United States Government Accountability Office

Report to Congressional Committees

May 2023

INFORMATION AND COMMUNICATIONS TECHNOLOGY

DOD Needs to Fully Implement Foundational Practices to Manage Supply Chain Risks

Accessible Version

GAO-23-105612

GAO Highlights

Highlights of GAO-23-105612, a report to congressional committees

May 2023

INFORMATION AND COMMUNICATIONS TECHNOLOGY

DOD Needs to Fully Implement Foundational Practices 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 risks that can compromise the confidentiality, integrity, or availability of an organization's systems and the information they contain.

Senate Report 117-39 accompanying the Fiscal Year 2022 National Defense Authorization Act included a provision for GAO to provide an assessment of DOD's efforts to address ICT supply chain risks. The specific objectives for GAO's report were to (1) assess the extent to which DOD is implementing foundational ICT supply chain risk management practices and (2) describe the extent to which DOD is leading or supporting government-wide efforts to protect the ICT supply chain.

GAO compared the department's policies, procedures, and related documentation to seven foundational practices. These practices are based on National Institute of Standards and Technology guidance for ICT risk management. In addition, GAO analyzed documentation describing DOD's efforts to lead or support government-wide efforts to protect its supply chains. GAO also interviewed relevant agency officials.

What GAO Recommends

GAO is making three recommendations to DOD to commit to time frames for fully implementing the remaining foundational practices in its ICT supply chain risk management efforts. DOD concurred with the recommendations.

View GAO-23-105612. For more information, contact Carol Harris at (202) 512-4456 or Harriscc@gao.gov.

What GAO Found

The Department of Defense (DOD) has fully implemented four and partially implemented three of seven selected foundational practices for managing information and communications technology (ICT) supply chain risks (see figure). These risks include threats posed by counterfeiters who may exploit vulnerabilities in the supply chain. Supply chain risk management is the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains.

Assessment of the Department of Defense's (DOD) Implementation of Selected Foundational Information and Communications Technology (ICT) Supply Chain Risk Management Practices

Practice	GAO assessment
Establish oversight of ICT risk management activities	Fully implemented
Develop an agency-wide ICT risk management strategy	Partially implemented
Establish an approach to identify and document agency ICT supply chain(s)	Fully implemented
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Fully implemented
Establish a process to conduct a risk management review of a potential supplier	Partially implemented
Develop organizational ICT risk management requirements for suppliers	Fully implemented
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Partially implemented

Source: GAO analysis based on DOD documentation. | GAO-23-105612

Accessible Data for Assessment of the Department of Defense's (DOD) Implementation of Selected Foundational Information and Communications Technology (ICT) Supply Chain Risk Management Practices

Practice	GAO assessment
Establish oversight of ICT risk management activities	Fully implemented
Develop an agency-wide ICT risk management strategy	Partially implemented
Establish an approach to identify and document agency ICT supply chain(s)	Fully implemented
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Fully implemented
Establish a process to conduct a risk management review of a potential supplier	Partially implemented
Develop organizational ICT risk management requirements for suppliers	Fully implemented
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Partially implemented

Source: GAO analysis based on DOD documentation. | GAO-23-105612

By fully implementing four of the foundational practices, DOD has taken steps to mitigate potential threats and secure its ICT supply chain. Regarding the three

partially implemented practices, the department has begun several efforts that are not yet complete. For example, the department has developed a risk management strategy but has not approved guidance for implementing it. DOD has also piloted the use of several tools to review potential suppliers but the review of the results is ongoing. However, DOD did not specify time frames for when these actions would be completed. Fully implementing the three remaining practices would enhance the department's understanding and management of supply chain risks.

DOD provided leadership and support for several government-wide efforts to protect the ICT supply chain. For example, the department offered a course and assisted small businesses in protecting their supply chains. Additionally, the department developed an action plan to facilitate cyber threat sharing and briefed a federal acquisition community of practice on performing cyber test and evaluations. DOD also shared ICT supply chain responsibilities as a member of the Federal Acquisition Security Council. Further, the council has the authority to issue exclusion orders to prevent purchasing from suppliers that may be compromised.

Contents

Abbreviations

CIO	Chief Information Officer
C-SCRM	cyber supply chain risk management
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DOD	Department of Defense
FCC	Federal Communications Commission
ICT	information and communications technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OUSD	Office of the Under Secretary of Defense
SCRM	supply chain risk management
SMWG	Scoping and Mitigation Working Group

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 18, 2023

Congressional Committees

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

In July 2021, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency reported that federal agencies faced approximately 180 different ICT supply chain-related threats. Supply chain risks include threats posed by actors, such as foreign intelligence services or counterfeiters, who may exploit vulnerabilities in the supply chain. This, in turn, could 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 2022 included at least $9.8 billion for cybersecurity funding, which supports the protection of federal information systems, including SCRM.

Given the importance of federal agencies' supply chains, the Senate Committee on Armed Services Report accompanying the National Defense Authorization Act for Fiscal Year 2022 included a provision for us to review the Department of Defense's (DOD) SCRM processes.[1] Our specific objectives were to (1) assess the extent to which DOD is implementing ICT SCRM practices and (2) describe the department's

[1]Committee on Armed Services, *National Defense Authorization Act for Fiscal Year 2022 Report*, Senate Report 117-39, pages 311-12. (Washington, D.C.: Sept. 22, 2021).

leadership or support for government-wide efforts to protect federal agencies' ICT supply chains.

To address our first objective, we reviewed policies and procedures established and implemented by DOD for non-national security systems[2] relevant to ICT SCRM practices. These included a DOD Manual and seven DOD Instructions.[3]

In addition, we reviewed ICT SCRM guidance documentation from the Office of the Chief Information Officer (OCIO); the Office of the Deputy Chief Information Officer (CIO) for Cybersecurity within the OCIO; the Office of the Under Secretary of Defense (OUSD) for Acquisition and Sustainment; the OUSD for Research and Engineering; and the Defense Information Systems Agency.

We compared DOD's ICT SCRM policies with seven foundational ICT SCRM practices identified in our prior report on federal ICT SCRM implementation.[4] These foundational practices are:

- establish executive oversight of ICT SCRM activities,
- develop an agency-wide ICT SCRM strategy,

[2]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.

