United States Government Accountability Office

Report to Congressional Requesters

December 2020

INFORMATION TECHNOLOGY

Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks

Accessible Version

GAO Highlights

Highlights of GAO-21-171, a report to congressional requesters

December 2020

INFORMATION TECHNOLOGY

Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks

Why GAO Did This Study

Federal agencies rely extensively on ICT products and services (e.g., computing systems, software, and networks) to carry out their operations. However, agencies face numerous ICT supply chain risks, including threats posed by counterfeiters who may exploit vulnerabilities in the supply chain and, thus, compromise the confidentiality, integrity, or availability of an organization's systems and the information they contain. For example, in September 2019, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency reported that federal agencies faced approximately 180 different ICT supply chain-related threats. To address threats such as these, agencies must make risk-based ICT supply chain decisions about how to secure their systems.

GAO was asked to conduct a review of federal agencies' ICT SCRM practices. The specific objective was to determine the extent to which federal agencies have implemented foundational ICT SCRM practices. To do so, GAO identified seven practices from NIST guidance that are foundational for an organization-wide approach to ICT SCRM and compared them to policies, procedures, and other documentation from the 23 civilian Chief Financial Officers Act agencies.

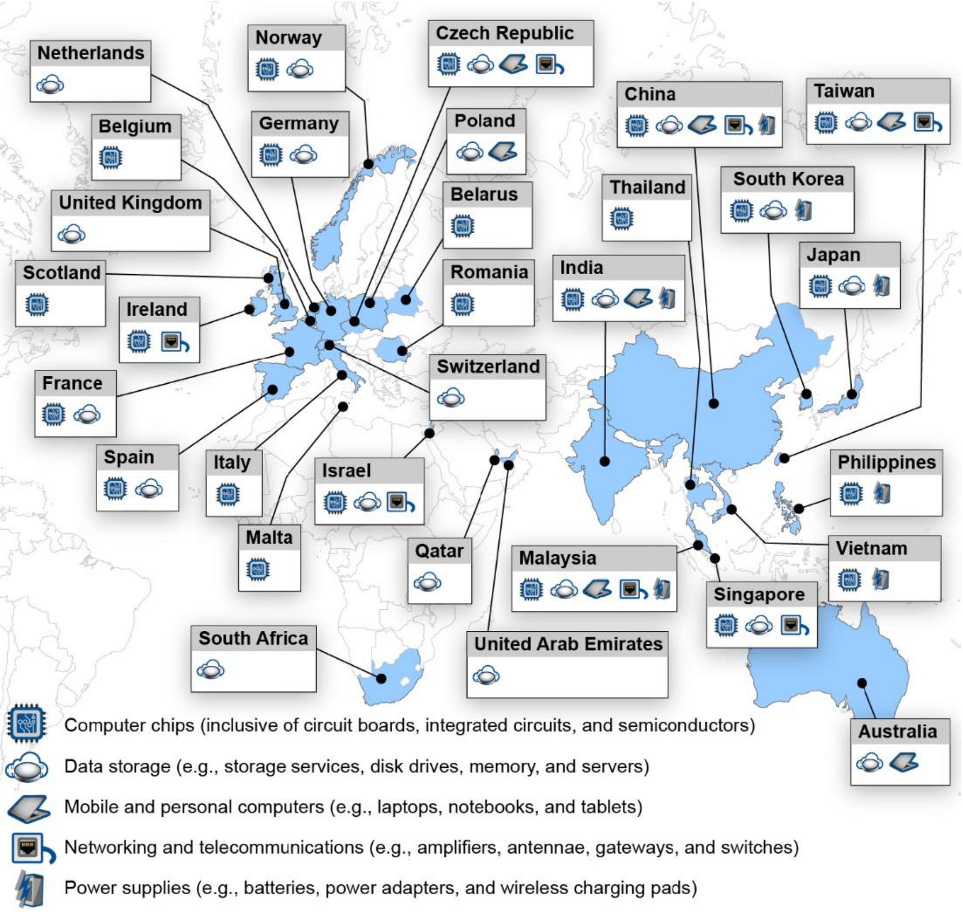
This is a public version of a sensitive report that GAO issued in October 2020. Information that agencies deemed sensitive was omitted and GAO substituted numeric identifiers that were randomly assigned for the names of the agencies due to sensitivity concerns.

View GAO-21-171. For more information, contact Carol C. Harris at (202) 512-4456 or harrisCC@gao.gov.

What GAO Found

Few of the 23 civilian Chief Financial Officers Act agencies had implemented seven selected foundational practices for managing information and communications technology (ICT) supply chain risks. Supply chain risk management (SCRM) is the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains. Many of the manufacturing inputs for these ICT products and services originate from a variety of sources throughout the world. (See figure 1.)

Figure 1: Examples of Locations of Manufacturers or Suppliers of Information and Communications Technology Products and Services


Netherlands
Norway
Czech Republic
China
Taiwan
Belgium
Germany
Poland
United Kingdom
Belarus
Thailand
South Korea
Scotland
Romania
India
Japan
Ireland
France
Switzerland
Spain
Italy
Israel
Philippines
Malta
Qatar
Malaysia
Vietnam
Singapore
South Africa
United Arab Emirates
Australia
Computer chips (inclusive of circuit boards, integrated circuits, and semiconductors)
Data storage (e.g., storage services, disk drives, memory, and servers)
Mobile and personal computers (e.g., laptops, notebooks, and tablets)
Networking and telecommunications (e.g., amplifiers, antennae, gateways, and switches)
Power supplies (e.g., batteries, power adapters, and wireless charging pads)

Source: GAO analysis of public information. | GAO-21-171

None of the 23 agencies fully implemented all of the SCRM practices and 14 of the 23 agencies had not implemented any of the practices. The practice with the highest rate of implementation was implemented by only six agencies. Conversely, none of the other practices were implemented by more than three agencies. Moreover, one practice had not been implemented by any of the agencies. (See figure 2.)

The foundational practices comprising ICT SCRM are:

- establishing executive oversight of ICT activities, including designating responsibility for leading agency-wide SCRM activities;
- developing an agency-wide ICT SCRM strategy for providing the organizational context in which risk-based decisions will be made;
- establishing an approach to identify and document agency ICT supply chain(s);
- establishing a process to conduct agency-wide assessments of ICT supply chain risks that identify, aggregate, and prioritize ICT supply chain risks that are present across the organization;
- establishing a process to conduct a SCRM review of a potential supplier that may include reviews of the processes used by suppliers to design, develop, test, implement, verify, deliver, and support ICT products and services;
- developing organizational ICT SCRM requirements for suppliers to ensure that suppliers are adequately addressing risks associated with ICT products and services; and

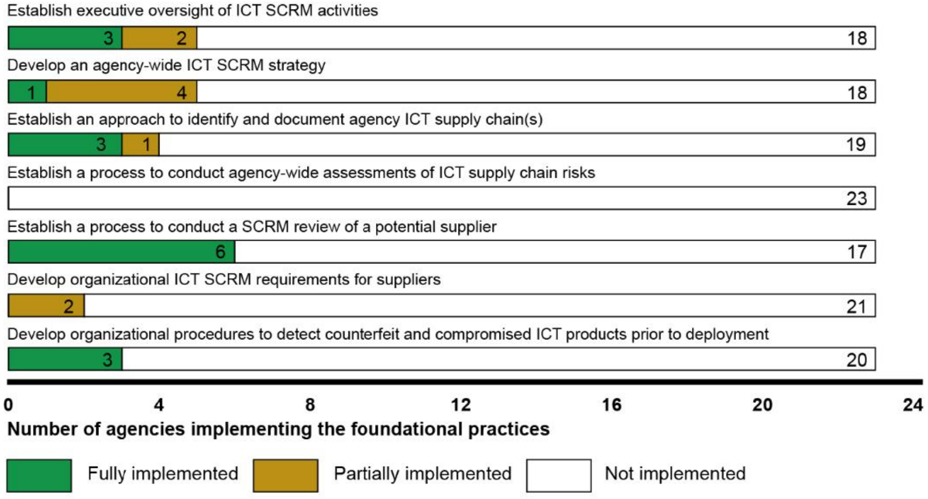
developing organizational procedures to detect counterfeit and compromised ICT products prior to their deployment.

GAO also interviewed relevant agency officials.

What GAO Recommends

In the sensitive report, GAO made a total of 145 recommendations to the 23 agencies to fully implement foundational practices in their organization-wide approaches to ICT SCRM. Of the 23 agencies, 17 agreed with all of the recommendations made to them; two agencies agreed with most, but not all of the recommendations; one agency disagreed with all of the recommendations; two agencies neither agreed nor disagreed with the recommendations, but stated they would address them; and one agency had no comments. GAO continues to believe that all of the recommendations are warranted, as discussed in the sensitive report.

Figure 2: Extent to Which the 23 Civilian Chief Financial Officers Act Agencies Implemented Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Practices



Source: GAO analysis of agency data. | GAO-21-171

Data table for Figure 2: Extent to Which the 23 Civilian Chief Financial Officers Act Agencies Implemented Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Practices

Foundational practices	Fully implemented	Partially implemented	Not implemented
Establish executive oversight of ICT SCRM activities	3	2	18
Develop an agency-wide ICT SCRM strategy	1	4	18
Establish an approach to identify and document agency ICT supply chain(s)	3	1	19
Establish a process to conduct agency-wide assessments of ICT supply chain risks	0	0	23
Establish a process to conduct reviews of potential suppliers prior to selecting products and services	6	0	17
Develop organizational ICT SCRM requirements for suppliers	0	2	21
Develop organizational procedures to detect counterfeit and compromised ICT products prior to deployment	3	0	20

As a result of these weaknesses, these agencies are at a greater risk that malicious actors could exploit vulnerabilities in the ICT supply chain causing disruption to mission operations, harm to individuals, or theft of intellectual property. For example, without establishing executive oversight of SCRM activities, agencies are limited in their ability to make risk decisions across the organization about how to most effectively secure their ICT product and service supply chains. Moreover, agencies lack the ability to understand and manage risk and reduce the likelihood that adverse events will occur without reasonable visibility and traceability into supply chains.

Officials from the 23 agencies cited various factors that limited their implementation of the foundational practices for managing supply chain risks. The most commonly cited factor was the lack of federal SCRM guidance. For example, several agencies reported that they were waiting for federal guidance to be issued from the Federal Acquisition Security Council—a cross-agency group responsible for providing direction and guidance to executive agencies to reduce their supply chain risks—before implementing one or more of the foundational practices. According to Office of Management and Budget (OMB) officials, the council expects to complete this effort by December 2020.

While the additional direction and guidance from the council could further assist agencies with the implementation of these practices, federal agencies currently have guidance to assist with managing their ICT supply chain risks. Specifically, the National Institute of Standards and Technology (NIST) issued ICT SCRM-specific guidance in 2015 and OMB has required agencies to implement ICT SCRM since 2016. Until agencies implement all of the foundational ICT SCRM practices, they will be limited in their ability to address supply chain risks across their organizations effectively.

Contents

Tables

Figure

Abbreviations

CFO	Chief Financial Officers
CIO	chief information officer
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
FASC	Federal Acquisition Security Council
ICT	information and communications technology
IT	information technology
LOUO	limited official use only
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SCRM	supply chain risk management

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

December 15, 2020

Congressional Requesters

Federal agencies rely extensively on information and communications technology (ICT) products and services to carry out their operations.[1] This dependence on ICT solutions has increased the complexity, diversity, and scale of the federal government's supply chains—that is, the set of public and private sector entities that interact to design, manufacture, assemble, distribute, implement, and use ICT solutions.

In September 2019, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) reported that federal agencies faced approximately 180 different ICT supply chain-related threats.[2] Supply chain 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 organization's systems and the information they contain. Given these threats, agencies must make risk-based ICT supply chain decisions about how to most effectively secure their systems and data.

Supply chain risk management (SCRM) is the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains. The President's Budget for Fiscal Year 2021 includes at least $18.8 billion for cybersecurity funding, which supports the protection of federal information systems, including SCRM.

You asked us to conduct a review of federal agencies' ICT SCRM practices. Accordingly, the objective of our review was to determine the

[1] According to the Federal Acquisition Supply Chain Security Act of 2018, ICT is information technology, information systems, and telecommunications equipment and telecommunications services. Examples of ICT products and services include printed circuit boards, cloud computing services, computing systems, software, satellite communications, and networks.

[2] CISA, *Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report, Status Update on Activities and Objectives of the Task Force*, (September 2019).

extent to which federal agencies implemented foundational ICT SCRM practices.

This report presents a public version of a “limited official use only” (LOUO) report that we issued in October 2020.[3] A number of agencies in our review determined that the information in that report should be protected from public disclosure. Therefore, we are not releasing the LOUO report to the general public because of the sensitive information it contains.

The LOUO report includes 145 recommendations that we made to 23 agencies to fully implement foundational practices in their organization-wide approaches to ICT SCRM. In this public version of the report, we substituted numeric identifiers that were randomly assigned for the names of the agencies due to sensitivity concerns.

Although the information provided in this report is more limited, this report addresses the same objective as the LOUO report and is based on the same audit methodology. We provided a draft of this report to agency officials to obtain their review and comments on the sensitivity of the information contained herein. We confirmed with the agency officials that this report can be made available to the public without jeopardizing the security of their ICT SCRM practices.

To address the objective, we identified and selected from our review of National Institute of Standards and Technology (NIST) guidance, as of February 2020, foundational practices that were of particular importance for providing an organization-wide approach to ICT SCRM.[4] This effort resulted in our selection of seven practices. Further, we validated our

[3] GAO, *Information and Communications Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-164SU (Washington, D.C.: October 27, 2020).

[4] NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (Gaithersburg, Md.: April 2018); *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST Special Publication 800-37, Revision 2 (December 2018); *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Special Publication 800-161 (Gaithersburg, Md.: April 2015); *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, Md.: April 2013); *Information Security: Guide for Conducting Risk Assessments*, Special Publication 800-30, Revision 1 (Gaithersburg, Md.: September 2012); and *Managing Information Security Risk: Organization, Mission, and Information System View*, Special Publication 800-39 (Gaithersburg, Md.: March 2011).

selection of the practices with internal subject matter experts and officials from NIST's Computer Security Division.

To ensure consistent understanding and application of the practices in our evaluation, we identified specific evaluation criteria in NIST guidance that were associated with each of the selected seven practices. The seven practices and their associated evaluation criteria are listed in table 1.

Table 1: Evaluation Criteria Associated with the Selected Foundational Practices for Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM)

Practice	Evaluation criteria
Establish executive oversight of ICT SCRM activities	The agency designated responsibility for leading agency-wide SCRM activities to an executive-level individual, office (supported by an expert staff), or group (e.g., a risk board, executive steering committee, or executive leadership council) regardless of an agency's specific organizational structure. The agency defined SCRM roles and responsibilities for senior leaders who participate in supply chain activities.
Develop an agency-wide ICT SCRM strategy	The agency developed an agency-wide ICT SCRM strategy that made explicit the agency's risk tolerance in clear and unambiguous terms, and identified how federal agencies intend to assess, respond to, and monitor ICT supply chain risks across the life cycle of ICT products and services.
Establish an approach to identify and document agency ICT supply chain(s)	The agency established an approach to identify and describe or depict information about its ICT supply chain that includes, as relevant, suppliers, manufacturing facilities, logistics providers, distribution centers, distributors, wholesalers, and other organizations involved in the manufacturing, operation, management, processing, design and development, handling, and delivery of products and services.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	The agency established a process for conducting agency-wide risk assessments that identified, aggregated, and prioritized ICT supply chain risks that are present across the organization, resulted in a determination of agency-wide risk that takes into consideration the criticality and interconnected nature of ICT products and services, and updated at an organizationally-defined frequency.
Establish a process to conduct a SCRM review of a potential supplier	The agency established an organizational process for conducting a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services.
Develop organizational ICT SCRM requirements for suppliers	The agency developed organizational ICT SCRM requirements for inclusion in contracts that are tailored to the type of contract and business needs.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	The agency developed organizational procedures to detect ICT products that are counterfeit and have been compromised prior to their deployment to an operational environment.

Source: GAO analysis based on NIST guidance. | GAO-21-171

We then evaluated the extent to which the 23 civilian Chief Financial Officers (CFO) Act of 1990 agencies[5] had implemented these practices for their non-national security systems.[6]

We collected agency policies, procedures, and other documentation and compared them to the seven selected foundational ICT SCRM practices and their associated evaluation criteria. To do so, we:

- analyzed policies and plans for establishing executive oversight of ICT SCRM activities;
- assessed documents and plans for developing an agency-wide ICT SCRM strategy;
- reviewed approaches for identifying and documenting agency ICT supply chains;
- reviewed documents pertaining to conducting agency-wide ICT supply chain risk assessments;
- assessed policies and procedures for conducting a SCRM review of a potential supplier;
- analyzed documentation regarding organizational ICT SCRM requirements for suppliers; and
- reviewed procedures for detecting counterfeit and compromised ICT products prior to their deployment.

[5] The 23 civilian *Chief Financial Officers Act of 1990* agencies are the Departments of Agriculture, Commerce, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development. There are 24 *Chief Financial Officers Act of 1990* agencies. We did not include the Department of Defense because our scope was the civilian agencies.

[6] According to the *Federal Information Security Modernization Act of 2014*, the term “national security system” is defined as any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function or use of which: involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, and is critical to the direct fulfillment of military or intelligence missions (with the exception of routine administrative and business application systems). Systems that do not meet any of the above criteria are considered non-national security systems.

We supplemented our analyses with interviews of relevant agency officials to discuss their activities regarding ICT SCRM. We also provided the results of our analysis of agency documentation to the officials to corroborate our findings, collect additional evidence, and identify causes for any gaps we identified in agencies' implementation of the seven practices.

We then determined whether the evidence provided by the agencies addressed the evaluation criteria for each practice. To determine an overall rating for each of the seven practices, we summarized the results of our assessments of the evaluation criteria as:

- fully implemented—the agency fully implemented all of the practice's evaluation criteria;
- partially implemented—the agency fully or partially implemented at least one, but not all, of the practice's evaluation criteria; and
- not implemented—the agency did not implement any of the practice's evaluation criteria.

A more complete description of our objective, scope, and methodology is provided in appendix I.

The performance audit upon which this report is based was conducted from December 2018 to October 2020 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We worked with the agencies from September 2020 to December 2020 to prepare this version of the original LOUO report for public release. This public version was also prepared in accordance with those standards.

