December 2020

INFORMATION TECHNOLOGY

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

GAO Highlights

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

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.

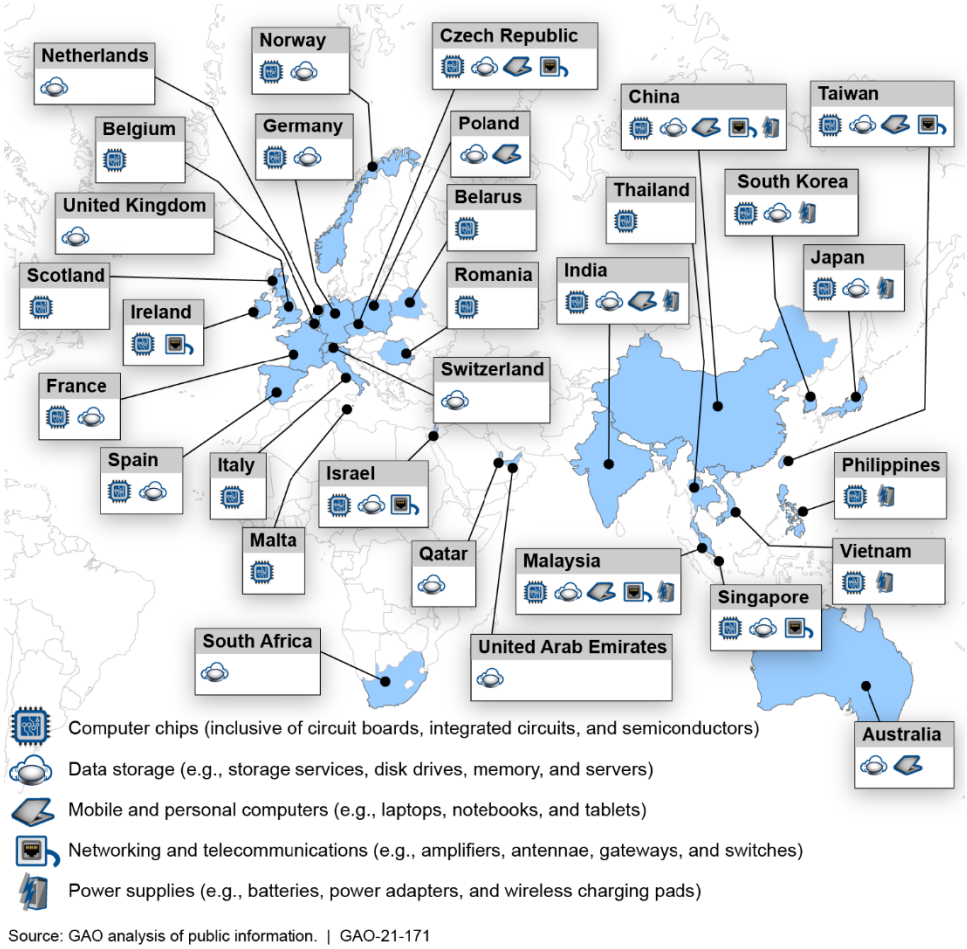
This is a public version of a sensitive report that GAO issued in October 2020. Information that agencies deemed sensitive was omitted and GAO substituted numeric identifiers that were randomly assigned for the names of the agencies due to sensitivity concerns.

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



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:

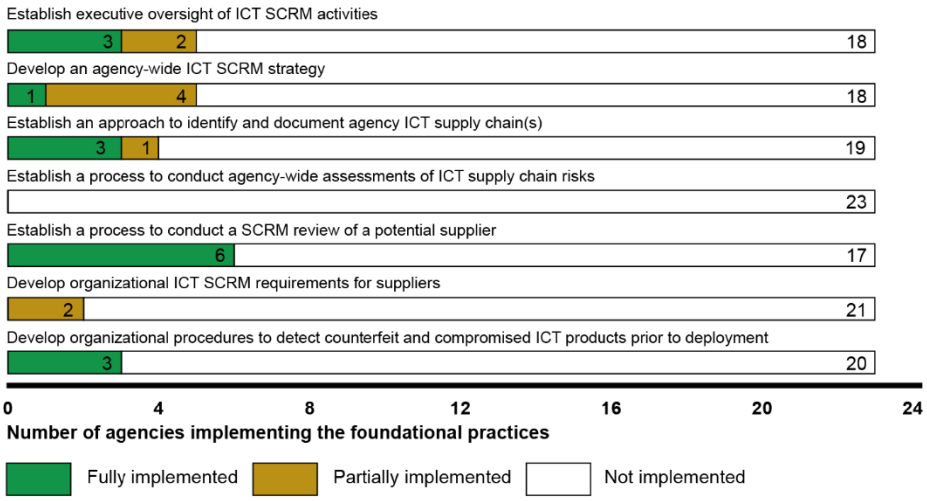
- establishing executive oversight of ICT activities, including designating responsibility for leading agency-wide SCRM activities;
- developing an agency-wide ICT SCRM strategy for providing the organizational context in which risk-based decisions will be made;
- establishing an approach to identify 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

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.