[3]DOD, DOD Manual 4140.01, Volume 1, *DOD Supply Chain Materiel Management Procedures: Operational Requirements*, (Washington, D.C.: December 2018); DOD Instruction 4140.67, *DOD Counterfeit Prevention Policy*, (Washington, D.C.: March 2020); DOD Instruction 5000.82, *Acquisition of Information Technology (IT)*, (Washington, D.C.: Apr. 21, 2020); DOD Instruction 5000.83, *Technology and Program Protection to Maintain Technological Advantage*, (Washington, D.C.: May 2021); DOD Instruction 5000.90, *Cybersecurity for Acquisition Decision Authorities and Program Managers*, (Washington, D.C.: December 2020); DOD Instruction 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks*, (Washington, D.C.: Oct. 15, 2018); DOD Instruction 8500.01, *Cybersecurity*, (Washington, D.C.: October 2019); and DOD Instruction 8510.01, *Risk Management Framework (RMF) for DOD Information Technology (IT)*, (Washington, D.C.: December 2020).

[4]GAO, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-171 (Washington, D.C.: Dec. 15, 2020).

- 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,
- develop organizational ICT SCRM requirements for suppliers, and
- develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment.

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

We supplemented our analyses with interviews of relevant DOD officials to discuss their activities regarding ICT SCRM. This included officials from the departments of the Army, Navy, and Air Force. We also provided the results of our analysis of DOD documentation to the officials to corroborate our findings, collect and analyze additional evidence, and identify causes for any gaps we identified in the implementation of the seven practices.

To address our second objective, we analyzed DOD reports, briefings, a risk assessment methodology, Defense Acquisition University course materials, and other documentation describing DOD's efforts to lead or support government-wide efforts to protect the ICT supply chain. We also analyzed executive orders related to securing the ICT supply chain.[5] In reviewing the various documents, we divided DOD's efforts into leadership and support categories.

We also interviewed agency officials responsible for overseeing the execution of DOD's leadership and support for government-wide efforts. In addition, we provided the results of our analysis of DOD documentation

[5]The White House, *Securing the Information and Communications Technology and Services Supply Chain*, Executive Order 13873 (Washington, D.C.: May 15, 2019).

to the officials to corroborate our characterizations of the department's leadership and support roles.

We conducted this performance audit from December 2021 to May 2023 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.

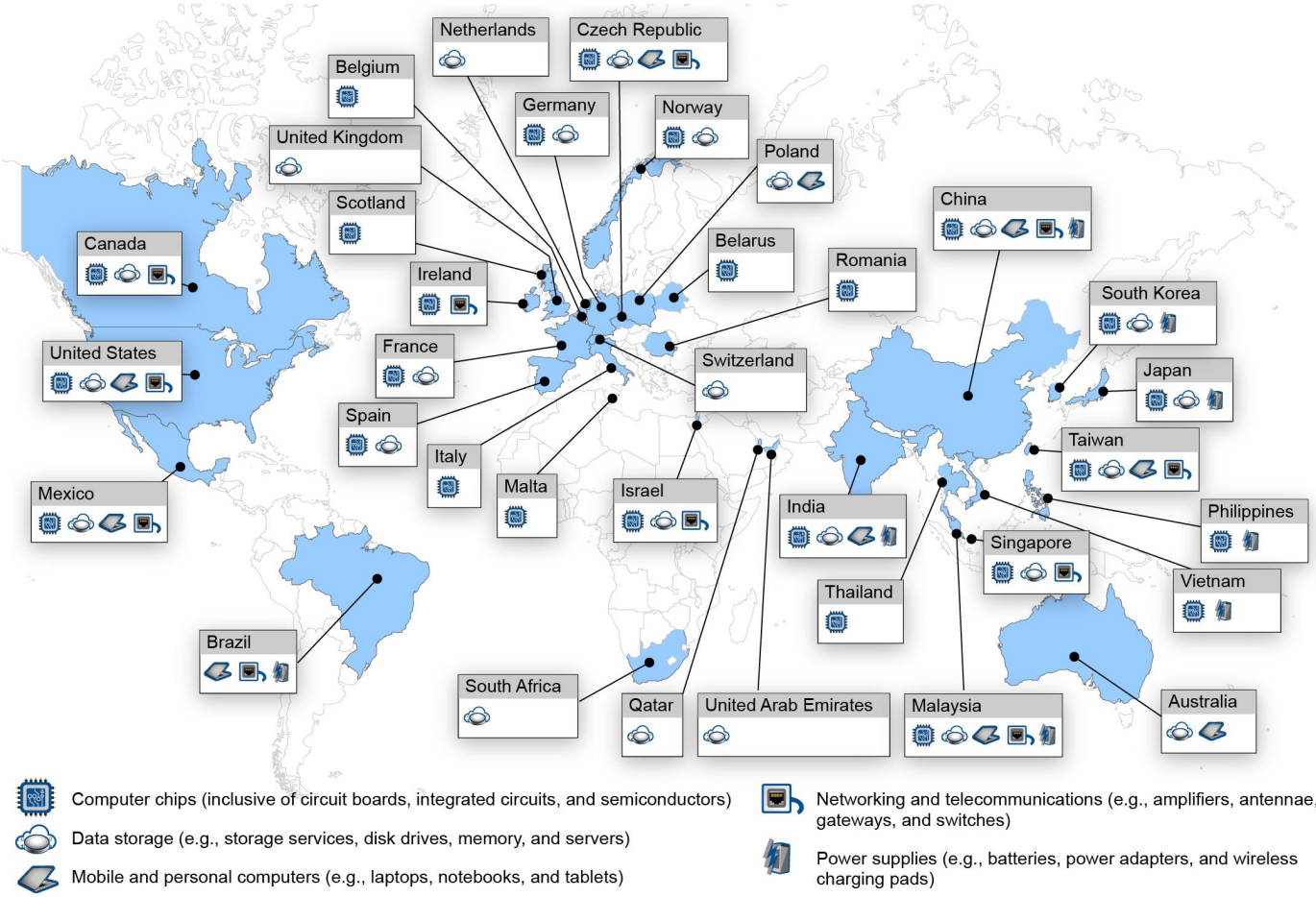
Background

As noted earlier, federal agencies rely extensively on ICT products and services to carry out their operations. This dependence on ICT solutions has increased the complexity of federal supply chains. In addition, federal procurement guidelines 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.[6] 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. 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.