Background

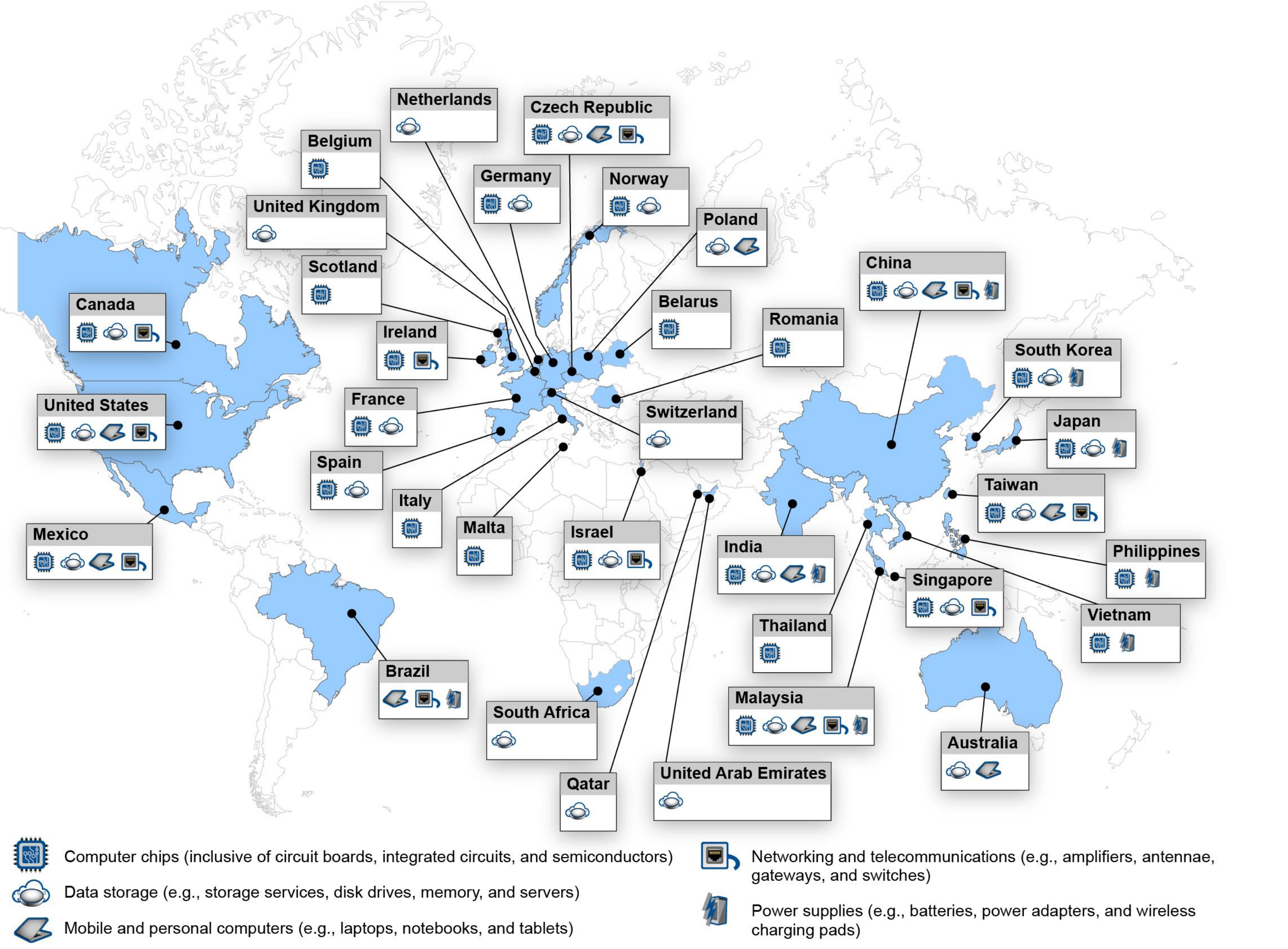
Federal procurement law and policies promote the acquisition of commercial products and services when they meet the government's needs. For example, provisions of the *Federal Acquisition Streamlining Act of 1994* are designed to encourage the government to buy commercial items by (1) requiring a preference 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.[7] Thus, federal agencies have rapidly increased their reliance on commercially available products, contractor support for custom-built systems, and external service providers for a multitude of ICT solutions.

Many of the manufacturing inputs for these ICT products and services—whether physical materials or knowledge—originate from a variety of sources throughout the world.[8] As a result, the federal government has also increased its reliance on complex, interconnected, and globally distributed supply chains that can include multiple tiers of outsourcing. Figure 1 highlights examples of locations of manufacturers or suppliers of various ICT products and services.

[7] *Federal Acquisition Streamlining Act of 1994*, Pub. L. No. 103-355, § 1001, 108 Stat. 3243 (1994). It is codified generally in Title 10 of the United States Code for the Department of Defense and Title 41 of the Code for civilian agencies.

[8] For a more general discussion see GAO, *International Trade: Foreign Sourcing in Government Procurement*, GAO-19-414 (Washington, D.C.: May 30, 2019).

Figure 1: Examples of Locations of Manufacturers or Suppliers of Information and Communications Technology Products and Services


Netherlands
Czech Republic
Belgium
Germany
Norway
United Kingdom
Poland
Scotland
China
Belarus
Canada
Ireland
Romania
South Korea
United States
France
Switzerland
Japan
Spain
Taiwan
Italy
Mexico
Malta
Israel
India
Philippines
Singapore
Thailand
Vietnam
Brazil
South Africa
Malaysia
Australia
Qatar
United Arab Emirates
Computer chips (inclusive of circuit boards, integrated circuits, and semiconductors)
Data storage (e.g., storage services, disk drives, memory, and servers)
Mobile and personal computers (e.g., laptops, notebooks, and tablets)
Networking and telecommunications (e.g., amplifiers, antennae, gateways, and switches)
Power supplies (e.g., batteries, power adapters, and wireless charging pads)

Source: GAO analysis of public information. | GAO-21-171

Dependence on the global supply chain can significantly limit federal agencies’ visibility into, understanding of, and control over how the technology they acquire is developed, distributed, and deployed. Agencies’ understanding of the procedures and practices used to ensure the integrity, security, resilience, and quality of ICT products and services can also be limited. Typically, an acquirer (such as a federal agency) will only know about the participants directly connected to it in the supply chain. For example, a program office at a federal 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,[9] or through open source[10] means.

In addition, 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 obtaining a complete understanding of the source of an ICT product and its potential vulnerabilities. For example, foreign-based companies sometimes manufacture and assemble products and components in the United States and companies based in the United States sometimes manufacture products and components overseas, or domestically employ foreign workers.

For example, a major technology company reported in 2018 that it had suppliers in 39 countries on six continents.[11] According to the company, its products were manufactured in-house in 10 factories and outsourced at more than 15 locations. In addition, the company relied on over 65 suppliers and over 150 factories with which it had a direct relationship. The company also reported that it was aware of more than 200 subordinate suppliers and over 300 factories for which the company did not have a direct contractual relationship.

The ICT Supply Chain Introduces Numerous Risks to Federal Agencies

The ICT supply chain introduces multiple risks to federal agencies and underscores the importance of risk management. Over several years, we have reported that the growing dependence on a globally distributed

[9] Commercial off-the-shelf refers to software and hardware products that already exist and are available from commercial sources.

[10] Open source software is code that is released under a license, which grants users the right to modify, share, and reuse the software.

[11] Dell Technologies, *FY 2018 Supply Chain Sustainability Progress Report* (June 2018).

supply chain—and the lack of control over and visibility into how ICT products and services are developed, integrated, and deployed—presents an increasing amount of risk to federal agencies.[12]

Supply chains are being targeted by increasingly sophisticated and well-funded threat actors,[13] including leading foreign cyber threat nations such as Russia, China, Iran, and North Korea.[14] Attacks by such entities are often especially sophisticated and difficult to detect. In addition, threat actors attack all tiers of the supply chain and at each phase of the system development life cycle and, thus, pose significant risk to federal agencies.[15]

Threat actors carry out attacks by exploiting vulnerabilities that exist at multiple points in the global supply chain. Specifically, they can introduce the use of ICT products and services that are counterfeit[16] or have been compromised to deliver degraded operations or malicious functionality. According to the Department of Defense's Information Assurance

[12] GAO, *Information Security: Supply Chain Risks Affecting Federal Agencies*, GAO-18-667T (Washington, D.C.: July 12, 2018); *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018); *State Department Telecommunications: Information on Vendors and Cyber-Threat Nations*, GAO-17-688R (Washington, D.C.: July 27, 2017); *Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment*, GAO-13-652T (Washington, D.C.: May 21, 2013); and *IT Supply Chain: National Security-Related Agencies Need to Better Address Risks*, GAO-12-361 (Washington, D.C.: Mar. 23, 2012).

[13] 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.

[14] 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. 13, 2018, and Jan. 29, 2019).

[15] Nonadversarial ICT supply chain threat events also pose a risk to federal agencies. These events include natural disasters, such as earthquakes or hurricanes, which can negatively impact the availability of critical resources; the inadvertent introduction of vulnerabilities into software products due to, for example, inherent weaknesses in programming languages and software development environments; and human errors.

[16] A component is considered counterfeit 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.

Technology Analysis Center, counterfeit ICT threatens the integrity, trustworthiness, and reliability of information systems for several reasons. For example, counterfeiting presents an opportunity for the counterfeiter to insert malicious logic[17] or backdoors[18] into replicas or copies that would be far more difficult in more secure manufacturing facilities.[19] In addition, counterfeits are usually less reliable and, therefore, may fail more often and more quickly than genuine parts. The following are examples of attacks carried out using counterfeit products:

- A major software company in the United States investigated counterfeit software and found malware[20] preinstalled on 20 percent of the devices they tested. The malware was installed on new desktops and laptop computers after these products had been shipped from a factory to a distributor, transporter, or reseller.[21]
- A U.S. citizen imported and resold thousands of counterfeit integrated circuits from China and Hong Kong to customers that included contractors for the Department of Defense.[22] The contractors were

[17] Malicious logic 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.

[18] A 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.

[19] 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 (IATAC) State-of-the-Art Report,* DO 380 (Herndon, Va.: August 2010).

[20] Malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim. Examples of malware include logic bombs, Trojan Horses, ransomware, viruses, and worms.

[21] CISA*, Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report, Status Update on Activities and Objectives of the Task Force*, (September 2019).

[22] Integrated circuits enable computers and other products such as telecommunication systems to store and process information. They are made of interconnected electronic components that are etched or imprinted onto a semiconducting material, such as silicon or germanium.

supplying the circuits to the U.S. Navy for use in nuclear submarines.[23]

Threat actors can also compromise a genuine ICT product or service by inserting additional code or functionality into the product or service that performs a new, malicious function. In addition, threat actors can substitute genuine products with counterfeit or genuine products that have been tampered with to include malicious functionality. For example:

- A manufacturer in the United States sourced firmware for its cell phones from a foreign company. This firmware was designed to make encrypted records of the cell phones' call and text histories, phone details, and contact information. The data were then transmitted to a foreign server every 72 hours.[24]
- A factory that manufactured switches[25] for a company in the United States installed malicious logic into memory storage devices during production that could compromise systems and spread malware across a computer network.[26]

Successful attacks by threat actors can have a range of impacts. For example, threat actors could take control of federal information systems; decrease the availability of materials or services needed to develop systems; destroy systems, causing injury and loss of life,[27] and

[23] CISA, *Interim Report,* (September 2019).

[24] CISA, *Interim Report,* (September 2019).

[25] Switches are devices that filter and forward data between network segments.

[26] CISA, *Interim Report,* (September 2019).

[27] For example, counterfeit batteries can contain volatile chemicals which may explode, counterfeit cabling and other components may lack insulation and melt during use and catch fire, and basic safety components may send dangerous electrical currents from a faulty charger directly into cell phones.

compromising national security; or steal intellectual property[28] and sensitive information.

Federal Law Established a Council to Enhance Protection of the ICT Supply Chain

The *Federal Acquisition Supply Chain Security Act of 2018* established a cross-agency council responsible for providing direction and guidance to executive agencies to reduce their supply chain risks.[29] According to the act, the Federal Acquisition Security Council (FASC) must include a lead representative from the Office of Management and Budget (OMB); General Services Administration; DHS, including CISA; the Office of the Director of National Intelligence, including the National Counterintelligence and Security Center; the Department of Justice, including the Federal Bureau of Investigation; the Department of Defense, including the National Security Agency; and the Department of Commerce, including NIST. FASC is required to perform functions that include developing a strategic plan for addressing supply chain risks, working with NIST to develop federal guidance that addresses acquisition-related supply chain risks, and developing criteria for sharing supply chain risk information among federal and nonfederal entities.

As of June 2020, FASC had taken steps to address federal requirements related to the management of ICT supply chain risks, including the following:

- In April 2019, the Director of OMB designated the Federal Chief Information Security Officer as the chairperson of FASC.
- According to officials in OMB's Office of the Chief Information Officer (CIO), the strategic plan was finalized in June 2020. The plan is

[28] In fiscal year 2018, U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement Homeland Security Investigations seized 213 shipments of computer networking equipment affixed with counterfeit trademarks with a total manufacturer suggested retail price value of nearly $15.5 million. This is a 25 percent increase in the number of seizures of computer networking equipment, and a 112 percent increase in manufacturer suggested retail price value over the previous fiscal year. The networking equipment seized allegedly violated a total of seven trademarks recorded with the Customs and Border Protection and occurred at 21 ports around the country.

[29] Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE Technology Act), Federal Acquisition Supply Chain Security Act of 2018, Pub. L. No. 115-390, § 201, 132 Stat. 5173, 5178 (2018).

intended to, among other things, establish requirements for sharing relevant information about supply chain risks with all federal agencies.

- The council is developing information and criteria to assist agencies with managing their ICT supply chain risks, including developing a SCRM policy. According to officials in OMB's Office of the CIO, the council expects to complete this effort by December 2020.

FASC has also collaborated with an ICT SCRM task force established by DHS's CISA in 2018.[30] For example, most of the agencies with representatives on the council also have participated in the task force's efforts. Among other things, FASC and the task force have identified current SCRM efforts at federal agencies and compiled related insights that could help the council to develop recommendations regarding SCRM policy. For example, in September 2019, DHS reported that the task force made a policy recommendation to FASC that ICT be purchased only from original manufacturers or their authorized resellers.[31]

Federal Policy Directs Agencies to Implement SCRM and NIST Guidance Identifies Practices for Managing ICT Supply Chain Risks

Federal agencies are responsible and accountable for the risk incurred with their growing dependence on products and services that interface with or operate in a global marketplace. For example, federal policy requires agencies to provide for managing the risks to the supply chain. Specifically, in July 2016, OMB Circular A-130, "Managing Information as a Strategic Resource," directed agencies to implement SCRM principles to protect against supply chain risks, such as the insertion of counterfeits, unauthorized production, tampering, the insertion of malicious software,

[30] The ICT SCRM task force is responsible for providing a forum to collaborate with private sector owners and operators of ICT critical infrastructure. This includes providing advice and recommendations to DHS on the means for assessing and managing risks associated with the ICT supply chain. The task force has constituent working groups that are comprised of sector members, subject matter experts from those sectors, and representatives from across the federal government.

[31] CISA, *Interim Report,* (September 2019).

as well as poor manufacturing and development practices throughout the system development life cycle.[32]

In addition, the *Federal Information Security Management Act of 2002* assigns NIST the responsibility for providing standards and guidelines pertaining to federal information systems.[33] As such, NIST developed guidance to assist agencies with establishing a capability to effectively manage their ICT supply chain risks. This guidance calls for a multi-tiered approach to SCRM, with activities at the information system, mission/business, and organization level. SCRM activities at the organization level provide the foundation for activities at the system and mission/business process levels. For example:

- NIST's cybersecurity framework outlines a risk-based approach to managing cybersecurity risk and protecting an organization's critical information assets.[34] The framework includes SCRM practices, such as establishing processes to assess ICT supply chain entities and using contracts with suppliers to implement appropriate measures designed to meet risk management objectives.[35]
- NIST Special Publication 800-161 integrates ICT SCRM-specific practices into federal agency risk management activities. This publication provides guidance to federal agencies on establishing a comprehensive approach to identifying, assessing, and mitigating ICT supply chain risks at all levels of their organizations.[36] The guidance also specifies several control activities that organizations could use to provide additional supply chain protections, such as conducting due

[32] OMB, Circular A-130: *Managing Information as a Strategic Resource* (Washington, D.C.: July 2016).

[33] *Federal Information Security Modernization Act of 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). The FISMA 2002 provisions regarding NIST standards continue in full force and effect.

[34] *The Cybersecurity Enhancement Act of 2014* (Pub. L. No. 113-274 (Dec. 18, 2014) and Executive Order No. 13636, 78 Fed. Reg. 11,739 (Feb. 19, 2013) are the basis for the NIST cybersecurity framework.

[35] NIST, *Framework for Improving Critical Infrastructure Cybersecurity,* v. 1.1 (Apr. 16, 2018).

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

diligence reviews of suppliers and developing acquisition policy, and implementing procedures that help protect against supply chain threats throughout the system development life cycle.

- NIST Special Publication 800-37 (Revision 2) provides guidance for implementing NIST's risk management framework for information systems. Among other things, the guidance integrates security-related SCRM concepts into the risk management framework to help promote a comprehensive approach to managing security and privacy risk.[37]
- NIST Special Publication 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.[38]

Table 2 describes the seven selected practices from NIST's guidance that we identified as providing a foundation for managing ICT supply chain risks.

Table 2: Selected Foundational Practices for Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM)

Practice	Description
Establish executive oversight of ICT SCRM activities	Effective ICT SCRM requires commitment, direct involvement, and ongoing support from senior leaders and executives. Federal agencies should designate responsibility for leading agency-wide SCRM activities to an executive-level individual, office (supported by an expert staff), or group (e.g., a risk board, executive steering committee, or executive leadership council) regardless of an agency's specific organizational structure. Because ICT supply chain risks can be present across every major business line, agencies should ensure that SCRM roles and responsibilities are defined for senior leaders who participate in supply chain activities (e.g., acquisition and procurement, information security, information technology, legal, program management, and supply chain and logistics). Without establishing executive oversight of SCRM activities, agencies are limited in their ability to make risk decisions across the organization about how to most effectively secure their ICT product and service supply chains.

[37] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST Special Publication 800-37, Revision 2 (December 2018).

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

Practice	Description
Develop an agency-wide ICT SCRM strategy	An agency-wide ICT SCRM strategy establishes a solid foundation for managing supply chain risks by, among other things, providing the organizational context in which risk-based decisions will be made. Federal agencies should develop an agency-wide ICT SCRM strategy. The strategy should make explicit the agency's risk tolerance in clear and unambiguous terms—that is, the degree of ICT supply chain risk or uncertainty that is acceptable to an organization. The strategy also should identify how federal agencies intend to assess, respond to, and monitor ICT supply chain risks across the life cycle of ICT products and services. In the absence of an organizational strategy, decision makers can have divergent perspectives on how to manage ICT supply chain risks. This can impede a common understanding of how mission or business function risks as well as information system risks contribute to organizational risk.
Establish an approach to identify and document agency ICT supply chain(s)	Knowing who and what is in the ICT supply chains of organizations is critical to gaining visibility into what is happening within these supply chains, as well as monitoring and identifying high-risk events and activities. Federal agencies should establish an approach to identify and describe or depict information about their ICT supply chains that includes, as relevant, suppliers, manufacturing facilities, logistics providers, distribution centers, distributors, wholesalers, and other organizations involved in the manufacturing, operation, management, processing, design and development, handling, and delivery of products and services. Without reasonable visibility and traceability into supply chains (i.e., elements, processes, and actors), organizations are challenged in their ability to understand and manage risk and reduce the likelihood that adverse events will occur.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Risk assessment is one of the fundamental components of organizational risk management and federal agencies should establish a process for conducting agency-wide risk assessments that identify, aggregate, and prioritize ICT supply chain risks that are present across the organization. The assessment should result in a determination of agency-wide risk that takes into consideration the criticality and interconnected nature of ICT products and services. These assessments should be updated at an organizationally-defined frequency in order to ensure that executives and senior leaders have timely and relevant information to make ongoing risk-based decisions. Without a process for agency-wide ICT supply chain risk assessments, agencies are limited in their ability to identify systemic weaknesses or deficiencies in multiple ICT products and services and to assess the overall risks that these present to operations, assets, and individuals.
Establish a process to conduct a SCRM review of a potential supplier	Reviews of potential suppliers can provide organizations with increased levels of visibility into supplier activities to promote more effective SCRM. Federal agencies should establish an organizational process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order.[a] This process may include reviews of the processes used by suppliers to design, develop, test, implement, verify, deliver, and support ICT products and services. In addition, the process may incorporate reviews to ensure that primary suppliers have security safeguards in place, including a practice for vetting subordinate suppliers (e.g., second- and third-tier suppliers, and any subcontractors). Without a process for reviewing risks associated with the potential use of suppliers (and their subordinate suppliers), agencies lack an important vehicle for protecting the ICT supply chain early in the life cycle of products and services.

