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

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.