[6]Federal Acquisition Streamlining Act of 1994, Pub. L. No. 103-355, Title VIII, 108 Stat. 3243, 3384 (Oct. 13, 1994). See also Federal Acquisition Regulations Part 12, Acquisition of Commercial Products and Commercial Services.

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



Source: GAO analysis of public information. | GAO-23-105612

GAO Has Reported on ICT SCRM Practices

The exploitation of IT products and services through the supply chain is an emerging threat. Given this threat, agencies are to make risk-based decisions to most effectively secure their supply chain data. To help them do so, the National Institute of Standards and Technology (NIST) has

issued guidance that identifies organization-wide ICT SCRM foundational practices.[7]

In December 2020, we released the public version of a report that examined the 23 civilian Chief Financial Officers Act agencies' implementation of ICT SCRM practices relative to select practices from NIST's guidance.[8] We identified and selected from our review of NIST guidance foundational practices that were of particular importance for providing an organization-wide approach to ICT SCRM.[9] We found none of the 23 agencies fully implemented all of the SCRM practices and 14 agencies had not implemented any of the practices.

In the sensitive version of the report, we 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. We continue to believe that all of the recommendations are still warranted, as discussed in the sensitive report. As of February 2023, 46 of the 145 recommendations have been fully implemented. Figure 2 identifies and describes the seven foundational ICT SCRM practices.

[7]NIST, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, NIST Special Publication 800-161, Revision 1 (Gaithersburg, MD: May 5, 2022)

[8]GAO-21-171.

[9]See GAO-21-171 for how we selected the foundational practices.

Figure 2: Evaluation Criteria Associated with Selected Foundational Practices for Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM)

Practice	Evaluation criteria
Establish oversight of ICT SCRM activities	The agency 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. The agency should define SCRM roles and responsibilities for senior leaders who participate in supply chain activities.
Develop an agency-wide ICT SCRM strategy	The agency should develop an agency-wide ICT SCRM strategy that makes explicit the agency's risk tolerance in clear and unambiguous terms, and identifies 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 should establish 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 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, resulting 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	The agency should establish 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 should develop 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 should develop 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 National Institute of Standards and Technology guidance. | GAO-23-105612

Accessible Data for Figure 2: Evaluation Criteria Associated with Selected Foundational Practices for Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM)

Practice	Evaluation criteria
Establish oversight of ICT SCRM activities	The agency 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. The agency should define SCRM roles and responsibilities for senior leaders who participate in supply chain activities.
Develop an agency-wide ICT SCRM strategy	The agency should develop an agency-wide ICT SCRM strategy that makes explicit the agency's risk tolerance in clear and unambiguous terms, and identifies 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 should establish 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 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, resulting 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	The agency should establish 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 should develop 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 compro- mised ICT products prior to their deployment	The agency should develop 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 National Institute of Standards and Technology guidance. | GAO-23-105612

DOD Has Fully Implemented Four of Seven Selected Foundational ICT SCRM Practices

DOD has fully implemented four and partially implemented three of the seven selected foundational practices for managing ICT supply chain risks. Table 1 and the narrative that follows summarize the extent to which DOD has implemented each practice.

Table 1: GAO Assessment of the Department of Defense's (DOD) Implementation of Foundational Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Practices

ICT SCRM practice	GAO assessment
Establish oversight of ICT SCRM activities	Fully implemented
Develop an agency-wide ICT SCRM strategy	Partially implemented
Establish an approach to identify and document agency ICT supply chain(s)	Fully implemented
Establish a process to conduct agency-wide assessments of ICT supply chain risks	Fully implemented
Establish a process to conduct a SCRM review of a potential supplier	Partially implemented
Develop organizational ICT SCRM requirements for suppliers	Fully implemented
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment	Partially implemented

Source: GAO analysis based on DOD documentation. | GAO-23-105612

DOD Has Established Oversight of ICT SCRM Activities

Effective ICT SCRM requires commitment, direct involvement, and ongoing support from senior leaders and executives. Also, 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. 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.

DOD has established ICT SCRM oversight by designating responsibility for leading the agency-wide ICT SCRM activities to the Deputy CIO for Cybersecurity within the OCIO. The overall resiliency and availability of ICT, as a commodity and supply item, is managed by the OUSD for Acquisition and Sustainment. The OCIO's Director for Risk Assessment and Operational Integration within the Office of the Deputy CIO for Cybersecurity leads and supports the collaborative effort within the Office of the Secretary of Defense and components in implementing ICT SCRM efforts. Those efforts are focused on the assurance aspects of supply chain risk, to include risks from foreign ownership, influence, and control.

In addition, the OUSD for Research and Engineering is responsible for developing a strategy for managing supply chain risk. It is supported by the OCIO, the Deputy CIO for Cybersecurity, and the OUSD for Acquisition and Sustainment.

Further, DOD has defined ICT SCRM leadership roles. For example, the CIO coordinates with the OUSD for Research and Engineering, the OUSD for Acquisition and Sustainment, and component leaders as a subject matter expert on ICT SCRM activities. These activities include implementing supply chain assurance practices and developing ICT SCRM training, requirements, best practices, and mitigation guidance. The CIO is also responsible for issuing guidance on the operational usage of suppliers and components that are restricted or excluded due to a significant ICT supply chain risk.

Evaluation criteria associated with selected foundational practices for ICT SCRM
Establish oversight of ICT SCRM activities
The agency 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. The agency should define SCRM roles and responsibilities for senior leaders who participate in supply chain activities.
Develop an agency-wide ICT SCRM strategy
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
Develop organizational ICT SCRM require-ments for suppliers
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment

Source: GAO analysis based on National Institute of Standards and Technology guidance. | GAO-23-105612

DOD Has Partially Developed an Agency-wide ICT SCRM Strategy

Evaluation criteria associated with selected foundational practices for ICT SCRM
Establish oversight of ICT SCRM activities
Develop an agency-wide ICT SCRM strategy
The agency should develop an agency-wide ICT SCRM strategy that makes explicit the agency's risk tolerance in clear and unambiguous terms, and identifies 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)
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
Develop organizational ICT SCRM requirements for suppliers
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment

Source: GAO analysis based on National Institute of Standards and Technology guidance. | GAO-23-105612

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. 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.