Practice	Description
Develop organizational ICT SCRM requirements for suppliers	Determining whether the risks associated with the use of ICT products and services are acceptable depends, in part, on the level of assurance that federal agencies can gain from their suppliers. Federal agencies should develop organizational ICT SCRM requirements for inclusion in contracts that are tailored to the type of contract and business needs. Requirements can address, for example, the agency's rules for suppliers' development methods, techniques, or practices; the use of secondary market components[b]; the prohibition of counterfeit products; the disposal[c] or retention of elements such as components, data, or intellectual property; and ensuring adequate supply of components. Communication requirements can also be defined that enforce early notification to agencies of ICT supply chain-related events occurring in the supplier environment (e.g., security incidents; new or updated components; the addition, replacement, or removal of supplier personnel; and new operating system rollouts, hardware upgrades, or replacements). Without organizational ICT supply chain security requirements for inclusion in contracts, agencies lack an essential mechanism to ensure that suppliers (and their suppliers) are adequately addressing risks associated with ICT products and services.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Ensuring the authenticity and integrity of acquired products—including new products, replacement parts, and existing products that require upgrades—is an essential element of ICT SCRM. Federal agencies should develop organizational procedures to detect ICT products that are counterfeit and have been compromised prior to their deployment to an operational environment.[d] Agencies' procedures for identifying counterfeit and compromised products may include manual inspections of the tracking and labeling information associated with delivered products to identify inconsistencies[e] and testing to ensure that products are genuine and have not been tampered with to include unwanted functionality. Without organizational procedures for detecting counterfeit and compromised ICT products, agencies lack adequate assurance regarding the integrity, security, and quality of the products they acquire.

Source: GAO analysis based on NIST guidance. | GAO-21-171

[a] Suppliers include developers, manufacturers, or providers (e.g., contractors) of ICT products or services, product resellers, and vendors.

[b] The secondary market (or gray market) refers to the trade of parts through distribution channels that, while not necessarily prohibited by law, are unofficial, unauthorized, or unintended by the original component manufacturer.

[c] Proper disposal of information systems components can help to prevent such components from entering the secondary market.

[d] Adversaries could compromise ICT products by inserting malware or a virus into hardware, software, or firmware at various points in the supply chain, including manufacturing and distribution.

[e] Potential inconsistencies include mismatched barcodes, labels, logos, and part numbers on the component and its documentation; and mismatched bar codes and printed part numbers.

Few Federal Agencies Implemented Foundational Practices for Managing ICT Supply Chain Risks

Few of the 23 civilian CFO Act agencies had implemented the seven selected foundational practices for managing ICT supply chain risks. Further, none of the agencies had fully implemented all of the selected practices for managing such risks and 14 of the 23 agencies had not implemented any of the practices. The practice with the highest rate of implementation was implemented by only six agencies. Conversely, none of the other practices were implemented by more than three agencies. Moreover, one practice had not been implemented by any of the agencies.

Table 3 and the narrative that follows summarize the extent to which the 23 agencies implemented the practices. A full discussion of the extent to which the agencies implemented the practices is provided in appendix II.

Table 3: Extent to Which the 23 Civilian Chief Financial Officers Act Agencies Implemented Information and Communications Technology Supply Chain Risk Management (SCRM) Foundational Practices

Agency[a]	Establish executive oversight of SCRM activities	Develop agency-wide SCRM strategy	Establish an approach to identify and document agency supply chain(s)	Establish a process to conduct agency-wide assessments of supply chain risks	Establish a process to conduct a SCRM review of a potential supplier	Develop organizational SCRM requirements for suppliers	Develop organizational procedures to detect counterfeit and compromised products prior to their deployment
Agency 1	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented
Agency 2	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented
Agency 3	Fully Implemented	Fully Implemented	Not Implemented	Not Implemented	Fully Implemented	Partially Implemented	Fully Implemented
Agency 4	Not Implemented[b]	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented
Agency 5	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented
Agency 6	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented
Agency 7	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented
Agency 8	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented
Agency 9	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented
Agency 10	Not Implemented	Not Implemented	Fully Implemented	Not Implemented	Fully Implemented	Not Implemented	Not Implemented
Agency 11	Partially Implemented	Not Implemented	Not Implemented	Not Implemented	Fully Implemented	Not Implemented	Not Implemented
Agency 12	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented

Agency 13	Not Implemented	Partially Implemented	Fully Implemented	Not Implemented	Fully Implemented	Not Implemented	Not Implemented
Agency 14	Partially Implemented	Not Implemented	Fully Implemented	Not Implemented	Fully Implemented	Not Implemented	Fully Implemented
Agency 15	Fully Implemented	Partially Implemented	Partially Implemented	Not Implemented	Fully Implemented	Not Implemented	Fully Implemented
Agency 16	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented
Agency 17	Fully Implemented	Partially Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented
Agency 18	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented
Agency 19	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented
Agency 20	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Partially Implemented	Not Implemented
Agency 21	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented
Agency 22	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented
Agency 23	Not Implemented	Partially Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented	Not Implemented

● Fully implemented— the agency fully implemented all of the practice’s evaluation criteria.

◐ Partially implemented— the agency fully or partially implemented at least one, but not all, of the practice’s evaluation criteria.

◌ Not implemented— the agency did not implement any of the practice’s evaluation criteria.

Source: GAO analysis of agency data. | GAO-21-171

[a] Due to sensitivity concerns, we substituted a numeric identifier for the agency names.

[b] Subsequent to sending a draft of the limited official use only report to agency 4 for comment in July 2020, agency officials provided evidence that it had fully implemented this practice.

Establish executive oversight of ICT SCRM activities. Three agencies had fully implemented the practice, two had partially implemented the practice, and 18 had not implemented it. The three agencies that had implemented the practice were agency 3, agency 15, and agency 17. Among these agencies, for example, an executive-level office within agency 3 provided high-level oversight for the agency-wide security program, including SCRM, with support from the two divisions within the agency. The Director delegated responsibility for the SCRM program to the CIO and Chief Operating Officer. The CIO, among other things, had assigned the Chief Information Security Officer the responsibility to oversee information technology (IT) acquisition activities, including SCRM activities, and provided guidance as necessary. Additionally, stakeholders’ roles and responsibilities for SCRM decision-making had been defined, including who had the required authority to take action and who had the accountability for an action.

Two agencies—agency 11 and agency 14—had partially implemented this practice. While these agencies had assigned a program manager to lead SCRM activities, they had not yet defined SCRM roles and responsibilities for senior leaders that participate in supply chain activities across multiple organizational functions.

The remaining 18 agencies had not implemented this practice.[39] Officials at six of these agencies (agency 2, agency 5, agency 7, agency 8, agency 10, and agency 13) stated that they had established executive oversight of ICT SCRM activities; however, they were unable to demonstrate that their agencies had implemented this practice.

Develop an agency-wide ICT SCRM strategy. One agency had fully implemented this practice, four had partially implemented the practice, and 18 had not implemented it. Specifically, agency 3 had fully implemented the practice by developing its SCRM Plan, also referred to as a strategy, for establishing an organizational capability to manage ICT supply chain risks. The plan included an expression of the supply chain risk tolerance, acceptable supply chain risk mitigation strategies, and a process for consistently evaluating and monitoring supply chain risk associated with the development, acquisition, maintenance, and disposal of systems.

Four agencies—agency 13, agency 15, agency 17, and agency 23—had partially implemented this practice. For example, agency 13's Cyber Risk Management Strategy Version 1.0 included a section on SCRM that detailed the agency's process for conducting supply chain risk assessments, but did not address supply chain risk tolerance. Additionally, while the strategy discussed assessing risks associated with potential ICT hardware and software procurements, it did not cover the system development life cycle. Officials in this agency acknowledged that the agency had not taken steps to assess, mitigate, or monitor supply chain risk across the system life cycle, but recognized the need to do so.

[39] Subsequent to sending a draft of this report to agency 4 for comment in July 2020, agency officials provided evidence that it had fully implemented this practice. Specifically, on June 1, 2020, the agency established a cross-functional board of executives within the agency to lead agency-wide SCRM activities and had defined SCRM roles and responsibilities for senior leaders that participate in supply chain activities across multiple organizational functions.

The remaining 18 agencies had not implemented the practice. For example:

- Three agencies (agency 4, agency 10, and agency 20) had begun drafting an enterprise-level SCRM strategy. Officials in agency 20’s Office of the CIO stated that the agency’s strategy was expected to be completed by the end of December 2020 and that implementation of the strategy was to begin by the end of August 2021. According to officials in agency 4’s Office of the CIO, the agency’s SCRM strategy would be finalized in fiscal year 2020 and include risk tolerance levels for managing supply chain risks. Additionally, according to agency 10’s SCRM owner, the agency expected to finalize, approve, and release its SCRM strategy before the end of December 2020.
- Three agencies (agency 5, agency 8, and agency 18) stated that they had plans to establish a strategy. Specifically, officials in agency 5’s Office of the CIO stated that they planned to establish an agency-wide SCRM strategy by the end of fiscal year 2021. Officials in agency 18’s Office of the CIO stated that the agency was preparing to review and update its cybersecurity risk management strategy. As part of this effort, agency 18 planned to incorporate ICT SCRM considerations. Officials stated that they expected this effort to be completed in early 2021. Additionally, officials in agency 8’s Office of Information Technology stated that they planned to complete the SCRM strategy by the first quarter of fiscal year 2021.
- Officials in agency 6’s Office of the CIO stated that the Chief Information Security Officer, in collaboration with the Risk Management Officer, Deputy CIO of Infrastructure and Operations Office, Chief Procurement Officer, and other respective offices, were working to develop an agency-wide SCRM strategy. However, agency 6 did not provide a time frame for completing this effort.

Establish an approach to identify and document agency ICT supply chain(s). Three agencies had fully implemented this practice, one had partially implemented it, and 19 had not implemented it. Specifically, agency 10, agency 13, and agency 14 had fully implemented the practice. For example, agency 10 used an automated tool to provide insights into the agency’s existing supply chain. The tool leveraged artificial intelligence and an underlying algorithm to analyze, among other things, publicly available information about suppliers (company and product), including company summaries. The tool also provided real-time alerts for specific suppliers within the agency’s environment. According to agency 10’s SCRM owner, the agency planned to leverage this tool to inform pre-acquisition decisions. Further, agency 13 used multiple processes to document its ICT supply chain.

Agency 15 had partially implemented this practice. According to the agency's standard operating procedure for conducting supply chain risk assessments, dated April 2020, the agency planned to identify and document its suppliers of critical ICT products and services. While the procedure included templates that the agency planned to use to document this information, it did not include the process that the agency will use to identify its suppliers.

The remaining 19 agencies had not implemented this practice. For example:

- Officials in agency 20's Office of the CIO stated that this office and a cybersecurity office within the agency were working with NIST to establish an approach to identifying and documenting the agency's ICT supply chain. Officials in the agency's Office of the Chief Information Security Officer stated that a time frame for completing this effort had not yet been determined.
- Agency 6 Office of the CIO officials stated that they did not have an ICT supply chain process or plan, but were engaged in an internal evaluation and expected to have a plan in place by the end of June 2020. As of July 7, 2020, the agency had not provided an update on the status of this effort.
- Agency 4 had not yet established an approach to map the inventory of ICT assets and systems to the associated suppliers, subordinate suppliers, and purchases. Officials in agency 4's Office of the CIO stated that they planned to implement an iterative process to document and identify supply chains for products, software systems, and shared services. They expected to form an initial process by the end of fiscal year 2020.
- Officials in agency 11's Office of the CIO stated that they did not identify their supply chain maps and, as of February 2020, did not have plans to do so. These officials also stated that they had limited insight into subordinate suppliers, including their parts and locations (i.e., transportation networks and distribution centers), and that any such data on these suppliers would quickly become out-of-date.

Establish a process to conduct agency-wide assessments of ICT supply chain risks. None of the 23 agencies had established a process to conduct risk assessments that identify, aggregate, and prioritize ICT supply chain risks that are present across the organization. For example:

- Officials at four agencies (agency 3, agency 9, agency 19, and agency 20) stated that they intend to take steps to address this practice after they receive guidance from the FASC.
- According to April 2020 documentation from agency 15's Office of the CIO, the agency plans to implement a standard operating procedure that will aggregate data from assessments of suppliers and products to produce and maintain an agency-wide supply chain risk assessment.
- Officials in agency 1's Office of the CIO stated that the agency had leveraged existing risk assessment processes and expected to take steps to incorporate additional SCRM reviews into those processes.
- Officials in agency 6's Office of the CIO stated that the Chief Information Security Officer was engaged in internal discussions to determine a strategy for conducting agency-wide supply chain risk assessments.

Establish a process to conduct a SCRM review of a potential supplier. Six agencies had fully implemented this practice and 17 had not implemented it. The six agencies that had implemented the practice were agency 3, agency 10, agency 11, agency 13, agency 14, and agency 15. For example:

- Agency 15 established a process to conduct reviews of potential suppliers prior to awarding a contract or issuing an order that included obtaining and evaluating supplier information pertaining to company ownership; foreign influence and control; the processes used to design, develop, test, implement, verify, deliver, and support products and services; and whether primary suppliers and their subcontractors maintain a formal security program that addresses SCRM.
- Agency 10 manually conducted pre-acquisition assessments of public information to determine the level of risk associated with a specific product or service. The agency provided examples of completed assessments that included information regarding the product name, product's country of origin, location of vendor, and vendor history. For high-risk acquisitions, the assessment included five questions regarding system repairs, use, compensating security measures (mitigations), connection to its networks, and whether the system will be scanned for malicious code prior to connecting to an operational network.

- Agency 13's *Supply Chain Risk Assessment Guidelines* provided guidance for conducting supply chain risk assessments during the initial stages of the procurement of IT products or services. For example, the assessment included questions regarding foreign ownership; the location of facilities for delivery, design, manufacturing, packaging, and storage prior to distribution; and the means and method for delivery.

The 17 other agencies had not implemented this practice. For example:

- Agency 6 provided a draft checklist which stated that the agency had requirements that included conducting a risk assessment prior to entering into a contract; however, officials from the Office of the CIO stated that these requirements had not been finalized and implemented within the agency. This agency did not provide a time frame for when this will be finalized and implemented within the agency.
- According to agency 4's draft SCRM strategic plan, the agency intended to establish a capability in the future that is to include making risk-based decisions when acquiring ICT products and services. The agency did not provide a date by which it expected this capability to be implemented.
- Two agencies (agency 12 and agency 19) stated that they had plans to conduct risk assessments of suppliers prior to award, but did not provide details on when they intend to do so.

Develop organizational ICT SCRM requirements for suppliers. Two agencies had partially implemented this practice and 21 had not implemented it. Specifically, agency 3 and agency 20 had partially implemented this practice. For example, agency 3's *Supply Chain Risk Management Plan* stated that the agency included cybersecurity requirements in requests for proposals and contracts that, among other things, required that system integrators incorporate supplier acceptance criteria to address potential risks when applicable. The requirements also called for system integrators to properly vet third-party suppliers with respect to the agency's SCRM requirements and verify compliance. However, agency 3 did not further define the supplier acceptance criteria or mechanisms to verify compliance.

However, 21 agencies had not implemented this practice. For example:

- Officials in agency 17’s Office of the CIO stated that IT security acquisition language was included in all contracts, but the language did not include SCRM requirements.
- Officials from agency 8 stated that the agency had established an approach which ensures that necessary security and privacy requirements are addressed in IT contracts. However, the approach did not provide details on SCRM requirements that specify what the suppliers must implement to protect against supply chain threats to be included in contracts, such as rules on prohibition of counterfeit products.
- Agency 4’s Chief Information Security Officer stated that, while the agency had some specific security acquisition language in its acquisition manual, much of the language needed to be updated. Officials in the agency’s Office of the CIO also stated that the Federal Acquisition Regulatory Council (of which this agency is a member) was reviewing whether to establish a set of standardized ICT SCRM requirements that could be used across the government and tailored to specific agency requirements. The agency did not provide expected dates by which it intended to take additional actions to establish such requirements.
- Officials in agency 13 stated that the agency had language for specific procurements, but it was not standardized and it was used on an ad hoc basis depending on the risk-based assessment (as described earlier in this report).

Develop organizational procedures to detect counterfeit or compromised ICT products prior to their deployment. Three agencies had fully implemented this practice and 20 had not implemented it. Specifically, agency 3, agency 14, and agency 15 had implemented the practice. For example, agency 15 had developed procedures to detect counterfeit goods that included completing a visual inspection process of all new purchases before implementation and use.

The other 20 agencies had not implemented this practice. For example:

- Agency 6 provided a draft checklist which stated that the agency had requirements that included (1) prohibiting tainted or counterfeit products; (2) ensuring that vendors use tamper-evident packaging during shipping/warehousing; and (3) ensuring proper labeling and tagging of software packages, modules, and hardware devices. However, officials in this agency’s Office of the CIO stated that these requirements had not been finalized and implemented within the agency and did not provide a time frame for doing so.

- Agency 23's SCRM roadmap stated that the agency planned to require all new assets to undergo an assessment prior to being deployed for implementation. However, the agency had not developed procedures for detecting counterfeit and compromised ICT products prior to their deployment. According to officials from the Office of the CIO, they intended to leverage relevant federal guidance for addressing this practice once it becomes available.

Agencies Identified Various Factors That Limited Implementation of ICT SCRM Practices

Officials from the 23 agencies pointed to various factors as having limited their implementation of the foundational practices for managing supply chain risks. The most commonly cited factor was the lack of federal SCRM guidance. Specifically, 11 agencies (agency 1, agency 3, agency 4, agency 7, agency 8, agency 9, agency 12, agency 18, agency 19, agency 20, and agency 23) reported that they were waiting for federal guidance to be issued before implementing one or more of the foundational practices.[40] For example:

- Agency 4 officials from the Office of the CIO stated that they plan to finalize the agency's ICT SCRM strategy when the FASC and NIST issue relevant guidance.
- Officials in agency 19's Office of the CIO stated that the agency had not addressed any of the foundational practices because the agency was waiting for guidance from the FASC before moving forward with defining and implementing approaches for addressing ICT supply chain risks.
- Officials in agency 12's Office of the CIO reported that the agency had not implemented controls specific to addressing supply chain risks, but over the coming fiscal years, intends to establish and implement processes, policies, and procedures regarding SCRM in accordance with guidance from the FASC.

