, we reported that the department was not in a position to monitor compliance or effectiveness.
- Although its information security guidance mentioned the NIST control related to supply chain protection, DHS had not defined the supply chain protection control activities that system owners should employ. The department's information security policy manager stated that DHS was in the process of developing policy that would address supply chain protection, but did not provide details on when it would be completed. In the absence of such a policy, DHS was not in a position to develop implementation procedures or to monitor compliance or effectiveness.

To assist Justice, Energy, and DHS in better addressing IT supply chain-related security risks for their departmental information systems, we made eight recommendations to these three agencies in our 2012 report. Specifically, we recommended that Energy and DHS:

- develop and document departmental policy that defines which security measures should be employed to protect against supply chain threats.

We also recommended that Justice, Energy, and DHS:

- 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.

The three agencies generally agreed with our recommendations and, subsequently, implemented seven of the eight recommendations. Specifically, we verified that Justice and Energy had implemented each of the recommendations we made to them by 2016. We also confirmed that DHS had implemented two of the three recommendations we made to that agency by 2015.

However, as of fiscal year 2016,[19] DHS had not fully implemented our recommendation to develop and implement a monitoring capability to verify compliance with, and assess the effectiveness of, supply chain protections. Although the department had developed a policy and approach for monitoring supply chain risk management activities, it could not provide evidence that its components had actually implemented the policy. Thus, we were not able to close the recommendation as implemented. Nevertheless, the implementation of the seven recommendations and partial implementation of the eighth recommendation better positioned the three agencies to monitor and mitigate their IT supply chain risks.

[19]GAO reviews agency actions to implement its recommendations and may decide to close a recommendation as not implemented if an agency has not implemented the recommendation within 4 fiscal years of GAO making the recommendation. Fiscal year 2016 was the fourth fiscal year after GAO made the recommendations to DHS in its March 2012 report.

In addition, we reported in March 2012 that the four national security-related agencies had participated in interagency efforts to address supply chain security, including participation in the Comprehensive National Cybersecurity Initiative,[20] development of technical and policy tools, and collaboration with the intelligence community. In support of the cybersecurity initiative, Defense and DHS jointly led an interagency initiative on supply chain risk management to address issues of globalization affecting the federal government's IT. Also, DHS had developed a comprehensive portfolio of technical and policy-based product offerings for federal civilian departments and agencies, including technical assessment capabilities, acquisition support, and incident response capabilities. The efforts of the four agencies could benefit all federal agencies in addressing their IT supply chain risks.

In summary, the global IT supply chain introduces a myriad of security risks to federal information systems that, if realized, could jeopardize the confidentiality, integrity, and availability of federal information systems. Thus, the potential exists for serious adverse impact on an agency's operations, assets, and employees. These factors highlight the importance and urgency of federal agencies appropriately assessing, managing, and monitoring IT supply chain risk as part of their agencywide information security programs.

Chairmen King and Perry, Ranking Members Rice and Correa, and Members of the Subcommittees, this completes my prepared statement. I would be pleased to answer your questions.

Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this statement include Jeffrey Knott (assistant director), Christopher Businsky, Nancy Glover, and Rosanna Guerrero.

[20]Begun by the Bush administration in 2008, the Comprehensive National Cybersecurity Initiative is a series of initiatives aimed at improving cybersecurity within the federal government. This initiative, which is composed of 12 projects with the objective of safeguarding federal executive branch information systems, includes a project focused on addressing global supply chain risk management.

(102906)

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 (https://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 https://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, https://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 https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@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

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548