DOD has partially implemented this practice by taking steps to develop its ICT SCRM strategy. For example, DOD's Manual 4140.01 outlines the

elements that SCRM strategies should include.[10] In addition, Instruction 5200.44 implements the Trusted System Networks strategy for systems assurance and trustworthiness.[11] It does this through program protection plans and cybersecurity implementation to provide uncompromised weapons and information systems. The Trusted System Networks strategy integrates systems engineering, SCRM, security, counterintelligence, intelligence, cybersecurity, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust.

Also, DOD's OCIO published a draft paper, *DOD CIO Strategy for Supporting Cyber Supply Chain Risk Management (C-SCRM): A Risk-Based Approach,* which describes the department's cybersecurity strategic goals and objectives to secure the cyber supply chain against adversary manipulation to ensure trusted systems and networks. This paper includes four strategic principles:

- develop an integrated framework that changes DOD and vendor behavior to address C-SCRM risk;
- evolve enterprise-wide DOD ICT acquisition practices and vendor engagement to address C-SCRM risk;
- improve collection of, access to, analysis of, and sharing of C-SCRM threat information; and
- agree upon a unified approach to C-SCRM threat response.

In addition, this paper identifies risk tolerance levels for suppliers and establishes a requirement that the program protection plans are to be updated regularly throughout the acquisition, maintenance, and sustainment processes.

Further, OUSD for Acquisition and Sustainment is working to establish an enterprise-level organizational structure to develop and implement an integrated SCRM framework and DOD SCRM policy. This framework will include, among other things, a standard taxonomy, governance, and oversight for department-wide SCRM processes.

However, although DOD developed a strategy that identifies its risk tolerance, its efforts to fully develop a department-wide process to

[10]DOD Manual 4140.01.

[11]DOD Instruction 5200.44.

assess, respond to, or monitor ICT supply chain risks across the life cycle of ICT products and services are ongoing and not yet complete. For example, *DOD CIO Strategy for Supporting Cyber Supply Chain Risk Management (C-SCRM): A Risk-Based Approach* is in draft form and has not been approved and implemented.

Officials in DOD's OCIO acknowledged that the paper needed to be updated and finalized, but did not provide a time frame for when this would be done. They also noted that there are gaps in the oversight of components' implementation of the department-wide SCRM processes. According to the officials, this is due, in part, to limited dedicated ICT SCRM funding that impacts how quickly the department-wide efforts can be implemented.

Without a complete ICT SCRM strategy, DOD decision makers lack the organizational context in which risk-based decisions should be made and 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 the department's organizational risk.

DOD Has Established an Approach to Identify and Document Agency ICT Supply Chains

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. 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.

DOD has implemented this practice by establishing a policy to collect data on suppliers. In particular, DOD's Instruction 5200.44 indicates that, for ICT components in applicable systems, intelligence analysis about suppliers of critical components shall be used to inform risk management decisions.[12]

[12]DOD Instruction 5200.44.

In addition, the CIO has explored the use of commercial illumination tools[13] to establish a mechanism to identify and document agency ICT supply chains. The illumination tools collect and document supplier data and can increase transparency of the connections and dependencies of the supply chain as well as continuous monitoring capabilities. The tools can be used to analyze various types of data, such as hardware assets including peripherals, policies for controlling hardware access, and detection of hardware manipulation. In addition, DOD's ongoing requirements for effective illumination tools include documenting supplier data such as manufacturing locations, subsidiaries, ownership, leadership and their nationalities, and partner and business relationships.

In addition, components have taken steps to develop and implement approaches to identify and document agency ICT supply chains. For example, Air Force has developed an ICT SCRM tool using a common commercial spreadsheet application to document supplier data. The tool is part of an approach designed to protect the hardware and software critical components and mission critical functions. Intelligence data that are collected are used to identify and describe the risk of products and services provided by the vendor. In addition, the tool describes the activities necessary for ICT SCRM, including procurement practices, a risk management framework and program protection plan, and data and information sharing and sensitivity levels.

DOD Has Established a Process to Conduct Agency-wide Assessments of ICT Supply Chain Risks

Risk assessment is one of the fundamental components of organizational risk management. Without a process for agency-wide ICT supply chain risk assessments, agencies are limited in their ability to (1) identify systemic weaknesses or deficiencies in multiple ICT products and services and (2) assess the overall risks that these present to operations, assets, and individuals.

DOD has established a process to conduct agency-wide assessments of ICT supply chain risks. In August 2020, DOD established a department-wide Scoping and Mitigation Working Group (SMWG) to identify, prioritize, and mitigate ICT supply chain risks. The SMWG developed a

[13]For example, the DOD CIO has explored using Sepio, ThreeSixty, Interos, and Exiger.

process to enhance scrutiny of procurement decisions and improve the integration of SCRM into the overall acquisition decision cycle. The SMWG is tasked with coordinating and approving risk management and mitigation activities for DOD national security systems and critical infrastructure.

In addition, on a monthly basis, the SMWG is responsible for assessing available threat information, identifying vulnerabilities, evaluating potential impacts of DOD operational usage, and devising appropriate risk management and mitigation plans and recommendations for leadership approval. The process that the SMWG has implemented includes collecting department-wide data such as incident reports, trends, and threats raised by intelligence sources. The intelligence sources then disseminate any supplier threat assessment to the SMWG.

In addition, components have taken steps to establish processes to conduct assessments of ICT supply chain risks. For example, Air Force's ICT SCRM tool provides a holistic view of actual SCRM activities performed, and enables an evidence-based collection of risk indicators to be documented and summarized for risk decision makers. This tool includes a tactical model that provides program offices a method of aggregating and analyzing supplier risks. In addition, Army officials explained that one of their long-term goals is to incorporate ICT SCRM data into the department's existing analytics tool in order to provide overarching information in real time.