While the additional direction and guidance from the council could further assist agencies with the implementation of these practices, federal agencies currently have guidance to assist them with managing their ICT

[40] Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE Technology Act)—Title II, Federal Acquisition Supply Chain Security Act of 2018 requires the FASC, led by OMB, to work with NIST to develop standards, guidelines, and practices for federal agencies to use when addressing their ICT supply chain risks.

supply chain risks. As previously discussed in this report, federal agencies have been required by OMB to address their ICT supply chain risks since July 2016.[41] In addition, NIST has issued a number of special publications for agencies to use to manage their ICT supply chain risks. For example, NIST issued comprehensive ICT SCRM-specific guidance in April 2015 and updated its cybersecurity framework and risk management framework to include supply chain risk considerations in April and December 2018, respectively.[42]

Further, agency officials cited other factors that limited their implementation of the foundational practices:

- Three agencies (agency 14, agency 16, and agency 21) reported that they had not fully implemented foundational ICT SCRM practices due to having federated organizational structures. For example, officials in agency 14's Office of the CIO stated that they had not developed an organizational ICT SCRM strategy because the agency has highly federated missions and a variety of risk tolerances associated with these missions. However, without organization-level practices, the agency may lack consistent implementation and oversight of ICT SCRM activities, as well as an effective agency-wide view for managing ICT supply chain risks. As another example, agency 21 officials, including officials in the Office of the CIO, stated that the agency had not implemented organizational-level ICT SCRM practices because the agency's federated governance structure designated individual bureaus within the agency with responsibility for defining and employing best practices and safeguards that protect against ICT supply chain threats. However, these officials noted that they are planning to move towards establishing a program that provides oversight of SCRM capabilities across the agency.
- Agency 22's Chief Information Security Officer reported that a risk-based decision had been made to not formally stand up a SCRM program. According to this official, the agency did not have enough

[41] OMB, Circular A-130: *Managing Information as a Strategic Resource* (Washington, D.C.: July 2016).

[42] NIST, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Special Publication 800-161 (Gaithersburg, Md.: April 2015); *Framework for Improving Critical Infrastructure Cybersecurity,* v. 1.1 (April 2018); and *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST Special Publication 800-37, Revision 2 (December 2018).

systems that required supply chain protections to justify the resources that would be needed to establish such a program. However, OMB requires agencies to establish agency-wide information security programs that implement SCRM principles and consider supply chain security issues for all planning and management activities so that risks are appropriately managed.[43]

- Officials in agency 20’s Office of the CIO stated that standing up a SCRM program and defining ICT SCRM-specific roles and responsibilities for the CIO and senior leaders had not been determined due to the complex nature of these efforts.

Until agencies implement all of the foundational ICT SCRM practices, they will be limited in their ability to address supply chain risks across their organizations effectively. As a result, these agencies are at a greater risk that malicious actors could exploit vulnerabilities in the ICT supply chain. Securing the supply chain and the information it contains is essential to protecting key agency mission operations, including those related to energy, economic, transportation, communications, and financial services.

Conclusions

Successful attacks by threat actors can have a range of impacts 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. Nevertheless, the majority of the 23 agencies had not implemented any of the seven selected foundational practices for managing ICT supply chain risks. These practices included establishing executive oversight of ICT SCRM activities, developing an agency-wide SCRM strategy, and establishing a process to conduct agency-wide assessment of ICT supply chain risks. Among those agencies that had implemented any of the practices, none had fully implemented all of them. Many of the agencies said that they were waiting for forthcoming guidance from the FASC and NIST before they implemented one or more of the practices. However, federal agencies are responsible for managing the risks that arise from depending on products that interface with a global marketplace. Further, guidance currently exists to assist agencies with managing their ICT supply chain risks. Until agencies implement all of the foundational ICT

[43] OMB, Circular A-130: *Managing Information as a Strategic Resource* (Washington, D.C.: July 2016).

SCRM practices, they will continue to be vulnerable to malicious actors that could exploit the ICT supply chain risks to disrupt mission operations, cause harm to individuals, or steal intellectual property.

Recommendations for Executive Action

In the LOUO report that we issued, we made a total of 145 recommendations to the 23 civilian CFO Act agencies in our review. These recommendations called for agencies to designate responsibility for leading agency-wide SCRM activities and define SCRM roles and responsibilities for senior leaders who participate in supply chain activities; develop an agency-wide ICT SCRM strategy that makes explicit the agency's risk tolerance and identifies how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of ICT products and services; establish an approach to identify and document agency ICT supply chain(s); establish a process to conduct agency-wide assessments of ICT supply chain risks; establish a process to conduct a SCRM review of a potential supplier prior to awarding a contract or issuing an order to that supplier for ICT products and services; develop organizational ICT SCRM requirements for inclusion in contracts that are tailored to the type of contract and business needs; and develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment.

Agency Comments and Our Evaluation

We provided a draft of the LOUO version of this report to the 23 civilian CFO Act agencies for their review and comment. In response, 17 of the agencies agreed with all of the recommendations made to them. In addition, two agencies agreed with most, but not all the recommendations made to them. Further, one agency did not agree with any of the recommendations; and two agencies neither agreed nor disagreed with the recommendations, but stated that they would address them. One agency stated that it had no comments on the report. We continue to believe that all of the recommendations made in the LOUO version of the report are warranted.

In this public version of the report, we omitted the original agency comment letters reprinted in the LOUO version due to sensitivity concerns. Alternatively, three of the agencies provided new comment letters suitable for inclusion in this report.

Specifically, the Department of Education provided a letter (reprinted in appendix III) stating that it has been reviewing OMB guidance and is further developing its supply chain risk management process and documentation with the assistance of OMB. In addition, the Department of Homeland Security sent a letter (reprinted in appendix IV) which stated that it was pleased that our report had noted FASC's collaboration with an ICT SCRM task force. The department added that it remains committed to its continuing work with FASC to identify supply chain-related threats and maintain the confidentiality, integrity, and availability of departmental systems and the information contained therein. DHS also noted its concurrence with our recommendations made to the agency in the LOUO version of the report. Finally, in a letter from the U.S. Agency for International Development (reprinted in appendix V), that agency stated that it concurred with our recommendations and did not have any further comments on the report.

We are sending copies of this report to the appropriate congressional committees, the secretaries and heads of the agencies addressed in this report, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

Should you or your staffs have any questions about information discussed in this report, please contact me at (202) 512-4456 or HarrisCC@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix VI.

CCHarris

Carol C. Harris
Director, Information Technology
Management Issues

List of Requesters

The Honorable Ron Johnson
Chairman
The Honorable Gary C. Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Carolyn B. Maloney
Chairwoman
The Honorable James Comer
Ranking Member
Committee on Oversight and Reform
House of Representatives

The Honorable Mark Takano
Chairman
Committee on Veterans' Affairs
House of Representatives
The Honorable Jim Jordan
House of Representatives

Appendix I: Objective, Scope, and Methodology

Our objective was to determine the extent to which federal agencies implemented foundational information and communications technology (ICT) supply chain risk management (SCRM) practices.

In conducting this engagement, we focused on the 23 civilian agencies covered by the *Chief Financial Officers Act of 1990*.[1] This report presents a public version of a "limited official use only" (LOUO) report that we issued in October 2020.[2] A number of agencies in our review determined that the information in that report should be protected from public disclosure. Therefore, we are not releasing the LOUO report to the general public because of the sensitive information it contains.

The LOUO report included145 recommendations that we made to 23 agencies to fully implement foundational practices in their organization-wide approaches to ICT SCRM. In this public version of the report, we substituted numeric identifiers that were randomly assigned for the names of the agencies due to sensitivity concerns.

Although the information provided in this report is more limited, this report addresses the same objective as the LOUO report and is based on the same audit methodology. We provided a draft of this report to agency officials to obtain their review and comments on the sensitivity of the information contained herein. We confirmed with the agency officials that

[1] The 23 civilian *Chief Financial Officers Act of 1990* agencies are the Departments of Agriculture, Commerce, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development. There are 24 *Chief Financial Officers Act of 1990* agencies. We did not include the Department of Defense because our scope was the civilian agencies.

[2] GAO, *Information and Communications Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks,* GAO-21-164SU (Washington, D.C.: October 27, 2020).

this report can be made available to the public without jeopardizing the security of their ICT SCRM practices.

To address the objective of this review, we collected and analyzed agencies' policies, procedures, and other documentation for their non-national security systems[3] and compared them to selected foundational practices and their associated evaluation criteria from the National Institute of Standards and Technology (NIST) guidance for ICT SCRM.

To identify the foundational practices, we reviewed Special Publication 800-161: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*.[4] We also reviewed NIST guidance as of February 2020, including the *Framework for Improving Critical Infrastructure Cybersecurity*;[5] Special Publication 800-37: *Risk Management Framework for Information Systems and Organizations*;[6] Special Publication 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*;[7] Special Publication 800-30: *Information Security: Guide for Conducting Risk Assessments*;[8] and

[3] According to the *Federal Information Security Modernization Act of 2014*, the term "national security system" is defined as any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function or use of which: involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, and is critical to the direct fulfillment of military or intelligence missions (with the exception of routine administrative and business application systems). Systems that do not meet any of the above criteria are considered non-national security systems.

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

[5] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, Md.: April 2018).

[6] NIST, *Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy*, NIST Special Publication 800-37 Revision 2 (December 2018).

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

[8] NIST, Information Security: Guide for Conducting Risk Assessments, Special Publication 800-30, Revision 1 (Gaithersburg, Md.: September 2012).

Special Publication 800-39: *Managing Information Security Risk: Organization, Mission, and Information System View*.[9]

From our review of the NIST guidance, we identified those practices that represented foundational practices that were of particular importance for providing an organization-wide approach to managing ICT supply chain risks. This effort resulted in our selection of seven practices.

To ensure consistent understanding and application of the practices in our evaluation, we identified specific evaluation criteria in NIST guidance that were associated with each of the selected seven practices. The seven practices and their associated evaluation criteria are listed in table 4.

Table 4: Evaluation Criteria Associated with the Selected Foundational Practices for Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM)

Practice	Evaluation criteria
Establish executive oversight of ICT SCRM activities	The agency designated responsibility for leading agency-wide SCRM activities to an executive-level individual, office (supported by an expert staff), or group (e.g., a risk board, executive steering committee, or executive leadership council) regardless of an agency's specific organizational structure. The agency defined SCRM roles and responsibilities for senior leaders who participate in supply chain activities.
Develop an agency-wide ICT SCRM strategy	The agency developed an agency-wide ICT SCRM strategy that made explicit the agency's risk tolerance in clear and unambiguous terms, and identified how it intended to assess, respond to, and monitor ICT supply chain risks across the life cycle of ICT products and services.
Establish an approach to identify and document agency ICT supply chain(s)	The agency established an approach to identify and describe or depict information about its ICT supply chains that includes, as relevant, suppliers, manufacturing facilities, logistics providers, distribution centers, distributors, wholesalers, and other organizations involved in the manufacturing, operation, management, processing, design and development, handling, and delivery of products and services.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	The agency established a process for conducting agency-wide risk assessments that identified, aggregated, and prioritized ICT supply chain risks that are present across the organization, resulted in a determination of agency-wide risk that takes into consideration the criticality and interconnected nature of ICT products and services, and updated at an organizationally-defined frequency.
Establish a process to conduct a SCRM review of a potential supplier	The agency established an organizational process for conducting a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services.
Develop organizational ICT SCRM requirements for suppliers	The agency developed organizational ICT SCRM requirements for inclusion in contracts that are tailored to the type of contract and business needs.

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

Practice	Evaluation criteria
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	The agency developed organizational procedures to detect ICT products that are counterfeit and have been compromised prior to their deployment to an operational environment.

Source: GAO analysis based on NIST guidance. | GAO-21-171

We validated our selection of the practices with internal subject matter experts and officials from NIST's Computer Security Division.

We then collected and analyzed documentation and other information from each agency related to ICT SCRM and compared it to the selected foundational practices and their associated evaluation criteria. Specifically, we:

- analyzed policies and plans for establishing executive oversight of ICT SCRM activities;
- assessed documents and plans for developing an agency-wide ICT SCRM strategy;
- reviewed approaches for identifying and documenting agency ICT supply chains;
- reviewed documents pertaining to conducting agency-wide ICT supply chain risk assessments;
- assessed policies and procedures for conducting a SCRM review of a potential supplier;
- analyzed documentation regarding organizational ICT SCRM requirements for suppliers; and
- reviewed procedures for detecting counterfeit and compromised ICT products prior to their deployment.

We supplemented our analyses with interviews of relevant agency officials to discuss their activities regarding ICT SCRM. We provided the results of our initial analysis of agency documentation to agency officials to corroborate our findings, collect additional evidence, and identify causes for any gaps. We then determined whether the evidence provided by the agency addressed the evaluation criteria of a practice. To determine an overall rating for each of the seven practices, we summarized the results of our assessments as:

- fully implemented—the agency fully implemented all of the practice's evaluation criteria;

- partially implemented—the agency fully or partially implemented at least one, but not all, of the practice's evaluation criteria; and
- not implemented—the agency did not implement any of the practice's evaluation criteria.

The performance audit upon which this report is based was conducted from December 2018 to October 2020 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We worked with the agencies from September 2020 to December 2020 to prepare this version of the original LOUO report for public release. This public version was also prepared in accordance with those standards.

Appendix II: Detailed Assessments of Agencies' Implementation of ICT Supply Chain Risk Management Practices

The tables in this appendix summarize the results of our assessments of the 23 civilian Chief Financial Officers Act agencies' implementation of information and communications technology (ICT) supply chain risk management (SCRM) foundational practices.[1]

Agency 1

Table 5: Agency 1's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Not implemented	Agency 1 did not establish executive oversight of ICT SCRM activities. Officials from the Office of the Chief Information Officer (CIO) stated that the CIO would be responsible for leading an approach to managing supply chain risk, but the agency had yet to define this role. In addition, the agency did not define SCRM roles and responsibilities for senior leaders who participate in supply chain activities. According to officials from the Office of the CIO, the agency intends to define roles and responsibilities for senior leaders that participate in supply chain activities, but they did not provide a time frame for doing so.
Develop an agency-wide ICT SCRM strategy	Not implemented	Agency 1 did not develop an agency-wide ICT SCRM strategy that included (1) making explicit the agency's risk tolerance in clear and unambiguous terms; and (2) identifying how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of products and services. Officials from the Office of the CIO stated that the agency's ICT SCRM was incorporated into its Cybersecurity Risk Management framework which defined the enterprise cybersecurity risk appetite and tolerance that includes supply chain protections. However, the framework did not constitute an agency-wide ICT SCRM strategy.

[1] The selected seven foundational practices were derived from the National Institute of Standards and Technology guidance.

Practice	Assessment	Discussion
Establish an approach to identify and document agency ICT supply chain(s)	Not implemented	Agency 1 did not establish an approach to identify and document the agency's ICT supply chain(s). Officials from the Office of the CIO stated that the agency had not identified and documented its ICT supply chain(s). These officials further stated that the agency was exploring leveraging a shared service to achieve this goal. This service would review upcoming and awarded contracts to determine supply chain mapping and associated risk. Officials noted that its efforts to implement this practice would be aligned with the guidance issued by the Federal Acquisition Security Council (FASC), which was pending.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 1 did not establish a process for conducting agency-wide ICT supply chain risk assessments. Officials from the Office of the CIO stated that the agency leveraged current risk assessment processes and would be taking steps to incorporate additional SCRM reviews into those processes. However, these officials did not provide details on how they incorporated supply chain risks into current risk assessments, or their plans to incorporate additional SCRM reviews into those processes.
Establish a process to conduct a SCRM review of a potential supplier	Not implemented	Agency 1 did not establish a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. Officials from the Office of the CIO stated that the agency reviewed supply chain risk issues as part of its process for reviewing gaps in security requirements documented in contracting documents, such as statements of work and performance work statements. However, the process did not include reviewing potential suppliers prior to entering into an agreement. For example, the agency did not review supplier processes used to design, develop, test, implement, verify, deliver, and support ICT products and services; and primary suppliers' security safeguards.
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 1 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. The agency provided documents on acquisition and security and privacy information for information technology procurements. However, these documents did not provide details on the organizational requirements that specified what the suppliers must implement to protect against supply chain threats to be included in contracts, including the agency's rules for suppliers' development methods, techniques, or practices; the use of secondary market components; the prohibition of counterfeit products; the disposal or retention of elements such as components, data, or intellectual property; and ensuring adequate supply of components.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 1 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. Officials from the Office of the CIO stated that the agency was working to leverage a shared service to achieve this goal and noted that its efforts to implement this practice would be aligned with the guidance issued by the FASC, which was pending.

Source: GAO analysis of agency 1 data. | GAO-21-171

Agency 2

Table 6: Agency 2's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Not implemented	Agency 2 did not establish executive oversight of ICT SCRM activities. According to agency officials, the agency established an ICT SCRM policy that places executive-level authority for ICT SCRM under the Chief Information Officer (CIO). However, the policy did not clearly designate the CIO as the designated executive-level individual for leading agency-wide SCRM activities. In addition, these officials stated that the CIO established a council for agency-wide information technology senior leaders to include initiatives on supply chain activities. However, it was not clear if this council will be designated to lead SCRM activities. These officials stated that the agency will define SCRM roles and responsibilities in the ICT SCRM strategy, which was in the process of being developed. Officials did not specify when the agency plans to finalize the ICT SCRM strategy.
Develop an agency-wide ICT SCRM strategy	Not implemented	Agency 2 did not develop an agency-wide ICT SCRM strategy that included (1) making explicit the agency's risk tolerance in clear and unambiguous terms; and (2) identifying how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of products and services. According to agency officials, the agency was in the process of developing an agency-wide ICT SCRM strategy, but did not specify when the agency plans to finalize it. In the meantime, these officials stated that the CIO, through an executive-level council, was establishing a Risk Board which will help define the risk tolerance for SCRM, and when available, these tolerances will be communicated throughout the agency, and included in the SCRM strategy.
Establish an approach to identify and document agency ICT supply chain(s)	Not implemented	Agency 2 did not establish an approach to identify and document agency ICT supply chain(s). Agency officials stated that the agency established an agency-wide approach to identify supply chains for ICT equipment, including relevant suppliers, and other providers to ensure SCRM risks are identified, assessed, and mitigated. However, officials did not provide evidence of establishing an approach to identify and document its ICT supply chain. These officials stated that the agency was in the process of identifying systems (and associated suppliers) that are critical to the resiliency of agency's essential functions and this will be reflected in the SCRM strategy, which is under development. Officials did not specify when the agency plans to finalize the ICT SCRM strategy.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 2 did not establish a process for conducting agency-wide assessments of ICT supply chain risks. Agency officials stated that the agency was completing the criticality assessments at the system, mission, and enterprise level. However, the agency did not establish a process for conducting agency-wide assessments of these ICT supply chain risks that identifies, aggregates, and prioritizes ICT supply chain risks that are present across the organization; results in a determination of agency-wide risk that takes into consideration the criticality and interconnected nature of ICT products and services; and is updated at an organizationally defined frequency to ensure that executives and senior leaders have timely and relevant information.
Establish a process to conduct a SCRM review of a potential supplier	Not implemented	Agency 2 did not establish a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. According to officials, the agency established a process for conducting reviews of potential equipment prior to purchasing, but it had not provided evidence of doing so and had not established a process to conduct reviews for ICT suppliers of the equipment prior to selection. These officials stated that supplier reviews for potential vendors may be part of implementing the ICT SCRM strategy, which was under development. However, they did not specify when they plan to finalize the ICT SCRM strategy.

Practice	Assessment	Discussion
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 2 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. According to officials, the agency had not developed organizational ICT SCRM requirements for inclusion in contracts. These officials stated while they have not developed organizational requirements for suppliers for inclusion in contracts, this may be included in the implementation of the ICT SCRM strategy, which was under development.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 2 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. According to officials, the agency established organizational procedures to detect counterfeit and compromised ICT products for equipment. However, officials did not provide evidence of procedures to detect these products. Additionally, officials stated that extending procedures to cover all ICT equipment may be a capability covered in the implementation of the agency-wide ICT SCRM strategy, which was being developed. Officials did not specify when they plan to finalize the ICT SCRM strategy.

