GAO@100

Highlights

Highlights of GAO-21-594T, a testimony before the Subcommittees on Investigations and Oversight and Research and Technology, Committee on Science, Space and Technology, House of Representatives

May 25, 2021

CYBERSECURITY

Federal Agencies Need to Implement Recommendations 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 malicious actors 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. Recent events involving a software supply chain compromise of SolarWinds Orion, a network management software suite, and the shutdown of a major U.S. fuel pipeline due to a cyberattack highlight the significance of these threats.

GAO was asked to testify on federal agencies' efforts to manage ICT supply chain risks. Specifically, GAO (1) describes the federal government's actions in response to the compromise of SolarWinds and (2) summarizes its prior report on the extent to which federal agencies implemented foundational ICT supply chain risk management practices. To do so, GAO reviewed its previously published reports and related information. GAO has ongoing work examining federal agencies' responses to SolarWinds and plans to issue a report on this in fall 2021.

What GAO Recommends

In a sensitive version of its December 2020 report, GAO made 145 recommendations to 23 federal agencies to fully implement selected foundational practices in their organization-wide approaches to ICT SCRM.

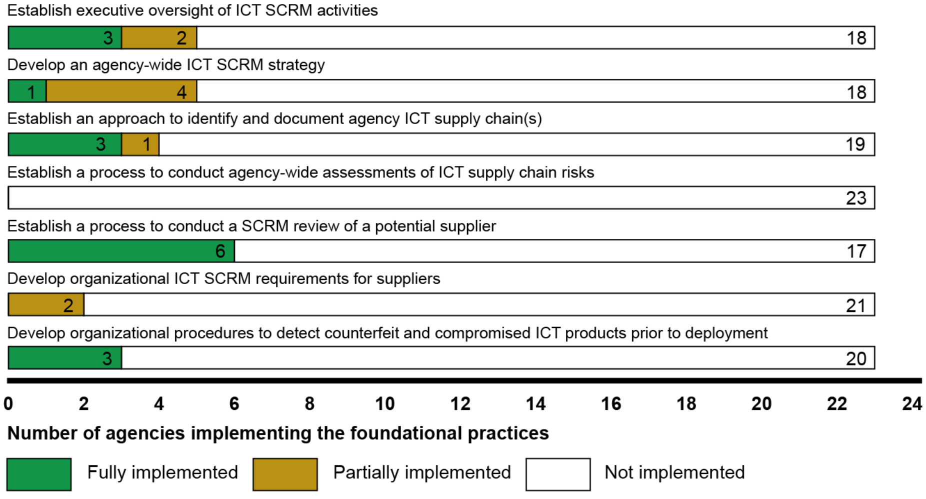
View GAO-21-594T. For more information, contact Vijay D'Souza (202) 512-6240 or dsouzav@gao.gov.

What GAO Found

Federal agencies continue to face software supply chain threats. In December 2020, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency issued an emergency directive requiring agencies to take action regarding a threat actor that had been observed leveraging a software supply chain compromise of a widely used enterprise network management software suite—SolarWinds Orion. Subsequently, the National Security Council staff formed a Cyber Unified Coordination Group to coordinate the government response to the cyberattack. The group took a number of steps, including gathering intelligence and developing tools and guidance, to help organizations identify and remove the threat.

During the same month that the SolarWinds compromise was discovered, GAO reported that none of 23 civilian agencies had fully implemented selected foundational practices for managing information and communication technology (ICT) supply chain risks—known as supply chain risk management (SCRM) (see figure).

Twenty-three Civilian Agencies' Implementation of Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM) Practices



Source: GAO analysis of agency data. | GAO-21-594T

GAO stressed that, as a result of not fully implementing the foundational practices, the agencies were at a greater risk that malicious actors could exploit vulnerabilities in the ICT supply chain, causing disruptions to mission operations, harm to individuals, or theft of intellectual property. Accordingly, GAO recommended that each of the 23 agencies fully implement these foundational practices. In May 2021, GAO received updates from six of the 23 agencies regarding actions taken or planned to address its recommendations. However, none of the agencies had fully implemented the recommendations. Until they do so, agencies will be limited in their ability to effectively address supply chain risks across their organizations.