Evaluation criteria associated with selected foundational practices for ICT SCRM
Establish oversight of ICT SCRM activities
Develop an agency-wide ICT SCRM strategy
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
The agency 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, resulting 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
Develop organizational ICT SCRM requirements for suppliers
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment

Source: GAO analysis based on National Institute of Standards and Technology guidance. | GAO-23-105612

DOD Has Partially Developed a Process for Conducting SCRM Reviews for Suppliers

Reviews of potential suppliers can provide organizations with increased levels of visibility into supplier activities to promote more effective SCRM. Such a 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.

DOD has partially implemented this practice by taking steps to develop policy that requires analyses of suppliers of critical components using illumination capabilities. In particular, DOD Instruction 5200.44 indicates that intelligence analysis of suppliers of critical components will be used to inform risk management decisions.[14] Also, DOD Instruction 5000.90 establishes policy, assigns responsibilities, and prescribes procedures for the management of cybersecurity risk by program decision authorities in the department's acquisition processes.[15] Further, DOD has statutory authority to identify and exclude potential suppliers that represent a national security risk to the supply chain.[16]

As previously noted, the CIO has piloted the use of commercial illumination tools to collect and document supplier data with the intent to increase transparency of the connections and dependencies of the supply chain as well as continuous monitoring capabilities. The department has deployed several tools that can provide analyses of various types of data, such as hardware assets including peripherals, policies for controlling hardware access, and detection of hardware manipulation. In addition, DOD's ongoing requirements for effective illumination tools include documenting supplier data such as manufacturing locations, subsidiaries, ownership, leadership and their nationalities, and partner and business relationships.

In addition, some DOD components have taken steps to establish this process at the program level. For example, Air Force officials stated that their ICT SCRM analysis tool describes the necessary activities for procurement practices, including data and information sharing and related sensitivity levels. The tool helps assess products and services against the ICT SCRM practices and to develop program protection plans, as necessary. As another example, Army has established a working group in coordination with the intelligence community. This working group is tasked to develop illumination tools and processes that will be used to evaluate suppliers. Army officials stated that several different illumination tools are used to analyze suppliers, services and products.

However, although the department has taken initial steps to evaluate potential ICT suppliers, it has not fully established a department-wide

[14]DOD Instruction 5200.44.

[15]DOD Instruction 5000.90.

[16]10 U.S.C. § 3252(2)(A).

process for supplier reviews. As noted previously, the department's efforts to develop tools and processes to evaluate potential ICT suppliers are ongoing and incomplete. For example, according to DOD OCIO officials, several pilots using the illumination tools ended recently and DOD has only begun to implement them.

Officials from DOD's OCIO noted that DOD has not published a specific, department-wide process for supplier reviews because each component will have to develop a supplier review process based on their own mission goals. Accordingly, those officials stated that components were expected to develop their own processes with which to review a potential supplier. In addition, those officials noted that some of the pilots for the tools had just been completed and they need to evaluate the results to determine what to recommend for use. However, they did not provide a time frame for when this would be completed.

We acknowledge the department needs time to evaluate the pilot results and the delegation of responsibility to the components to have their own processes for supplier reviews. However, there are benefits to having a department-level organizational process for conducting reviews of subordinate suppliers. For example, the components may not have the resources to conduct reviews of subordinate suppliers. In addition, they may lack the strategic visibility to manage risk that a department-level process could bring.

Without a process for reviewing risks associated with the potential use of suppliers (and their subordinate suppliers), DOD lacks an important vehicle for protecting the ICT supply chain early in the life cycle of products and services. Without this capability, the department lacks assurance that it fully understands risks and increases the likelihood that adverse events could occur within its ICT supply chains.

Evaluation criteria associated with selected foundational practices for ICT SCRM
Establish oversight of ICT SCRM activities
Develop an agency-wide ICT SCRM strategy
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
The agency should establish 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
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment

Source: GAO analysis based on National Institute of Standards and Technology guidance. | GAO-23-105612

DOD Has Developed 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. 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.

DOD has implemented this practice by developing policy that identifies component organizations' responsibilities when issuing ICT contracts. Specifically, DOD Instruction 8500.01 requires that contracts and other agreements include requirements to provide cybersecurity for the

department's information and the IT used to process that information.[17] For example, this instruction requires that contracts include language indicating that suppliers will conduct cybersecurity testing and evaluation throughout the acquisition life cycle.

In addition, the development requirements state that a cybersecurity representative is to participate in planning, execution, and reporting of integrated testing and evaluation activities; and that DOD information is maintained and disposed of appropriately. Further, communication requirements state that all personnel with access to DOD IT are to be appropriately cleared and qualified.

Additionally, DOD has developed its Defense Federal Acquisition Regulation Supplement (DFARS) provisions that contain, among other things, specific supply chain contract language and clauses that are to be included in supplier contracts, as appropriate. For example, one DFARS provision[18] defines supply chain risk and indicates that potential mitigation options may include using the statutory authority of the department to exclude suppliers.[19] Another DFARS provision identifies requirements for a contractor counterfeit electronic part detection and avoidance system.[20]

[17]DOD Instruction 8500.01.

[18]DFARS, § 252.239-7017, Notice of Supply Chain Risk (December 2022).

[19]10 U.S.C. § 3252(a).

[20]DFARS, § 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System (January 2023).

Evaluation criteria associated with selected foundational practices for ICT SCRM
Establish oversight of ICT SCRM activities
Develop an agency-wide ICT SCRM strategy
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
Develop organizational ICT SCRM requirements for suppliers
The agency should develop 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

Source: GAO analysis based on National Institute of Standards and Technology guidance. | GAO-23-105612

DOD Has Partially Developed Organizational Procedures to Detect Counterfeit and Compromised ICT Products

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. 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.

DOD has partially implemented this practice by taking steps to develop guidance for preventing counterfeit products from entering the department's supply chains. For example, DOD Instruction 4140.67 establishes policy and assigns responsibilities for prevention, detection, remediation, investigation, and restitution to defend the department

against counterfeit materiel that poses a threat to personnel safety and mission assurance.[21]

In addition, DOD has developed a DFARS provision that identifies requirements for a contractor counterfeit electronic part detection and avoidance system.[22] The provision requires potential contractors to, among other things, inspect and test electronic parts in an effort to identify counterfeit parts and reduce risk to the government, report and quarantine any identified counterfeit parts, and ensure that this provision is passed down to any subcontractors.