Source: GAO analysis of agency 2 data. | GAO-21-171

Agency 3

Table 7: Agency 3's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Fully implemented	Agency 3 established executive oversight of ICT SCRM activities. An executive-level official delegated the responsibility for the agency's SCRM program to the Chief Information Officer (CIO) and Chief Operating Officer. The CIO, among other things, delegated to the Chief Information Security Officer the responsibility to oversee information technology (IT) acquisition activities including SCRM activities, and provided guidance as necessary. The agency defined its roles and responsibilities for SCRM to engage stakeholders in decision-making across multiple organizational functions including acquisition, information security, IT, legal, and supply chain.
Develop an agency-wide ICT SCRM strategy	Fully implemented	Agency 3 developed the SCRM Plan, also referred to as a strategy, for establishing an organizational capability to manage ICT supply chain risks. The strategy included an expression of risk tolerance (i.e., makes explicit the agency's limit for risk in clear and unambiguous terms). In addition, the strategy identified how the agency intends to assess, respond to, and monitor ICT supply chain risks.
Establish an approach to identify and document agency ICT supply chain(s)	Not implemented	Agency 3 did not establish an approach to identify and document the agency's ICT supply chain(s). Specifically, agency officials stated that the agency had not identified and documented the agency's ICT supply chain(s). These officials stated that they intended to define a comprehensive organizational supply chain map upon release of guidance from the Federal Acquisition Security Council (FASC).
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 3 did not establish a process for conducting agency-wide assessments of ICT supply chain risks. Agency officials stated that the agency had not conducted an agency-wide assessment and that IT procurements were centrally coordinated, which allowed acquisition personnel to review purchases and coordinate with a division for information systems and the CIO, as appropriate, for security, supply chain or sourcing concerns regarding the use of IT products and services. These officials stated that they intended to document detailed supply chain assessments upon release of guidance from the FASC.

Practice	Assessment	Discussion
Establish a process to conduct a SCRM review of a potential supplier	Fully implemented	Agency 3 established a process for conducting a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. Specifically, its SCRM plan and a cyber-espionage report detailed the process that the agency used to conduct reviews of potential suppliers. For example, the plan included questions, such as how the vendor assures security through product life cycle; what type of employee background checks are conducted and how frequently; and how the data is destroyed when the contractual agreement between the vendor and agency has dissolved.
Develop organizational ICT SCRM requirements for suppliers	Partially implemented	Agency 3 partially implemented this practice. Specifically, the Supply Chain Risk Management Plan stated that the agency had cybersecurity requirements included in requests for proposals and contracts. The agency required, among other things, that system integrators incorporate supplier acceptance criteria to address potential risks when applicable, properly vet third-party suppliers with respect to its SCRM requirements and verify compliance, and incorporate audit supply chain-relevant events within system boundaries using appropriate audit mechanisms. However, the agency did not further define the supplier acceptance criteria or mechanisms used to incorporate audit supply chain-relevant events within system boundaries.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Fully implemented	Agency 3 developed organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. The procedures included using tools and techniques—such as visual and physical inspections, proposal reviews, vulnerability management scanning, and independent third-party penetration testing of IT systems—prior to accepting and updating (e.g., deploying a patch or an upgrade of an ICT component).

Source: GAO analysis of agency 3 data. | GAO-21-171

Agency 4

Table 8: Agency 4's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Not implemented	Agency 4 did not establish executive oversight of ICT SCRM activities. Officials from the Office of the Chief Information Officer (CIO) acknowledged that they had not established executive oversight of SCRM activities and stated that they planned to take steps to implement this practice by June 2020. These steps included designating an executive to lead the agency's approach to SCRM and establishing an executive-level board to set priorities for internal, agency-wide SCRM activities. Officials also stated that the executive-level board would be responsible for facilitating a coordinated response to managing supply chain risks across the agency's responsible business units. As of July 7, 2020, the agency had not provided an update on the status of this effort.[a]
Develop an agency-wide ICT SCRM strategy	Not implemented	Agency 4 did not develop an agency-wide ICT SCRM strategy that included (1) making explicit the agency's risk tolerance in clear and unambiguous terms; and (2) identifying how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of products and services. According to officials from the Office of the CIO, the agency intends to finalize an enterprise-level SCRM strategy in fiscal year 2020 that includes risk tolerance levels for managing supply chain risks. Officials noted that they would finalize the SCRM strategy after the Federal Acquisition Security Council (FASC) issues and the National Institute of Standards and Technology (NIST) updates their respective guidance for managing supply chain risks, which was pending.

Practice	Assessment	Discussion
Establish an approach to identify and document agency ICT supply chain(s)	Not implemented	Agency 4 did not establish an approach to identify and document the agency's ICT supply chain(s). Officials from the Office of the CIO stated that the agency maintained an inventory of its ICT products and services but did not map the inventory's items to their respective suppliers, sub-suppliers, and purchases. Agency officials from the Office of the CIO stated that they will implement an iterative process to document and identify supply chains for products, software systems, and shared services. They expected to form an initial process by the end of fiscal year 2020.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 4 did not establish a process for conducting agency-wide ICT supply chain risk assessments. Officials from the Office of the CIO stated that the agency had assessed supply chain risks associated with specific systems but had not established a process to conduct agency-wide assessments. These officials stated that they planned to implement this practice after the FASC issues and NIST updates their respective SCRM guidance, which was pending for both entities.
Establish a process to conduct a SCRM review of a potential supplier	Not implemented	Agency 4 did not establish a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. The agency's draft strategic plan for managing supply chain risks stated that the agency intends to implement this practice in the future.
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 4 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. The agency's draft strategic plan for managing supply chain risks stated that the agency plans to integrate SCRM considerations into contracts with suppliers in the future. The Chief Information Security Officer stated that while the agency had some specific security acquisition language in its acquisition manual, much of the language would be updated to align with the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act of 2018.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 4 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. Officials from the Office of the CIO stated that the agency had a number of initiatives in place related to implementing this practice. However, the documents provided by officials regarding these initiatives did not include procedures for detecting counterfeit or compromised products.

Source: GAO analysis of agency 4 data. | GAO-21-171

[a] Subsequent to sending a draft of the limited official use only report to agency 4 for comment in July 2020, agency officials provided evidence that it had fully implemented this practice. Specifically, on June 1, 2020, the agency established a cross-functional board of executives within the agency to lead agency-wide SCRM activities and had defined SCRM roles and responsibilities for senior leaders that participate in supply chain activities across multiple organizational functions.

Agency 5

Table 9: Agency 5's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Not implemented	Agency 5 did not establish executive oversight of ICT SCRM activities. According to officials in the Office of the Chief Information Officer (CIO), they are incorporating SCRM roles and responsibilities into two draft policies but have currently placed this effort on hold until the second half of fiscal year 2020. These officials stated that they expect to issue the policies by the fourth quarter of fiscal year 2021 that would define SCRM roles and responsibilities.

Practice	Assessment	Discussion
Develop an agency-wide ICT SCRM strategy	Not implemented	Agency 5 did not develop an agency-wide ICT SCRM strategy that included (1) making explicit the agency's risk tolerance in clear and unambiguous terms; and (2) identifying how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of products and services. According to officials from the Office of the CIO, they plan to establish an agency-wide SCRM strategy by the end of fiscal year 2021.
Establish an approach to identify and document agency ICT supply chain(s)	Not implemented	Agency 5 did not establish an approach to identify and document the agency's ICT supply chain(s). Specifically, officials from the Office of the CIO stated that they have not mapped their ICT supply chain(s), but will document the agency's ICT supply chain(s) by the end of fiscal year 2021.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 5 did not establish a process for conducting agency-wide ICT supply chain risk assessments. Officials from the Office of the CIO will modify existing cyber risk assessments and risk management procedures to include SCRM activities. These officials also stated that the agency will conduct agency-wide ICT supply chain risk assessments in the first quarter of fiscal year 2021.
Establish a process to conduct a SCRM review of a potential supplier	Not implemented	Agency 5 did not establish a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. Officials from the Office of the CIO stated that many supply chain risk activities are coordinated with contractors across the agency, but implementation is inconsistent across all offices. While these officials stated that the agency's contracting desk book provides procedures, guidance and information to personnel that addresses, among other things, market research and U.S. ownership and citizenship, it does not define the process for reviewing the processes used by potential suppliers, including that primary suppliers have security safeguards in place and including a practice for vetting subordinate suppliers. These officials stated that the agency's existing contracting guidance will be updated to include potential and actual subordinate suppliers (e.g., second-/third-tier suppliers and subcontractors), to address ICT product and service selection, and support and enforce ICT SCRM activities by the end of the second quarter in fiscal year 2021.
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 5 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. According to a regulation on system and information integrity, the agency should document and include system and information integrity requirements in contracts, such as protections against malicious code and other types of attacks. However, it did not provide details on the organizational requirements that specify what the suppliers must implement to protect against supply chain threats to be included in contracts, such as rules on prohibition of counterfeit products. According to officials from the Office of the CIO, the agency is developing contract language to address subordinate supplier requirements and will incorporate guidance developed by the Department of Defense and the National Aeronautics and Space Administration to support and enforce ICT SCRM activities by the end of fiscal year 2021.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 5 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. While an agency regulation on system and information integrity addressed achieving system and information integrity, it did not include procedures to detect and prevent counterfeit and compromised ICT products from being used by the agency. Officials from the Office of the CIO stated that the agency plans to develop cost effective procedures for suppliers and subordinate suppliers to gain assurance that information technology products are authentic and have not been maliciously modified by the end of fiscal year 2021.

Source: GAO analysis of agency 5 data. | GAO-21-171

Agency 6

Table 10: Agency 6's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Not implemented	Agency 6 did not establish executive oversight of ICT SCRM activities. Officials from the Office of the Chief Information Officer (CIO) acknowledged that they had not established executive oversight of SCRM activities and instead its policy assigned responsibility for managing supply chains risks to program offices and system owners. These officials further stated that the agency's Chief Information Security Officer would be designated with responsibility for leading SCRM activities in the future. These officials also noted that they planned to ensure that senior leaders who participate in supply chain activities were collectively engaged in managing supply chain risks.
Develop an agency-wide ICT SCRM strategy	Not implemented	Agency 6 did not develop an agency-wide ICT SCRM strategy that included (1) making explicit the agency's risk tolerance in clear and unambiguous terms; and (2) identifying how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of products and services. Officials from the Office of the CIO acknowledged that they had not developed an agency-wide ICT SCRM strategy. They also stated that the agency's Chief Information Security Officer was in the process of developing a strategy with input from executives responsible for infrastructure and operations, procurements, and risk management.
Establish an approach to identify and document agency ICT supply chain(s)	Not implemented	Agency 6 did not establish an approach to identify and document the agency's ICT supply chain(s). Officials from the Office of the CIO stated that they expected to implement this practice by the end of June 2020. As of July 7, 2020, the agency had not provided an update on the status of this effort.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 6 did not establish a process for conducting agency-wide ICT supply chain risk assessments. Officials from the Office of the CIO stated that the agency's Chief Information Security Officer was engaged in internal discussions with stakeholders to develop a strategy for implementing this practice.
Establish a process to conduct a SCRM review of a potential supplier	Not implemented	Agency 6 did not establish a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. The agency provided a draft checklist that stated it has enacted requirements internally that include conducting a risk assessment prior to entering into a contract, but officials from the Office of the CIO stated that these requirements had not been finalized and implemented within the agency. The agency did not provide a time frame for when this will be finalized and implemented.
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 6 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. Officials from the Office of the CIO provided a draft checklist that outlined an initial set of contract requirements specific to SCRM. However, these officials stated that they would consult with internal procurement officials before finalizing the requirements and placing them in policy.

Practice	Assessment	Discussion
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 6 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. While the agency developed a handbook that is focused on acquiring services and systems, the handbook did not address this practice. The agency also provided a draft checklist that stated it had enacted requirements internally that include (1) prohibiting tainted or counterfeit products; (2) ensuring that vendors use tamper-evident packaging during shipping/warehousing; and (3) ensuring proper labeling and tagging of software packages, modules, and hardware devices. However, agency officials from the Office of the CIO stated that these requirements had not been finalized and implemented within the agency and did not provide a time frame for doing so.

Source: GAO analysis of agency 6 data. | GAO-21-171

Agency 7

Table 11: Agency 7's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Not implemented	Agency 7 did not establish executive oversight of ICT SCRM activities. While the agency had governance boards with responsibilities related to cybersecurity risks, it had not designated responsibility for leading agency-wide SCRM activities. Agency officials, including those from the Office of the Chief Information Officer (CIO) stated that the current practices of the agency's boards must be outlined in agency policy to formally establish executive oversight of ICT SCRM activities, and the agency intends to start this activity by the fourth quarter of fiscal year 2020. In addition, these officials stated that the agency ensured risk management decision making was a collaborative effort that involved senior leaders. However, the agency had not defined SCRM roles and responsibilities for senior leaders that participate in supply chain activities (e.g., acquisition and procurement, finance, human resources, information security, information technology (IT), legal, and supply chain and logistics).
Develop an agency-wide ICT SCRM strategy	Not implemented	Agency 7 did not develop an agency-wide ICT SCRM strategy that included (1) making explicit the agency's risk tolerance in clear and unambiguous terms; and (2) identifying how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of products and services. Agency officials, including those from the Office of the CIO, stated that the agency had an enterprise risk management process which balanced all perceived risk(s) into a single, agency-wide strategy for awareness and mitigation efforts, and supply chain risks are considered as part of this strategy. These officials stated that they intend to develop an ICT SCRM strategy, but did not provide time frames for doing so.
Establish an approach to identify and document agency ICT supply chain(s)	Not implemented	Agency 7 did not establish an approach to identify and document the agency's ICT supply chain(s). Agency officials, including those from the Office of the CIO, stated that the agency had not established an approach to identify and document agency ICT supply chains, but cited plans to do so. Specifically, these officials stated that the agency had multiple data sources available to inform and track items associated with its supply chain and plans to automate the links to provide a traceable mechanism to establish an approach to identify and document the supply chain. However, these officials did not provide an estimated time frame.

Practice	Assessment	Discussion
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 7 did not establish a process for conducting agency-wide ICT supply chain risk assessments. According to agency officials, including those from the Office of the CIO, the agency conducted IT supply chain risk assessments for high-impact systems. However, the agency did not provide evidence of this occurring. Additionally, these officials stated that the agency will use its traceable data repository to establish assessments and reports associated with ICT SCRM, but did not provide any plans in how it intends to do this.
Establish a process to conduct a SCRM review of a potential supplier	Not implemented	Agency 7 did not establish a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. Agency officials, including those from the Office of the CIO, stated that the agency had refined the approach for evaluating potential suppliers, which included a cybersecurity subject matter expert review prior to purchasing equipment. However, this evaluation approach did not include supplier processes used to design, develop, test, implement, verify, deliver, and support ICT products and services; and primary suppliers' security safeguards, including practices for vetting subordinate suppliers (e.g., second- and third-tier suppliers, and any subcontractors).
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 7 did not develop organizational ICT SCRM requirements for suppliers for inclusion in contracts with suppliers. An agency's management directive stated that all its IT-related contracts shall include cybersecurity requirements identifying the personnel security and system security requirements for contractors and any subcontractors, including contractor background checks and access approval clauses. However, the directive did not provide details on the organizational requirements that specifies what the suppliers must implement to protect against supply chain threats to be included in contracts, including the agency's rules for suppliers' development methods, techniques, or practices; the use of secondary market components; the prohibition of counterfeit products; the disposal or retention of elements such as components, data, or intellectual property; and ensuring adequate supply of components.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 7 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. While the agency's excerpt from its periodic system cybersecurity assessment report stated that the agency employs analysis of vendors, suppliers, and countries of origin in the supply chain to ensure that system components are not manufactured with embedded spyware or by incorporating counterfeit elements, the report was specific to systems instead of organizational procedures. Additionally, the report did not describe any organizational procedures on how the agency detects counterfeit and compromised ICT products.

Source: GAO analysis of agency 7 data. | GAO-21-171

Agency 8

Table 12: Agency 8's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Not implemented	Agency 8 did not establish executive oversight of ICT SCRM activities. While officials from its information technology office stated that the responsibilities for SCRM was a collaborative effort between two offices, the agency had not designated responsibility for leading agency-wide SCRM activities to an executive-level individual, office, group, or its governance boards. In addition, it had not defined a set of SCRM roles and responsibilities for senior leaders who participate in supply chain activities. Agency officials stated that the agency planned to use its governance boards to review and assess all risks, including supply chain risks, but did not yet have a formal SCRM program in place.

Practice	Assessment	Discussion
Develop an agency-wide ICT SCRM strategy	Not implemented	Agency 8 did not develop an agency-wide ICT SCRM strategy that included (1) making explicit the agency's risk tolerance in clear and unambiguous terms; and (2) identifying how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of products and services. Officials from the agency's information technology office stated that the agency planned to complete the SCRM strategy by the first quarter of fiscal year 2021.
Establish an approach to identify and document agency ICT supply chain(s)	Not implemented	Agency 8 did not establish an approach to identify and document the agency's ICT supply chain(s). Agency officials stated that the agency could benefit from continued close alignment between the executive and legislative branch knowing information about vendors that could be potentially high risk, but did not cite plans to establish an approach to identify and document agency ICT supply chains.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 8 did not establish a process for conducting agency-wide assessments of ICT supply chain risks. According to officials, the agency's policies and procedures for conducting risk assessments did not include any specific language related to assessments of ICT supply chain risks. These officials stated that the agency planned to conduct an assessment of the supply chain risk associated with focusing on critical systems, encompassing an analysis of threats, vulnerabilities, the likelihood of an event, and the potential consequences of an event. However, these officials did not provide a time frame for doing so.
Establish a process to conduct a SCRM review of a potential supplier	Not implemented	Agency 8 did not establish a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. Specifically, the agency's risk management framework for its information systems dated March 10, 2015 did not provide details on the process for conducting reviews of potential suppliers prior to entering into an agreement.
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 8 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. Agency officials provided documents that they stated constituted the agency's approach to ensuring the necessary security and privacy requirements were addressed in ICT contracts. However, these documents did not identify ICT SCRM requirements for suppliers, such as rules for prohibition of counterfeit products.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 8 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. While the agency provided documents that stated that its contractors must (1) provide only new equipment and new parts for the required products (i.e., no used, refurbished, or remanufactured equipment or parts); and (2) implement security safeguards, including the use of tamper-evident packages during shipping/warehouse, the documents did not describe any organizational procedures on how the agency detects counterfeit and compromised ICT products.

Source: GAO analysis of agency 8 data. | GAO-21-171

Agency 9

Table 13: Agency 9's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Not implemented	Agency 9 did not establish executive oversight of ICT SCRM activities. Specifically, it had not designated an executive-level individual, office or group with responsibility for leading agency-wide SCRM activities; and had not defined SCRM roles and responsibilities for senior leaders that participate in these activities. According to officials from the Office of the Chief Information Officer (CIO), the agency was awaiting guidance from the Federal Acquisition Security Council (FASC) to assist with establishing an ICT SCRM governance structure.
Develop an agency-wide ICT SCRM strategy	Not implemented	Agency 9 did not develop an agency-wide ICT SCRM strategy that included (1) making explicit the agency's risk tolerance in clear and unambiguous terms; and (2) identifying how federal agencies intend to assess, respond to, and monitor ICT supply chain risks across the life cycle of ICT products and services. According to officials from the Office of the CIO, the agency had not established strategies for managing ICT supply chain risk, but will do so upon receiving guidance from the FASC.
Establish an approach to identify and document agency ICT supply chain(s)	Not implemented	Agency 9 did not establish an approach to identify and document the agency's ICT supply chain(s). According to officials from the Office of the CIO, the agency was awaiting guidance from the FASC to establish a governance structure.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 9 did not establish a process for conducting agency-wide assessments of ICT supply chain risks. According to officials from the Office of the CIO, the agency is awaiting guidance from the FASC to assist with establishing a process to conduct agency-wide assessments of ICT supply chain risks.
Establish a process to conduct a SCRM review of a potential supplier	Not implemented	Agency 9 did not establish a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. According to officials from the Office of the CIO, the agency was awaiting guidance from the FASC to establish a governance structure.
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 9 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. According to officials from the Office of the CIO, the agency was awaiting guidance from the FASC to establish a governance structure.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 9 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. According to officials from the Office of the CIO, the agency was awaiting guidance from the FASC to establish a governance structure.

Source: GAO analysis of agency 9 data. | GAO-21-171

Agency 10

Table 14: Agency 10's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Not implemented	Agency 10 did not establish executive oversight of ICT SCRM activities. The agency outlined a draft set of responsibilities for establishing an organizational capability to manage supply chain risks. For example, the agency Chief Information Officer would be responsible for maintaining an effective SCRM capability, and the agency's SCRM owner would be responsible for developing a SCRM strategy and implementation plan. However, these responsibilities had not been finalized and approved. The SCRM owner stated that the agency was taking steps to ensure that senior leaders from relevant disciplines would be collectively engaged in managing supply chain risks in the future, including stakeholders from counter intelligence, procurement, and the General Counsel's office.
Develop an agency-wide ICT SCRM strategy	Not implemented	Agency 10 did not develop an agency-wide ICT SCRM strategy that included (1) making explicit the agency's risk tolerance in clear and unambiguous terms; and (2) identifying how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of products and services. While the agency provided a handbook for managing supply chain risks that the agency stated had addressed the key elements of a SCRM strategy, this handbook did not make explicit the agency's supply chain risk tolerance. In addition, while the handbook identified how it intends to assess, respond to, and monitor supply chain risk across the life cycle of products, the agency identified this document as a draft and, therefore, it was subject to change. The SCRM owner stated that the agency would finalize, approve, and issue the SCRM strategy before the end of December 2020.
Establish an approach to identify and document agency ICT supply chain(s)	Fully implemented	Agency 10 established an approach to identify and document the agency's ICT supply chain(s). Specifically, the agency used an automated tool that provided insights into the agency's existing suppliers, including the number of connections in a particular supplier's supply chain.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 10 did not establish a process for conducting agency-wide ICT supply chain risk assessments. The SCRM owner stated that the agency would form a group that includes stakeholders from multiple business units to implement this practice. As of July 8, 2020, the agency had not determined the group's membership.
Establish a process to conduct a SCRM review of a potential supplier	Fully implemented	Agency 10 established a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. This process included obtaining and evaluating supplier information pertaining to company ownership and a product's country of origin. For acquisitions that were high risk, the agency obtained and evaluated additional information pertaining to, for example, the security measures that suppliers had in place to mitigate their supply chain risks.
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 10 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. The SCRM owner stated that the agency would leverage forthcoming Department of Homeland Security guidance to implement this practice.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 10 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. The SCRM owner stated that this practice had been addressed in agency documents, such as the agency's incident response plan. However, these documents did not include processes for detecting counterfeit or compromised products.

Source: GAO analysis of agency 10 data. | GAO-21-171

Agency 11

Table 15: Agency 11's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Partially implemented	Agency 11 partially implemented this practice. Specifically, the agency designated a SCRM program manager with responsibility for leading SCRM activities. However, it did not define SCRM roles and responsibilities for senior leaders that participate in supply chain activities across multiple organizational functions.
Develop an agency-wide ICT SCRM strategy	Not implemented	Agency 11 did not develop an agency-wide ICT SCRM strategy that included (1) making explicit the agency's risk tolerance in clear and unambiguous terms; and (2) identifying how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of products and services. According to the SCRM program manager, the agency established a Procurement Guidance Document, which included procedures for the acquisition of high- and moderate-impact information technology systems including assessments of supply chain security risks of vendors. However, this document was not an ICT SCRM strategy.
Establish an approach to identify and document agency ICT supply chain(s)	Not implemented	Agency 11 did not establish an approach to identify and document the agency's ICT supply chain(s). While the agency used labels for asset management for tracking and accountability, officials from the Office of the Chief Information Officer (CIO) stated that it did not identify and document the agency's ICT supply chain(s), and these officials did not cite any plans to do so.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 11 did not establish a process to conduct agency-wide ICT supply chain risk assessments. Officials from the Office of the CIO stated that the agency provided a capability to automate the aggregation of risk assessments but did not include a process for conducting agency-wide ICT supply chain risk assessments.
Establish a process to conduct a SCRM review of a potential supplier	Fully implemented	Agency 11 established a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. Specifically, the agency's Procurement Guidance Document included procedures for the acquisition of high- and moderate-impact information technology systems, including assessments of supply chain security risks of vendors prior to entering into an agreement.
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 11 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. The agency's Procurement Guidance document required that prior to awarding contracts, potential suppliers provide and update specific information that it needs to conduct reviews and identify any risks associated with these suppliers. However, the agency did not establish ICT SCRM requirements with which suppliers must comply (e.g., specific development, delivery, or disposal techniques that suppliers must use or the prohibition of counterfeit or secondary market goods in the supplier environment).
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 11 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. Specifically, the agency's System and Services Acquisition standards did not define procedures to detect counterfeit and compromised ICT products prior to deployment to an operational environment.

Source: GAO analysis of agency 11 data. | GAO-21-171

Agency 12

Table 16: Agency 12's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Not implemented	Agency 12 did not establish executive oversight of ICT SCRM activities. While the agency had plans for establishing executive oversight of ICT SCRM, including establishing a supply chain manager and having a SCRM executive board that includes senior leaders from across the agency (e.g., logistics, information technology, acquisition, security, human resources, and legal), it had not yet implemented these plans. Officials from the Office of the Chief Information Officer (CIO) stated that, over the coming fiscal years, the agency intends to establish and implement the processes, policies, and procedures regarding SCRM.
Develop an agency-wide ICT SCRM strategy	Not implemented	Agency 12 did not develop an agency-wide strategy that included (1) making explicit the agency's risk tolerance in clear and unambiguous terms; and (2) identifying how the agency intends to assess, respond to, and monitor ICT supply chain risks at all levels of the agency and across all phases of the life cycle of products and services. According to officials from the Office of the CIO, they had not categorized any systems as high-impact and therefore had not implemented mechanisms to protect its ICT supply chain. Nonetheless, these officials stated that, over the coming fiscal years, the agency intends to establish and implement the processes, policies, and procedures regarding SCRM.
Establish an approach to identify and document agency ICT supply chain(s)	Not implemented	Agency 12 did not establish an approach to identify and document the agency's ICT supply chain(s). According to officials from the Office of the CIO, they had not categorized any systems as high-impact and therefore had not implemented mechanisms to protect its ICT supply chain. Nonetheless, these officials stated that, over the coming fiscal years, the agency intends to establish and implement the processes, policies, and procedures regarding SCRM.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 12 did not establish a process to conduct agency-wide assessments of ICT supply chain risks. While the agency had a plan to conduct SCRM assessments, it had not yet established a process to conduct agency-wide ICT supply chain risk assessments. According to officials from the Office of the CIO, over the coming fiscal years, the agency intends to establish and implement the processes, policies, and procedures regarding SCRM.
Establish a process to conduct a SCRM review of a potential supplier	Not implemented	Agency 12 did not establish a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. While the agency had a document that states it was to conduct research and exercise due diligence regarding suppliers prior to doing business with them, as well as build an understanding of suppliers' security practices, it had not yet defined how it will do so. According to officials from the Office of the CIO, over the coming fiscal years, the agency intends to establish and implement the processes, policies, and procedures regarding SCRM.
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 12 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. The agency had a plan to ensure that contract language with key suppliers included implementation of SCRM requirements into contractual language with third party vendors and an audit capability for key suppliers' supply chain processes. However, it had not defined what these organizational ICT SCRM requirements are for suppliers, including rules for prohibition of counterfeit products. According to officials from the Office of the CIO, over the coming fiscal years, the agency intends to establish and implement the processes, policies, and procedures regarding SCRM.

Practice	Assessment	Discussion
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 12 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. According to agency officials from the Office of the CIO, they had not categorized any systems as high-impact and therefore had not implemented mechanisms to protect its ICT supply chain. According to officials, because the agency did not establish these mechanisms, it had not developed organizational procedures to detect ICT products that were counterfeit or had been subject to tampering. However, these officials stated, that over the coming fiscal years, it intends to establish and implement the processes, policies, and procedures regarding SCRM.

Source: GAO analysis of agency 12 data. | GAO-21-171

Agency 13

Table 17: Agency 13's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Not implemented	Agency 13 did not establish executive oversight of ICT SCRM activities. Agency officials stated that the agency's Chief Information Officer (CIO) had designated responsibility for assessing the agency's supply chain risk to the Chief Information Security Officer. These officials stated that the Chief Information Security Officer was also responsible for providing direction and guidance to relevant stakeholders. However, the documentation did not designate and define SCRM roles and responsibilities for the Chief Information Security Officer and the senior leaders who participate in supply chain activities.
Develop an agency-wide ICT SCRM strategy	Partially implemented	Agency 13 partially implemented this practice. Specifically, the strategy identified how the agency intended to assess risks associated with potential hardware and software procurements but did not identify how the agency intended to assess, mitigate, and monitor supply chain risk across the entire life cycle of ICT products and services. In addition, the strategy did not make explicit the agency's supply chain risk tolerance. Agency officials stated that they recognized the need to address these gaps in the future.
Establish an approach to identify and document agency ICT supply chain(s)	Fully implemented	Agency 13 established an approach to identify and document the agency's ICT supply chain(s). Specifically, the agency used multiple processes to document its ICT supply chain.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 13 did not establish a process for conducting agency-wide ICT supply chain risk assessments. Agency officials stated that the agency was focused on determining risks associated with the procurement of new ICT investments. These officials also stated that the agency had increased its cybersecurity budget and planned to invest in strengthening the agency's SCRM capabilities, which included taking steps to implement this practice.

Practice	Assessment	Discussion
Establish a process to conduct a SCRM review of a potential supplier	Fully implemented	Agency 13 established a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. Specifically, the agency's Supply Chain Risk Assessment Guidelines outlined steps for conducting supply chain risk assessments during the initial stages of the procurement of ICT products or services. This guidance included solicitation questions for potential awardees and subcontractors pertaining to, for example, foreign ownership; the location of facilities for delivery, design, manufacturing, packaging, and storage prior to distribution; the means and method for product delivery; and the provision of disposal services. The guidance stated that the agency reviews the answers provided by potential suppliers in response to the solicitation questions. The guidance also stated that the agency conducts independent investigations of the suppliers and their suppliers—investigations based on publicly available information—to identify any participation in criminal activities or subversive work for a foreign government.
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 13 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. Agency officials stated that the agency included requirements related to managing supply chain risks in contracts on an ad hoc basis when such requirements are warranted by the level of risk associated with the procurement of a specific product.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 13 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. While the agency used a tool that tracked activities related to testing software patches and upgrades, the tool was not part of an organizational procedure for detecting the range of ICT products that might be counterfeit or compromised to include unwanted functionality.

Source: GAO analysis of agency 13 data. | GAO-21-171

Agency 14

Table 18: Agency 14's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Partially implemented	Agency 14 partially implemented this practice. Specifically, the agency designated responsibility for leading agency-wide SCRM activities to the Chief Information Security Officer, also known as the SCRM program manager. While the SCRM Final Operating Capability Process document outlined the roles for those involved in the process including for the entity executives, it did not fully define SCRM roles and responsibilities for senior leaders that participate in supply chain activities across multiple organizational functions such as acquisition and procurement and legal.
Develop an agency-wide ICT SCRM strategy	Not implemented	Agency 14 did not develop an agency-wide ICT SCRM strategy that included (1) making explicit the agency's risk tolerance in clear and unambiguous terms; and (2) identifying how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of products and services. While the agency developed its SCRM Final Operating Capability Process document that identified how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of products and services, this document was not an ICT SCRM strategy. Additionally, the agency did not make explicit the agency's risk tolerance.

Practice	Assessment	Discussion
Establish an approach to identify and document agency ICT supply chain(s)	Fully implemented	Agency 14 established an approach to identify and document the agency's ICT supply chain(s). The agency established a SCRM program that enables it to evaluate the supply chain components that are the most relevant to its mission and risk tolerance, among other things.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 14 did not establish a process for conducting agency-wide assessments of ICT supply chain risks. Officials from the Office of the Chief Information Officer (CIO) stated that the agency established a process to conduct agency-wide ICT supply chain risk assessments through an 'on demand' service that was intended to provide assessments for all entities within the agency as requested, but did not provide details on the process to conduct these assessments across the agency.
Establish a process to conduct a SCRM review of a potential supplier	Fully implemented	Agency 14 established a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. The agency's SCRM process examined risks associated with vendors based on several risk factors, such as supplier management (i.e., strategy and plans on how the company manages external suppliers); quality assurance (i.e., vendor's policies/standards, testing, and consumer reviews); cybersecurity (i.e., technical vulnerabilities and instances of cyber breach or historic trends); and evaluation of physical security across the supply chain. In addition, according to officials from the Office of the CIO, the SCRM process enabled the agency to perform an analysis of vendors and associated products and/or services to understand underlying risk that vendors may pose. As of April 23, 2020, these officials stated that the agency had assessed more than 210 vendors by using assessments of potential suppliers compiled from validated data sources.
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 14 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. The agency's Cybersecurity Program policy stated that the contractor must ensure that security specifications were included in procurements of components for information technology and operational technology. However, it did not define the security specifications that suppliers must implement to protect against supply chain risks. Additionally, while the agency published a handbook on suspect and counterfeit efforts which documents that all contracts should contain clauses that prohibit counterfeit items, it stated that it was highly recommended to make it a requirement, and was thus not a requirement.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Fully implemented	Agency 14 developed organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. For example, the agency's handbook on suspect and counterfeit efforts provides information to assist the agency in preventing suspect/counterfeit ICT products prior to their deployment, including identifying and reporting requirements.

Source: GAO analysis of agency 14 data. | GAO-21-171

Agency 15

Table 19: Agency 15's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Fully implemented	Agency 15 established executive oversight of ICT SCRM activities. Specifically, the agency designated an executive-level individual to lead the agency's approach to managing supply chain risks. In April 2020, Agency 15 developed an ICT SCRM Program Charter that defined SCRM roles and responsibilities for this individual and other senior leaders who participate in supply chain activities including the SCRM program manager, Office of General Counsel, Office of Acquisition, and agency bureaus.
Develop an agency-wide ICT SCRM strategy	Partially implemented	Agency 15 partially implemented this practice. Specifically, the agency developed a strategy that discussed how it intends to assess risks and monitor supply chain risks. However, the strategy did not identify how the agency should respond to these risks. Instead, the strategy assigned its bureau Chief Information Officers (CIO) with responsibility for determining how their bureaus will respond to supply chain risks. Additionally, the strategy did not make explicit the agency's supply chain risk tolerance. The Acting CIO stated that the agency would conduct a gap analysis to determine if updates to the strategy are needed.
Establish an approach to identify and document agency ICT supply chain(s)	Partially implemented	Agency 15 partially implemented this practice. Specifically, the agency's standard operating procedure for conducting supply chain risk assessments states that the agency plans to identify and document its suppliers of critical ICT products and services. While the procedure included templates that the agency plans to use to document this information, it did not include the process that the agency will use to identify its suppliers.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 15 did not establish a process for conducting agency-wide ICT supply chain risk assessments. According to agency documentation, it plans to implement a standard operating procedure that will aggregate data from assessments of suppliers and products to produce and maintain an agency-wide supply chain risk assessment.
Establish a process to conduct a SCRM review of a potential supplier	Fully implemented	Agency 15 established a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. This process included obtaining and evaluating supplier information pertaining to company ownership; foreign influence and control; the processes used to design, develop, test, implement, verify, deliver, and support products and services; and if primary suppliers and their subcontractors maintain a formal security program that addresses SCRM.
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 15 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. Prior to awarding contracts, the agency required potential suppliers to provide and update specific information that the agency needs to conduct reviews and identify any risks associated with these suppliers. However, the agency did not establish requirements with which suppliers must comply (e.g., specific development, delivery, or disposal techniques that suppliers must use or the prohibition of counterfeit or secondary market goods in the supplier environment). The Acting CIO stated that the agency would evaluate if an update to current policy will be needed in order to implement this practice.

Practice	Assessment	Discussion
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Fully implemented	Agency 15 developed organizational guidance to detect ICT products that are counterfeit and compromised prior to their deployment to an operational environment. For example, the agency's guidance outlined steps for unpacking and completing visual inspections of all new purchases prior to their implementation and use.

Source: GAO analysis of agency 15 data. | GAO-21-171

Agency 16

Table 20: Agency 16's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Not implemented	Agency 16 did not establish executive oversight of ICT SCRM activities. While the agency's draft Policy for Cyber Supply Chain Risk Management stated that the Chief Information Officer (CIO) was responsible for ensuring the agency employs an approach to managing ICT supply chain risks, the policy was under review. Additionally, the agency did not fully define SCRM roles and responsibilities for senior leaders who participate in supply chain activities. Agency officials from the Office of the CIO stated that the SCRM policy was scheduled to be completed in the fourth quarter of fiscal year 2020.
Develop an agency-wide ICT SCRM strategy	Not implemented	Agency 16 did not develop an agency-wide ICT SCRM strategy that included (1) making explicit the agency's risk tolerance in clear and unambiguous terms; and (2) identifying how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of products and services. While the agency developed a draft *Policy for Cyber Supply Chain Risk Management* that was intended to provide guidance on assessing and mitigating ICT supply chain risks, among other things, the policy was under review. Officials from the Office of the CIO stated that it was scheduled to be completed in the fourth quarter of fiscal year 2020.
Establish an approach to identify and document agency ICT supply chain(s)	Not implemented	Agency 16 did not establish an approach to identify and document the agency's ICT supply chain(s). Agency officials from the Office of the CIO stated that the draft SCRM policy would require the agency to identify and document maps of its supply chain(s) and was scheduled to be completed in the fourth quarter of fiscal year 2020.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 16 did not establish a process to conduct agency-wide assessments of ICT supply chain risks. Officials from the Office of the CIO stated that they used an ad hoc approach and take action when they were made aware of a potential issue or threat. Additionally, while the draft *Policy for Cyber Supply Chain Risk Management* included a reference to using risk assessment processes after the impact level had been defined, the policy was under review. Officials from the Office of the CIO stated that the draft policy was scheduled to be completed in the fourth quarter of fiscal year 2020.

Practice	Assessment	Discussion
Establish a process to conduct a SCRM review of a potential supplier	Not implemented	Agency 16 did not establish a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. The agency's policy on information systems security and privacy noted that to address the security mechanism relating to protecting the supply chain it was to employ risk reviews upon notification of supply chain threat and whenever possible select components that have been previously reviewed by other government entities. However, this policy did not describe a process to conduct reviews of potential suppliers prior to entering into an agreement. In addition, according to these officials from the Office of the CIO, they will be able to implement the supply chain related protections as appropriate once they finalize the SCRM policy, which is scheduled to be completed in the fourth quarter of fiscal year 2020.
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 16 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. Officials from the Office of the CIO stated that ICT SCRM language will be incorporated into the next version of the security and privacy language for information and information technology procurement documentation, scheduled for completion in fiscal year 2020. These officials stated that the Office of the CIO, in collaboration with the agency's Acquisitions Office, will review a sample of suppliers periodically to ensure suppliers are compliant with the SCRM policy when it is completed. The officials anticipated that the policy will be completed by the fourth quarter of fiscal year 2020.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 16 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. Agency officials from the Office of the CIO stated that the draft SCRM policy would require the agency to avoid procuring products that have potentially malicious functionality and that are vulnerable due to poor manufacturing and development practices. The officials anticipated that the policy will be completed by the fourth quarter of fiscal year 2020.