Further, as previously mentioned, DOD has explored several illumination tools to analyze the capabilities to detect and respond to counterfeit materials within the supply chain. These tools can provide counterfeit process elements such as detect, examine, assess, secure, defend, and build.

In addition, some components have taken steps to implement this practice. For example, Air Force has established a hardware and software assurance process that verifies the legitimacy of hardware and software components provided by vendors to rule out any counterfeit parts. The software analysis evaluates the validity of the code, and generates information on the possibility that the code may not be from a trusted source or has been tampered with.

In addition, the Defense Logistics Agency has implemented pre- and post-award activities intended to identify counterfeit parts in the products it acquires for operations and maintenance. The agency's Counterfeit Detection and Avoidance Program documentation shows flow charts for processes to test for counterfeit parts and provide traceability documentation that tracks the parts from original source to government acceptance.

However, although DOD and its components have begun developing processes and using tools to help identify potential counterfeit parts, those efforts have not been fully implemented department-wide and do not apply to all systems prior to deployment. For example, the program manager for the Defense Logistics Agency's anti-counterfeiting program agreed that its processes apply primarily to its acquisition of spare and

[21]DOD Instruction 4140.67.

[22]DFARS § 252.246-7007 (January 2023).

replacement parts and not to new systems in development. In addition, DOD has not yet fully implemented the illumination tools that can help identify and respond to counterfeit parts. Therefore, it has not yet implemented organizational procedures to manage counterfeit ICT products prior to their acceptance and deployment to an operational environment.

According to officials in DOD's OCIO, this is due to the pilots having just been completed and the need to evaluate the results to determine what to recommend for use. The officials did not provide a time frame for completing these tasks. They also noted that limited dedicated ICT SCRM funding impacts how quickly the department-wide efforts can be implemented.

We acknowledge that the department needs time to evaluate the pilot results and determine the appropriate course of action. However, without organizational procedures for detecting counterfeit and compromised ICT products, the department lacks adequate assurance regarding the integrity, security, and quality of the products it acquires. Without full implementation of those processes, the department will continue to be vulnerable to malicious actors that could exploit the ICT supply chain and possibly disrupt mission operations.

Evaluation criteria associated with selected foundational practices for ICT SCRM
Establish oversight of ICT SCRM activities
Develop an agency-wide ICT SCRM strategy
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
Develop organizational ICT SCRM requirements for suppliers
Develop organizational procedures to detect counterfeit and compromised ICT products prior to their deployment
The agency should develop 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 National Institute of Standards and Technology guidance. | GAO-23-105612

DOD Has Provided Leadership and Support for Government-Wide Efforts to Protect the ICT Supply Chain

DOD provided leadership and support for several government-wide efforts to protect the ICT supply chain. For example, it offered a SCRM course and assisted small businesses in protecting their ICT supply chains. In addition, DOD has provided support by being a member of the Federal Acquisition Security Council and an interagency group, among other things.

DOD Has Provided Several Leadership Efforts to Protect the ICT Supply Chain

DOD provided leadership for several government-wide efforts to protect the ICT supply chain. Specifically, the department offered a SCRM course, assisted small businesses, developed a risk assessment guide, developed an action plan, and briefed a community of practice.

- **SCRM course.** In 2021, the department offered a Defense Acquisition University SCRM course.[23] The purpose of the course was to establish a basic standard for SCRM knowledge across the acquisition workforce. Members of this acquisition workforce consists of DOD employees and contractors, non-DOD federal agency employees, and members of the defense industry. Moreover, ICT SCRM is discussed in the fourth of five modules, which includes topics such as prohibitions and exclusion orders, telecommunications and video surveillance, and the Federal Acquisition Security Council. According to documentation provided by the Federal Acquisition Institute, as of August 2022, 6,614 students completed the course, with an additional 2,857 students in progress, since it launched in September 2021.
- **Small business assistance.** The department assisted small businesses in protecting their ICT supply chain by participating in the Defense Industrial Base Cybersecurity Program.[24] According to DOD officials, once a month, the department moderates and takes the opportunity to share information with the working group. Cybersecurity best practices, tools, and other topics are shared and discussed from the perspectives of small businesses.
- **Risk assessment guide.** The department developed a draft supply chain risk assessment guide that provides steps to research and analyze vendor information by non-

[23]The Federal Acquisition Institute, *Supply Chain Risk Management Course* (Washington, D.C.: 2021).

[24]This program is a bi-directional cyber threat information sharing program between DOD and cleared defense industry contractors. Participants receive products, tools, direct technical assistance, and virtual and in-person meetings at no cost from DOD. In return, participants share suspicious or confirmed cyber activity on their networks with the agency.

counterintelligence organizations.[25] According to DOD OCIO officials, the guide was created to be a focused vendor assessment tool suitable for smaller organizations. The steps described in the guide are intended to allow organizations to conduct a supply chain risk assessment by using a template to perform analysis on publicly available vendor, supplier, and manufacturer information. Specifically, potential vendors and their products are evaluated in categories that include supply chain, business structure, foreign ownership, financial information, and identification of vulnerabilities. The results of the assessment should aid small businesses in making risk-based decisions and determine if counterintelligence personnel should be consulted.

- **Action plan.** The department developed an action plan to facilitate cyber threat sharing and coordination. In February 2021, Executive Order 14017, America's Supply Chains, was issued and called for a comprehensive review of supply chains in critical sectors, including the Defense Industrial Base.[26] To implement the order, DOD's offices of the Assistant Secretary, Industrial Base Policy, and Under Secretary of Defense created an action plan that included a recommendation to:
    - facilitate greater acquisition-focused supply chain and cyber threat sharing and increase partnership activities, and
    - work with its interagency partners to identify and defend mission critical cyber terrain from advanced cyber threats for the highest priority companies providing critical supplies.
- **Community of practice brief.** In November 2021, DOD's OUSD for Research and Engineering briefed the Acquisition Cyber-SCRM community of practice—a group tasked with bringing interagency partners together. The brief included information on draft guidance for performing cyber test and evaluation, DOD acquisition programs and cyber test and evaluation processes, and reducing risk through hardware and firmware assurance.

[25]DOD, *80/20 Methodology Supply Chain Risk Assessments, Deputy Chief Information Officer/ Cybersecurity Risk Assessment and Operational Integration* (Alexandria, VA: 2022) (draft).