Source: GAO analysis of agency 16 data. | GAO-21-171

Agency 17

Table 21: Agency 17's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Fully implemented	Agency 17 established executive oversight of ICT SCRM activities. The agency's Office of the Chief Information Officer (CIO) manages the agency-wide supply chain program, which includes conducting supply chain risk assessments. The agency also defined SCRM roles and responsibilities for senior leaders who participate in supply chain activities.
Develop an agency-wide ICT SCRM strategy	Partially implemented	Agency 17 partially implemented this practice. Specifically, it had developed an agency-wide ICT SCRM plan, also referred to as a strategy, which identifies how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of products and services. However, the plan did not make explicit the agency's supply chain risk tolerance.

Practice	Assessment	Discussion
Establish an approach to identify and document agency ICT supply chain(s)	Not implemented	Agency 17 did not establish an approach to identify and document the agency's ICT supply chain(s). According to officials from the Office of the CIO, the Cyber Threat Intelligence team was responsible for, among other things, continuously monitoring the agency's hardware, software, and cloud services for the threat information that provides insight into the agency's existing suppliers. However, the agency did not provide details on how the team identifies and documents its ICT supply chains, including suppliers.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 17 did not establish a process for conducting agency-wide ICT supply chain risk assessments. Officials from the Office of the CIO stated that the organizational risk assessment plan includes how the agency plans to evaluate supply chain risks. However, the plan did not provide details on how these assessments are conducted to identify, aggregate, and prioritize ICT supply chain risks that are present across the organization; results in a determination of agency-wide risk that takes into consideration the criticality and interconnected nature of ICT products and services; and is updated at an organizationally defined frequency.
Establish a process to conduct a SCRM review of a potential supplier	Not implemented	Agency 17 did not establish a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. While the ICT SCRM plan identified how the agency manages supply chain risks, it did not document how it conducts SCRM reviews of potential suppliers.
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 17 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. Agency officials from the Office of the CIO stated that information technology security acquisition language was included in all contracts, but the language did not specify requirements that the suppliers must implement to protect against supply chain threats. These officials also stated that the Office of the CIO was in the process of updating this language to include evaluation requirements.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 17 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. While the agency's SCRM implementation and management plan noted that the agency tests devices for possible compromised ICT products, it did not document procedures on how the agency uses this approach.

Source: GAO analysis of agency 17 data. | GAO-21-171

Agency 18

Table 22: Agency 18's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Not implemented	Agency 18 did not establish executive oversight of ICT SCRM activities. Officials from the Office of the Chief Information Officer (CIO) stated that the agency would designate its Enterprise Risk Manager as the individual responsible for leading the agency's approach to managing supply chain risks. These officials also stated that they were considering the need to form a committee of senior leaders from relevant offices to ensure that they participate in managing supply chain risks. Officials noted that its efforts to implement this practice would be aligned with guidance issued by the Federal Acquisition Security Council (FASC), which was pending.

Practice	Assessment	Discussion
Develop an agency-wide ICT SCRM strategy	Not implemented	Agency 18 did not develop an agency-wide ICT SCRM strategy that included (1) making explicit the agency's risk tolerance in clear and unambiguous terms; and (2) identifying how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of products and services. Agency officials acknowledged that they had not developed an agency-wide ICT SCRM strategy. Officials from the Office of the CIO stated that they were preparing to review and update its cybersecurity risk management strategy to include SCRM considerations. These officials stated that they expected to complete this update in early calendar year 2021.
Establish an approach to identify and document agency ICT supply chain(s)	Not implemented	Agency 18 did not establish an approach to identify and document the agency's ICT supply chain(s). Officials from the Office of the CIO stated that they intended to mitigate the agency's risk exposure by requiring its suppliers of ICT products and services to identify and document their supply chains in accordance with federal laws and guidance established by entities such as the FASC, which was pending.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 18 did not establish a process for conducting agency-wide ICT supply chain risk assessments. Officials from the Office of the CIO stated that the agency would align any future efforts to implement this practice to guidance issued by the FASC, which was pending.
Establish a process to conduct a SCRM review of a potential supplier	Not implemented	Agency 18 did not establish a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. Officials from the Office of the CIO stated that the agency would align any future efforts to implement this practice to guidance issued by the FASC, which was pending.
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 18 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. Officials from the Office of the CIO stated that the agency would align any future efforts to implement this practice to guidance issued by the FASC, which was pending.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 18 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. Officials from the Office of the CIO stated that they plan to implement this practice after federal entities such as the National Institute of Standards and Technology update their respective SCRM guidance, which was pending.

Source: GAO analysis of agency 18 data. | GAO-21-171

Agency 19

Table 23: Agency 19's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Not implemented	Agency 19 did not establish executive oversight of ICT SCRM activities. Officials from the Office of the Chief Information Officer (CIO) acknowledged that they had not established executive oversight of SCRM activities. Instead of designating responsibility for managing supply chain risks to an agency executive and defining SCRM roles and responsibilities for senior leaders who participate in supply chain activities, the agency's policy currently designates responsibility for managing supply chain risks to lower level system owners. These officials stated that the agency would take steps to implement this practice after the Federal Acquisition Security Council (FASC) issues its guidance, which was pending.

Practice	Assessment	Discussion
Develop an agency-wide ICT SCRM strategy	Not implemented	Agency 19 did not develop an agency-wide ICT SCRM strategy that included (1) making explicit the agency's risk tolerance in clear and unambiguous terms; and (2) identifying how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of products and services. Officials from the Office of the CIO acknowledged that they had not developed an agency-wide ICT SCRM strategy and stated that the agency would take steps to develop a strategy after the FASC issues its guidance, which was pending.
Establish an approach to identify and document agency ICT supply chain(s)	Not implemented	Agency 19 did not establish an approach to identify and document the agency's ICT supply chain(s). Officials from the Office of the CIO stated that they would take steps to implement this practice after the FASC issues its guidance, which was pending.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 19 did not establish a process for conducting agency-wide ICT supply chain risk assessments. Officials from the Office of the CIO stated that the agency would take steps to implement this practice after the FASC issues its guidance, which was pending.
Establish a process to conduct a SCRM review of a potential supplier	Not implemented	Agency 19 did not establish a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. Agency policy designated responsibility for determining how and whether to conduct reviews of potential suppliers to individual system owners. Officials from the Office of the CIO stated that the agency would take steps to implement this practice after the FASC issues its guidance, which was pending.
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 19 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. According to officials from the Office of the CIO, although the agency had standard contract clauses that required contractors to comply with the agency's information technology policies, these standard clauses did not include SCRM requirements. These officials stated that the agency would take steps to implement this practice after the FASC issues its guidance, which was pending.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 19 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. Officials from the Office of the CIO acknowledged that they had not developed organizational procedures and instead, agency policy designated responsibility for implementing this practice to individual system owners. Officials stated that the agency would take steps to implement this practice after the FASC issues its guidance, which was pending.

Source: GAO analysis of agency 19 data. | GAO-21-171

Agency 20

Table 24: Agency 20's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Not implemented	Agency 20 did not establish executive oversight of ICT SCRM activities. Agency officials, including those from the Office of the Chief Information Officer (CIO) stated that the agency intends to establish a program for managing supply chain risks that would be led by the Office of the CIO. According to Office of the CIO officials, the agency has taken steps to form a working group of senior leaders to develop and implement SCRM procedures. However, the agency has not defined roles and responsibilities for the working group. These officials noted that they expect to begin to implement this practice by the end of September 2021.

Practice	Assessment	Discussion
Develop an agency-wide ICT SCRM strategy	Not implemented	Agency 20 did not develop an agency-wide ICT SCRM strategy that included (1) making explicit the agency's risk tolerance in clear and unambiguous terms; and (2) identifying how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of products and services. Officials from the Office of the CIO stated that they were in the process of developing a strategy that they plan to complete by the end of December 2020 and implement by the end of August 2021. These officials further noted that these time frames were dependent on when federal entities, such as the Federal Acquisition Security Council (FASC), issue SCRM guidance that the agency would need to incorporate into its strategy.
Establish an approach to identify and document agency ICT supply chain(s)	Not implemented	Agency 20 did not establish an approach to identify and document the agency's ICT supply chain(s). Officials from the Office of the CIO stated that they were working with the agency's various lines of business to implement this practice at a future, yet undetermined, date.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 20 did not establish a process for conducting agency-wide ICT supply chain risk assessments. According to agency officials, including officials from the Office of the CIO, they would take steps to implement this practice after they obtain adequate staffing, establish assessment capabilities, and receive guidance from the FASC.
Establish a process to conduct a SCRM review of a potential supplier	Not implemented	Agency 20 did not establish a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. According to agency officials, including officials from the Office of the CIO, the agency had taken steps toward implementing this practice. However, documents provided by these officials to support this assertion, including the agency's draft framework and process map, did not discuss an organizational process for assessing potential suppliers of ICT products and services.
Develop organizational ICT SCRM requirements for suppliers	Partially implemented	Agency 20 partially implemented this practice. Specifically, the agency developed a contract clause that requires contractors to notify the agency's security operations center in the event that they discover a prohibited product or service being used during contract performance. Officials from the Office of the Chief Procurement Officer stated that the agency had initiated an effort to develop a standard set of SCRM requirements for inclusion in contracts. However, officials did not provide a date by which they expected to complete this effort.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 20 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. Officials from the Office of the CIO stated that they were exploring how to implement this practice.

Source: GAO analysis of agency 20 data. | GAO-21-171

Agency 21

Table 25: Agency 21's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Not implemented	Agency 21 did not establish executive oversight of ICT SCRM activities. Officials from the Office of the Chief Information Officer (CIO) acknowledged that they had not established executive oversight of SCRM activities. These officials stated that the agency would establish a SCRM program that provides executive oversight of SCRM activities across the agency, but did not provide a time frame for doing so.

Practice	Assessment	Discussion
Develop an agency-wide ICT SCRM strategy	Not implemented	Agency 21 did not develop an agency-wide ICT SCRM strategy that included (1) making explicit the agency's risk tolerance in clear and unambiguous terms; and (2) identifying how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of products and services. Officials from the Office of the CIO stated that the agency would establish a SCRM program that includes an agency-wide ICT SCRM strategy to determine risk tolerance across the agency, but did not provide a time frame for doing so.
Establish an approach to identify and document agency ICT supply chain(s)	Not implemented	Agency 21 did not establish an approach to identify and document the agency's ICT supply chain(s). Officials from the Office of the CIO stated that the agency would establish a SCRM program that addresses this practice through collaboration with acquisition organizations within the agency, but did not provide a time frame for doing so.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 21 did not establish a process for conducting agency-wide ICT supply chain risk assessments. Officials from the Office of the CIO stated that the agency would establish a SCRM program that addresses this practice, but did not provide a time frame for doing so.
Establish a process to conduct a SCRM review of a potential supplier	Not implemented	Agency 21 did not establish a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. Officials from the Office of the CIO stated that the agency would establish a SCRM program that addresses this practice, but did not provide a time frame for doing so.
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 21 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. Officials from the Office of the CIO stated that the agency would establish a SCRM program that addresses this practice, but did not provide a time frame for doing so.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 21 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. Officials from the Office of the CIO stated that the agency would establish a SCRM program that addresses this practice, but did not provide a time frame for doing so.

Source: GAO analysis of agency 21 data. | GAO-21-171

Agency 22

Table 26: Agency 22's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Not implemented	Agency 22 did not establish executive oversight of ICT SCRM activities. The agency's Risk Executive Group charter and information security procedures did not designate responsibility for leading agency-wide SCRM activities to an executive-level individual or office. These documents also did not define SCRM roles and responsibilities for senior leaders who participate in supply chain activities.
Develop an agency-wide ICT SCRM strategy	Not implemented	Agency 22 did not develop an agency-wide ICT SCRM strategy that included (1) making explicit the agency's risk tolerance in clear and unambiguous terms; and (2) identifying how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of products and services. Officials from the Office of Information Security and Privacy acknowledged that they had not developed an agency-wide ICT SCRM strategy and stated that the agency did not plan to implement this practice.

Practice	Assessment	Discussion
Establish an approach to identify and document agency ICT supply chain(s)	Not implemented	Agency 22 did not establish an approach to identify and document the agency's ICT supply chain(s). Officials from the Office of Information Security and Privacy stated that they did not plan to implement this practice.
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 22 did not establish a process for conducting agency-wide ICT supply chain risk assessments. Officials from the Office of Information Security and Privacy stated that they did not plan to implement this practice.
Establish a process to conduct a SCRM review of a potential supplier	Not implemented	Agency 22 did not establish a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. Officials from the Office of Information Security and Privacy stated that they did not plan to implement this practice.
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 22 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. Officials from the Office of Information Security and Privacy stated that they did not plan to implement this practice.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 22 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. Officials from the Office of Information Security and Privacy stated that they did not plan to implement this practice.

Source: GAO analysis of agency 22 data. | GAO-21-171

Agency 23

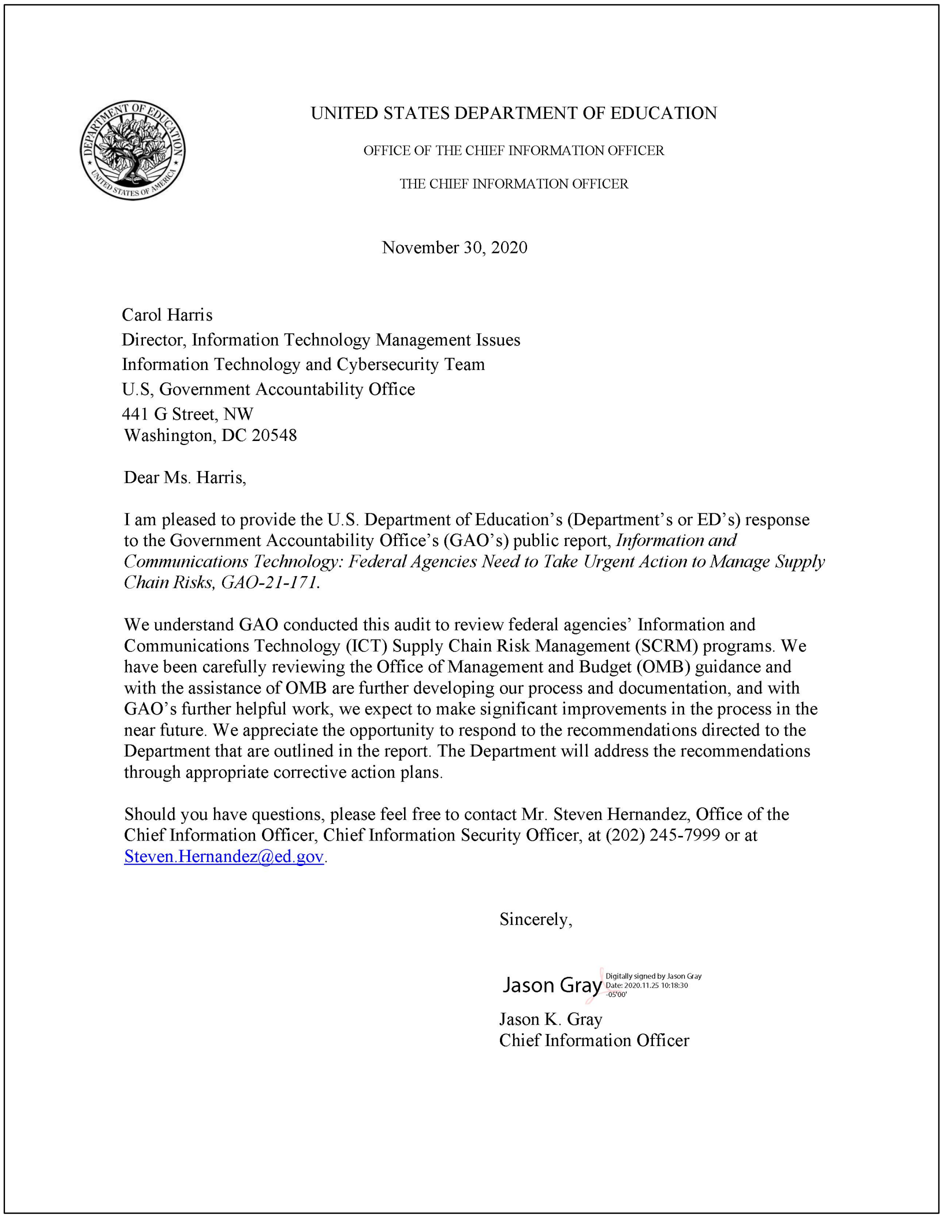
Table 27: Agency 23's Implementation of Practices for Managing Information and Communications Technology (ICT) Supply Chain Risks

Practice	Assessment	Discussion
Establish executive oversight of ICT supply chain risk management (SCRM) activities	Not implemented	Agency 23 did not establish executive oversight of ICT SCRM activities. Officials from the Office of the Chief Information Officer (CIO) stated that they planned to designate an executive to lead SCRM activities and define SCRM roles and responsibilities for senior leaders in the future. These officials stated that they planned to align their efforts with federal guidance from the Department of Homeland Security.
Develop an agency-wide ICT SCRM strategy	Partially implemented	Agency 23 partially implemented this practice. Specifically, it developed a roadmap for implementing SCRM capabilities that identified how the agency intends to assess, respond to, and monitor supply chain risks across the life cycle of ICT products and services. However, the roadmap did not make explicit the agency's supply chain risk tolerance. Officials from the Office of the CIO stated that they would address this gap to align their efforts with federal guidance.
Establish an approach to identify and document agency ICT supply chain(s)	Not implemented	Agency 23 did not establish an approach to identify and document the agency's ICT supply chain(s). Officials from the Office of the CIO stated that they would implement this practice to align their efforts with federal guidance.

Practice	Assessment	Discussion
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Not implemented	Agency 23 did not establish a process for conducting agency-wide ICT supply chain risk assessments. According to the agency's roadmap for implementing SCRM capabilities, the agency did not plan to focus its efforts on implementing this practice. Instead, the agency planned to use its resources to determine any risks associated with its suppliers.
Establish a process to conduct a SCRM review of a potential supplier	Not implemented	Agency 23 did not establish a process to conduct a SCRM review of a potential supplier prior to entering into a contract or issuing an order to that supplier for ICT products and services. Officials from the Office of the CIO stated that they would implement this practice to align their efforts with federal guidance.
Develop organizational ICT SCRM requirements for suppliers	Not implemented	Agency 23 did not develop organizational ICT SCRM requirements for inclusion in contracts with suppliers. According to the agency's roadmap for implementing SCRM capabilities, it intends to develop a policy that outlines contracting terms and requirements for suppliers that provide the agency with the right to monitor and review supplier compliance with laws and regulation; specify supplier requirements regarding security and privacy controls; and include supplier requirements for reporting security breaches to the agency. Officials from the Office of the CIO stated that they also planned to leverage relevant federal guidance to implement this practice.
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Not implemented	Agency 23 did not develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment to an operational environment. According to the agency's roadmap for implementing SCRM capabilities, all new assets will be required to undergo an assessment prior to their deployment. Officials from the Office of the CIO stated that they would leverage federal SCRM guidance to implement this practice.

Source: GAO analysis of agency 23 data. | GAO-21-171

Appendix III: Comments from the Department of Education



UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF THE CHIEF INFORMATION OFFICER

THE CHIEF INFORMATION OFFICER

November 30, 2020

Carol Harris
Director, Information Technology Management Issues
Information Technology and Cybersecurity Team
U.S, Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Harris,

I am pleased to provide the U.S. Department of Education's (Department's or ED's) response to the Government Accountability Office's (GAO's) public report, *Information and Communications Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks, GAO-21-171.*

We understand GAO conducted this audit to review federal agencies' Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) programs. We have been carefully reviewing the Office of Management and Budget (OMB) guidance and with the assistance of OMB are further developing our process and documentation, and with GAO's further helpful work, we expect to make significant improvements in the process in the near future. We appreciate the opportunity to respond to the recommendations directed to the Department that are outlined in the report. The Department will address the recommendations through appropriate corrective action plans.

Should you have questions, please feel free to contact Mr. Steven Hernandez, Office of the Chief Information Officer, Chief Information Security Officer, at (202) 245-7999 or at Steven.Hernandez@ed.gov.

Sincerely,

Jason Gray Digitally signed by Jason Gray Date: 2020.11.25 10:18:30 -05'00'

Jason K. Gray
Chief Information Officer

Text of Appendix III: Comments from the Department of Education

November 30, 2020

Carol Harris

Director, Information Technology Management Issues Information Technology and Cybersecurity Team U.S, Government Accountability Office

441 G Street, NW Washington, DC 20548

Dear Ms. Harris,

I am pleased to provide the U.S. Department of Education's (Department's or ED's) response to the Government Accountability Office's (GAO's) public report, Information and Communications Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks, GAO-21-171.

We understand GAO conducted this audit to review federal agencies' Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) programs. We have been carefully reviewing the Office of Management and Budget (OMB) guidance and with the assistance of OMB are further developing our process and documentation, and with GAO's further helpful work, we expect to make significant improvements in the process in the near future. We appreciate the opportunity to respond to the recommendations directed to the Department that are outlined in the report. The Department will address the recommendations through appropriate corrective action plans.

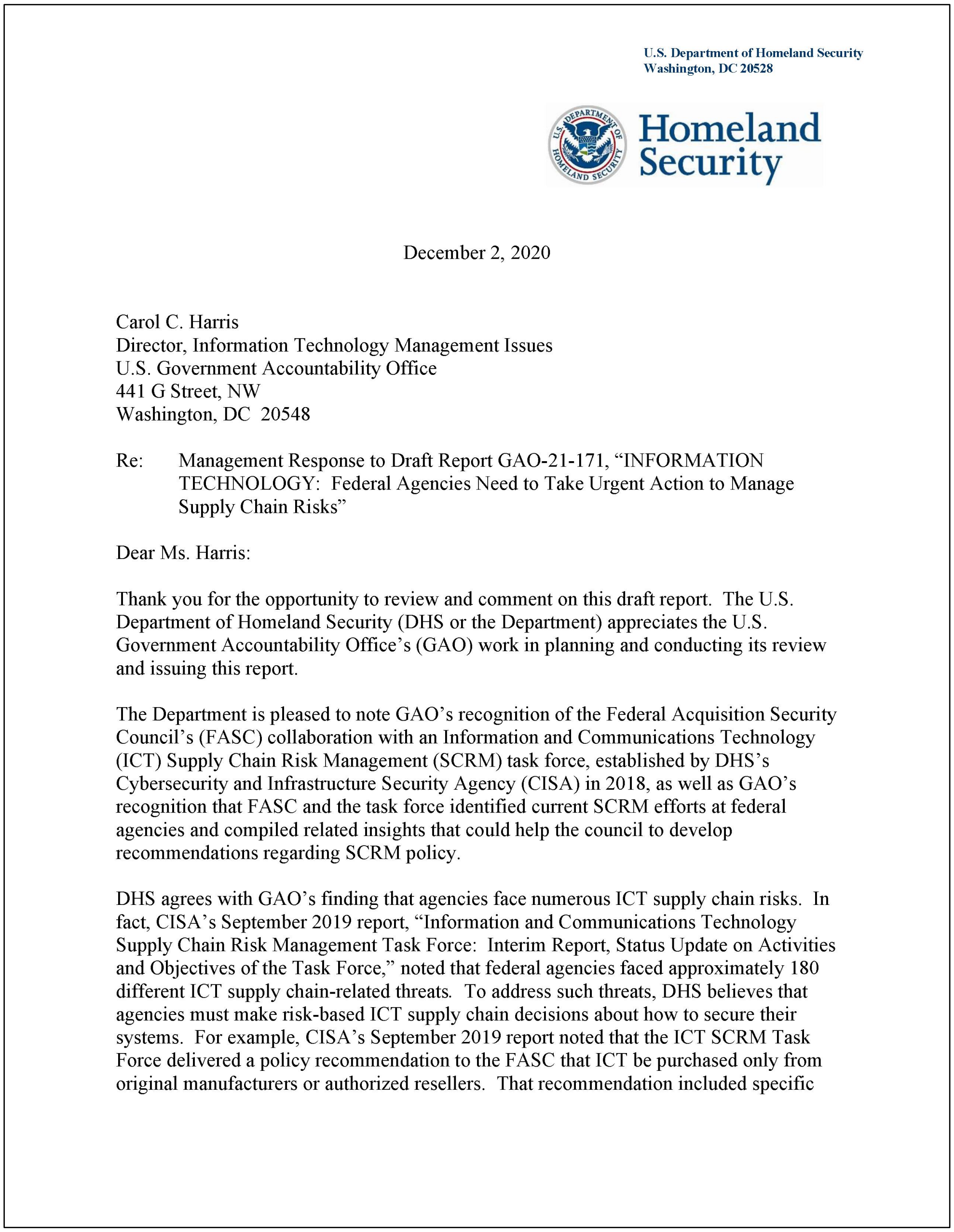
Should you have questions, please feel free to contact Mr. Steven Hernandez, Office of the Chief Information Officer, Chief Information Security Officer, at (202) 245-7999 or at Steven.Hernandez@ed.gov.

Sincerely,

Jason K. Gray

Chief Information Officer

Appendix IV: Comments from the Department of Homeland Security



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

Homeland
Security

December 2, 2020

Carol C. Harris
Director, Information Technology Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

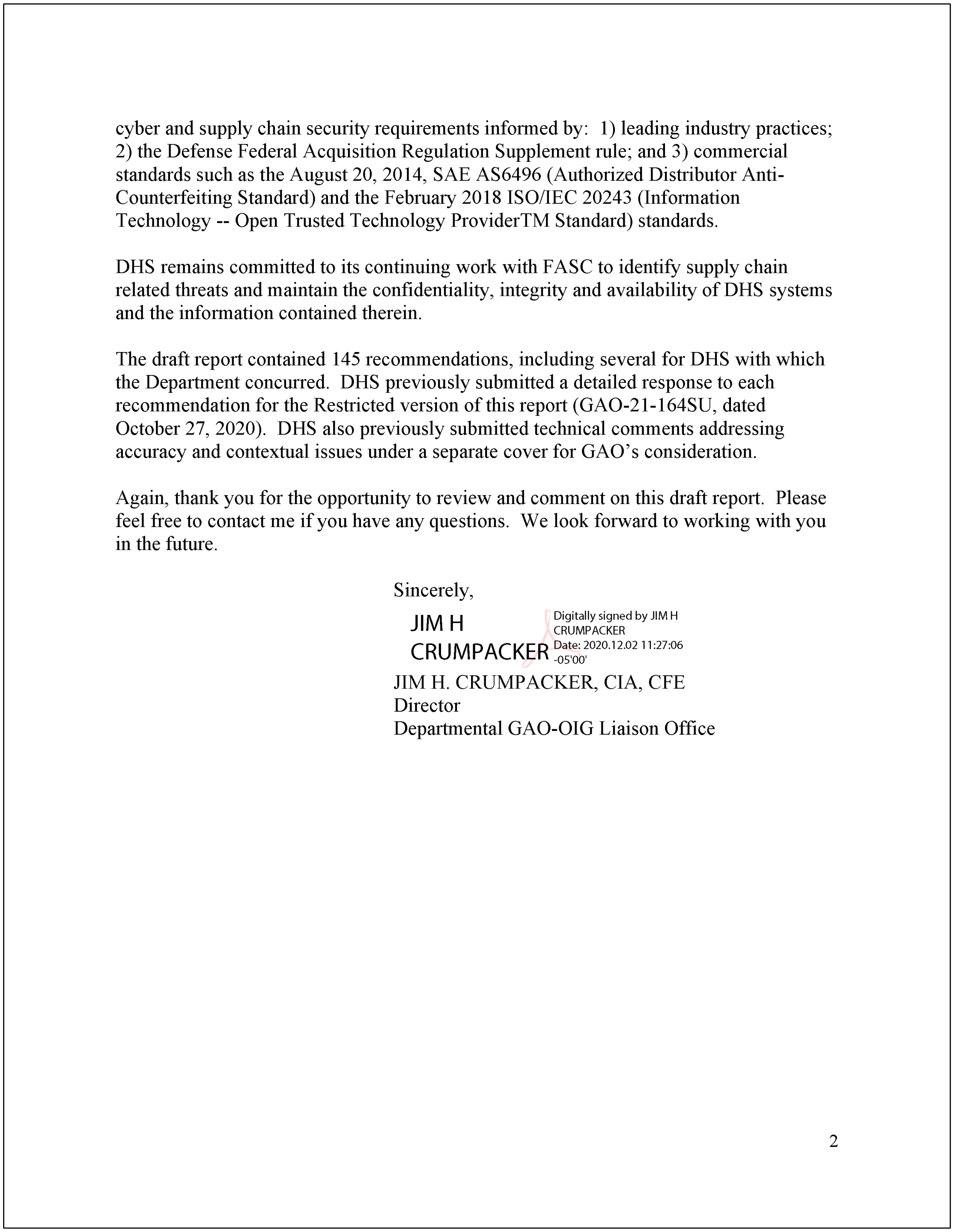
Re: Management Response to Draft Report GAO-21-171, "INFORMATION TECHNOLOGY: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks"

Dear Ms. Harris:

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

The Department is pleased to note GAO's recognition of the Federal Acquisition Security Council's (FASC) collaboration with an Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) task force, established by DHS's Cybersecurity and Infrastructure Security Agency (CISA) in 2018, as well as GAO's recognition that FASC and the task force identified current SCRM efforts at federal agencies and compiled related insights that could help the council to develop recommendations regarding SCRM policy.

DHS agrees with GAO's finding that agencies face numerous ICT supply chain risks. In fact, CISA's September 2019 report, "Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report, Status Update on Activities and Objectives of the Task Force," noted that federal agencies faced approximately 180 different ICT supply chain-related threats. To address such threats, DHS believes that agencies must make risk-based ICT supply chain decisions about how to secure their systems. For example, CISA's September 2019 report noted that the ICT SCRM Task Force delivered a policy recommendation to the FASC that ICT be purchased only from original manufacturers or authorized resellers. That recommendation included specific



cyber and supply chain security requirements informed by: 1) leading industry practices; 2) the Defense Federal Acquisition Regulation Supplement rule; and 3) commercial standards such as the August 20, 2014, SAE AS6496 (Authorized Distributor Anti-Counterfeiting Standard) and the February 2018 ISO/IEC 20243 (Information Technology -- Open Trusted Technology ProviderTM Standard) standards.

DHS remains committed to its continuing work with FASC to identify supply chain related threats and maintain the confidentiality, integrity and availability of DHS systems and the information contained therein.

The draft report contained 145 recommendations, including several for DHS with which the Department concurred. DHS previously submitted a detailed response to each recommendation for the Restricted version of this report (GAO-21-164SU, dated October 27, 2020). DHS also previously submitted technical comments addressing accuracy and contextual issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

JIM H
CRUMPACKER

Digitally signed by JIM H
CRUMPACKER
Date: 2020.12.02 11:27:06
-05'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Text of Appendix IV: Comments from the Department of Homeland Security

Page 1

December 2, 2020

Carol C. Harris

Director, Information Technology Management Issues

U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548

Re: Management Response to Draft Report GAO-21-171, "INFORMATION TECHNOLOGY: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks"

Dear Ms. Harris:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S.

Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition of the Federal Acquisition Security Council's (FASC) collaboration with an Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) task force, established by DHS's Cybersecurity and Infrastructure Security Agency (CISA) in 2018, as well as GAO's recognition that FASC and the task force identified current SCRM efforts at federal agencies and compiled related insights that could help the council to develop recommendations regarding SCRM policy.

DHS agrees with GAO's finding that agencies face numerous ICT supply chain risks. In fact, CISA's September 2019 report, "Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report, Status Update on Activities and Objectives of the Task Force," noted that federal agencies faced approximately 180 different ICT supply chain-related threats. To address such threats, DHS believes that agencies must make risk-based ICT supply chain decisions about how to secure their systems. For example, CISA's September 2019 report noted that the ICT SCRM Task Force delivered a policy recommendation to the FASC that ICT be purchased only from original manufacturers or authorized resellers. That recommendation included specific

Page 2

cyber and supply chain security requirements informed by: 1) leading industry practices;

2) the Defense Federal Acquisition Regulation Supplement rule; and 3) commercial standards such as the August 20, 2014, SAE AS6496 (Authorized Distributor Anti-Counterfeiting Standard) and the February 2018 ISO/IEC 20243 (Information Technology -- Open Trusted Technology ProviderTM Standard) standards.

DHS remains committed to its continuing work with FASC to identify supply chain related threats and maintain the confidentiality, integrity and availability of DHS systems and the information contained therein.

The draft report contained 145 recommendations, including several for DHS with which the Department concurred. DHS previously submitted a detailed response to each recommendation for the Restricted version of this report (GAO-21-164SU, dated October 27, 2020). DHS also previously submitted technical comments addressing accuracy and contextual issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

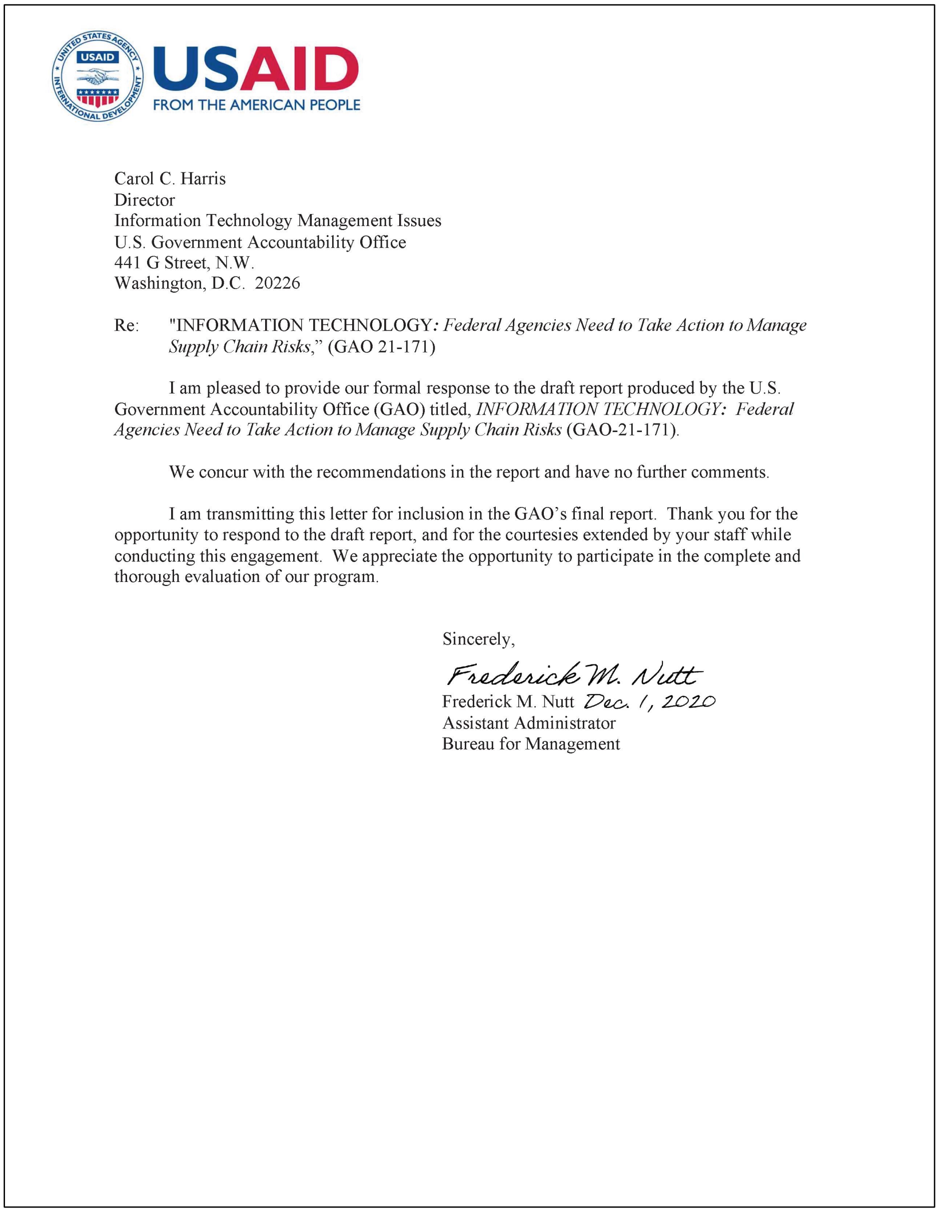
Sincerely,

JIM H. CRUMPACKER, CIA, CFE

Director

Departmental GAO-OIG Liaison Office

Appendix V: Comments from the United States Agency for International Development



USAID
FROM THE AMERICAN PEOPLE

Carol C. Harris
Director
Information Technology Management Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20226

Re: "INFORMATION TECHNOLOGY*: Federal Agencies Need to Take Action to Manage Supply Chain Risks*," (GAO 21-171)

I am pleased to provide our formal response to the draft report produced by the U.S. Government Accountability Office (GAO) titled, *INFORMATION TECHNOLOGY: Federal Agencies Need to Take Action to Manage Supply Chain Risks* (GAO-21-171).

We concur with the recommendations in the report and have no further comments.

I am transmitting this letter for inclusion in the GAO's final report. Thank you for the opportunity to respond to the draft report, and for the courtesies extended by your staff while conducting this engagement. We appreciate the opportunity to participate in the complete and thorough evaluation of our program.

Sincerely,

Frederick M. Nutt

Frederick M. Nutt Dec. 1, 2020
Assistant Administrator
Bureau for Management

Text of Appendix V: Comments from the United States Agency for International Development

Carol C. Harris Director

Information Technology Management Issues

U.S. Government Accountability Office 441 G Street, N.W.

Washington, D.C. 20226

Re: "INFORMATION TECHNOLOGY: Federal Agencies Need to Take Action to Manage Supply Chain Risks," (GAO 21-171)

I am pleased to provide our formal response to the draft report produced by the U.S. Government Accountability Office (GAO) titled, INFORMATION TECHNOLOGY: Federal Agencies Need to Take Action to Manage Supply Chain Risks (GAO-21-171).

We concur with the recommendations in the report and have no further comments.

I am transmitting this letter for inclusion in the GAO's final report. Thank you for the opportunity to respond to the draft report, and for the courtesies extended by your staff while conducting this engagement. We appreciate the opportunity to participate in the complete and thorough evaluation of our program.

Sincerely, Frederick M. Nutt

Assistant Administrator

Bureau for Management

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

Carol C. Harris at (202) 512-4456 or Harriscc@gao.gov

Staff Acknowledgments

In addition to the contact name above, the following staff also made key contributions to this report: Niti Tandon and Eric Winter (Assistant Directors), Donald Baca, Chris Businsky, Donna Epler, Rebecca Eyler, Catherine Maloney, and Angela Watson.

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 our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

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 Email 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 FraudNet:

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

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