[26]The White House, *Executive Order on America's Supply Chains*, Executive Order 14017 (Washington, D.C.: Feb. 24, 2021).

DOD Has Provided Support for Government-wide Efforts to Protect the ICT Supply Chain

DOD also provided support for various government-wide efforts to protect the ICT supply chain. Specifically, the department is a member of the Federal Acquisition Security Council, has the authority to issue exclusions, and is a member of a telecommunications working group:

- **Federal Acquisition Security Council.** The department is a member of the Federal Acquisition Security Council (see figure 3).[27] Among other things, an official in DOD's OCIO and the other six members of the council are responsible for:
- recommending exclusion or removal of high risk products that pose a great risk to the federal government (e.g., the product transmits or utilizes data outside of the United States),
- developing criteria for sharing supply chain risk information and how information may be used across the federal government,
- engaging with the private sector and other non-government organization stakeholders on standards/guidelines and information sharing,
- coordinating with other relevant councils and interagency committees, and
- establishing a program office and other bodies to carry out its functions.

[27]The Federal Acquisition Supply Chain Security Act of 2018, Title II of the SECURE Technology Act, established the Federal Acquisition Security Council with DOD as one of the represented agencies. Pub. L. No. 115-390, title II § 202(a) (Dec. 21, 2018), codified at 41 U.S.C. § 1322(b)(1)(F).

Figure 3: Members of the Federal Acquisition Security Council (FASC)

Source: GAO analysis of 41 U.S.C. 1322(b). | GAO-23-105612

- **Authority to issue exclusions.** The department serves as a deciding official of product removal or exclusion orders. The Federal Acquisition Supply Chain Security Act of 2018 directed the heads of DOD, DHS, and the Director of National Intelligence to make decisions to issue orders for removal or exclusion of products that pose a great risk to the federal enterprise based on recommendations from the Federal Acquisition Security Council.
- **Interagency group.** The department participates in the U.S. Telecommunications Services Sector (also known as Team Telecom). This interagency group, composed of representatives from DOD,

DHS, and the Department of Justice, provides national security and law enforcement assessments to the Federal Communications Commission (FCC) regarding certain FCC license holders or applications. According to the group's April 2022 report, the FCC historically has referred applications that involved companies with a 10 percent or greater foreign ownership, investment, or control.[28] The assessments assist the FCC in determining whether granting the application is in the public interest, convenience, and necessity.

Conclusions

Successful attacks by threat actors could jeopardize the confidentiality, integrity, and availability of federal information systems. By implementing key foundational practices, DOD has acted to mitigate those threats and secure its ICT supply chains.

Fully implementing the remaining practices on an agency-wide SCRM strategy, supplier reviews, and counterfeit detection are particularly important for providing an organization-wide approach to ICT SCRM. However, DOD has not committed to time frames for when these practices will be implemented. Until DOD implements these key foundational practices, it 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

We are making three recommendations to DOD:

- The Secretary of Defense should direct the DOD CIO to commit to a time frame to fully implement an agency-wide ICT SCRM strategy, including how the department will assess, respond to, or monitor ICT supply chain risks across the life cycle of ICT products and services. (Recommendation 1)
- The Secretary of Defense should direct the Undersecretary of Defense for Acquisition and Sustainment and the DOD CIO to commit

[28]Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, *Executive Order 13913 Annual Report to the President of the United States* (April 2022).

to a time frame to fully implement a process to conduct SCRM reviews of potential suppliers. (Recommendation 2)

- The Secretary of Defense should direct the Undersecretary of Defense for Acquisition and Sustainment and the DOD CIO to commit to a time frame to fully implement organizational counterfeit detection procedures for products prior to deployment. In doing so, the department should take into consideration the results of its pilot efforts of applicable tools. (Recommendation 3)

Agency Comments and Our Evaluation

We provided a draft of this report to DOD for review and comment. In its comments reproduced in appendix I, DOD agreed with the recommendations and described plans and time frames for completing actions intended to address the recommendations.

Regarding our first recommendation stating that the DOD CIO commit to a time frame to fully implement an agency-wide ICT SCRM strategy, the department concurred and noted actions it is taking to finalize a document intended to be the basis for a DOD enterprise-wide strategy. DOD expects to finalize the draft of its enterprise-wide ICT SCRM strategy in September 2023.

Regarding our second recommendation stating that the Undersecretary of Defense for Acquisition and Sustainment and DOD CIO commit to a time frame to fully implement a process to conduct ICT SCRM reviews of potential suppliers, the department concurred. In its response, the department identified several key policies it is in the process of updating to incorporate relevant policies and procedures, as appropriate.

Regarding our third recommendation stating that the Undersecretary of Defense for Acquisition and Sustainment and DOD CIO commit to a time frame to fully implement organizational counterfeit detection procedures for products prior to deployment, the department concurred with the assumption that the scope of the recommendation was for ICT products. As result, we clarified our third recommendation to confirm the intended scope of implementing counterfeit detection procedures for ICT products. In addition, the department noted that it expected the completion of its pilot efforts to evaluate various ICT counterfeit detection tools and development of related policies and procedures in fiscal year 2023. DOD

expects to incorporate those policies and procedures into department-wide policy by the end of March 2024.

If implemented effectively, the actions DOD described in its comments would address our recommendations. The department also provided technical comments, which we have incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees and the Secretary of Defense. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff members have any questions on matters 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 II.

Carol C. Harris
Director, Information Technology, Management Issues

List of Committees

The Honorable Jack Reed
Chairman
The Honorable Roger Wicker
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Jon Tester
Chair
The Honorable Susan Collins
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Mike Rogers
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Ken Calvert
Chair
The Honorable Betty McCollum
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Comments from the Department of Defense

CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

APR 2 1 2023

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

Dear Ms. Harris,

This is the Department of Defense (DoD) response to GAO Draft Report No. GAO-23-105612, "INFORMATION AND COMMUNICATIONS TECHNOLOGY: DOD Needs to Fully Implement Foundational Practice to Manage Supply Chain Risks," dated February 1, 2023.

Enclosed are DoD's comments to the three recommendations in the draft report. My point of contact is Michele Iversen who can be reached at michele.t.iversen.civ@mail.mil and (703) 697-6101.

Sincerely,

John B. Sherman

Enclosure:
As stated

GAO Draft Report No. GAO-23-105612
"INFORMATION AND COMMUNICATIONS TECHNOLOGY: DOD Needs to Fully Implement Foundational Practices to Manage Supply Chain Risks," dated February 2023.

DEPARTMENT OF DEFENSE COMMENTS
IN RESPONSE TO THE GAO RECOMMENDATIONS

GAO Recommendation 1 – The Secretary of Defense should direct the DoD Chief Information Officer to commit to a time frame to fully implement an agency-wide ICT SCRM Strategy, including how the department will assess, respond to, or monitor ICT supply chain risks across the lifecycle of ICT products and services.

DoD Response – DoD concurs. The DoD CIO is finalizing its update (expected April 2023) to the DoD CIO's internal ICT SCRM Strategy. The DoD CIO then intends to use that document as the basis for development of a DoD enterprise-level ICT SCRM Strategy, which will be consistent with the DoD's ongoing participation in the Federal Acquisition Security Council (FASC), established pursuant to the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) (Pub. L. 115-390). The DoD ICT SCRM Strategy will be developed and finalized through an iterative and coordinated process, to include a concept draft for DoD community review (expected April 2023), and a detailed strategy for review (expected July 2023). DoD expects to release the final draft for formal coordination in September 2023.

GAO Recommendation 2 – The Secretary of Defense should direct the USD(A&S) and the DoD CIO to commit to a time frame to fully implement a process to conduct ICT SCRM reviews of potential suppliers.

DoD Response – DoD concurs. The DoD CIO and the USD(R&E), in coordination with the USD(A&S) are in process of updating DoD Instruction (DoDI) 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN). In addition, the DoD CIO intends to update DoDI 5000.82, Acquisition of Information Technology (IT), and will pursue updates to other DoD policy documents, as appropriate, to incorporate relevant policies and procedures to address all DoD ICT acquisition.

GAO Recommendation 3 – The Secretary of Defense should direct the USD(A&S) and DoD CIO to commit to a time frame to fully implement organizational counterfeit detection procedures for products prior to deployment. In doing so, the department should take into consideration the results of its pilot efforts of applicable tools.

DoD Response – DoD concurs based upon the understanding that the scope of this recommendation is ICT products. DoD CIO pilot efforts to evaluate various ICT counterfeit detection tools, and the internal development of policies and procedures regarding the detection of potentially counterfeit ICT products is expected to be accomplished in Fiscal Year (FY) 2023. DoD will then pursue incorporation of these policies and procedures into DoD guides and policy documents, which is expected to be completed by the end of the 2nd quarter of FY 2024.

Accessible Text for Appendix I: Comments from the Department of Defense

APR 21 2023

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

Dear Ms. Harris,

This is the Department of Defense (DoD) response to GAO Draft Report No. GAO-23- 105612, "INFORMATION AND COMMUNICATIONS TECHNOLOGY: DOD Needs to Fully Implement Foundational Practice to Manage Supply Chain Risks," dated February 1, 2023.

Enclosed are DoD's comments to the three recommendations in the draft report. My point of contact is Michele Iversen who can be reached at michele.t.iversen.civ@mail.mil and (703) 697-6101.

Enclosure: As stated

Sincerely,

John B. Sherman

Enclosure:
As stated

GAO Draft Report No. GAO-23-105612
"INFORMATION AND COMMUNICATIONS TECHNOLOGY: DOD Needs to Fully Implement Foundational Practices to Manage Supply Chain Risks," dated February 2023.

DEPARTMENT OF DEFENSE COMMENTS
IN RESPONSE TO THE GAO RECOMMENDATIONS

GAO Recommendation 1 - The Secretary of Defense should direct the DoD Chief Information Officer to commit to a time frame to fully implement an agency-wide JCT SCRM Strategy, including how the department will assess, respond to, or monitor JCT supply chain risks across the lifecycle of JCT products and services.

DoD Response- DoD concurs. The DoD CIO is finalizing its update (expected April 2023) to the DoD CIO's internal ICT SCRM Strategy. The DoD CIO then intends to use that document as the basis for development of a DoD enterprise-level [CT SCRM Strategy, which will be consistent with the DoD's ongoing participation in the Federal Acquisition Security Council (FASC), established pursuant to the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) (Pub. L. 115-390). The DoD ICT SCRM Strategy will be developed and finalized through an iterative and coordinated process, to include a concept draft for DoD community review (expected April 2023), and a detailed strategy for review (expected July 2023). DoD expects to release the final draft for formal coordination in September 2023.

GAO Recommendation 2 - The Secretary of Defense should direct the USD(A&S) and the DoD CIO to commit to a time frame to fully implement a process to conduct JCT SCRM reviews of potential suppliers.

DoD Response - DoD concurs. The DoD CIO and the USD(R&E), in coordination with the USD(A&S) are in process of updating DoD Instruction (DoDI) 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN). In addition, the DoD CIO intends to update DoDI 5000.82, Acquisition of Information Technology (IT), and will pursue updates to other DoD policy documents, as appropriate, to incorporate relevant policies and procedures to address all DoD JCT acquisition.

GAO Recommendation 3 - The Secretary of Defense should direct the USD(A&S) and DoD CIO to commit to a time frame to fully implement organizational counterfeit detection procedures for products prior to deployment. In doing so, the department should take into consideration the results of its pilot efforts of applicable tools.

DoD Response- DoD concurs based upon the understanding that the scope of this recommendation is JCT products. DoD CIO pilot efforts to evaluate various JCT counterfeit detection tools, and the internal development of policies and procedures regarding the detection of potentially counterfeit ICT products is expected to be accomplished in Fiscal Year (FY) 2023. DoD will then pursue incorporation of these policies and procedures into DoD guides and policy documents, which is expected to be completed by the end of the 2nd quarter of FY 2024.

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Carol 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: Eric Winter (Assistant Director), Justin Booth (Analyst in Charge), Chris Businsky, Rebecca Eyler, Kendrick Johnson, Sandra Kerr, and Scott Pettis.

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/about/what-gao-does/fraudnet

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

Congressional Relations

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