United States Government Accountability Office

Testimony

Before the Subcommittees on Investigations and Oversight and Research and Technology, Committee on Science, Space and Technology, House of Representatives

For Release on Delivery
Expected at 2:00 p.m ET,
Tuesday, May 25, 2021

CYBERSECURITY

Federal Agencies Need to Implement Recommendations to Manage Supply Chain Risks

Statement of Vijay A. D'Souza, Director,
Information Technology and Cybersecurity

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO-21-594T

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.

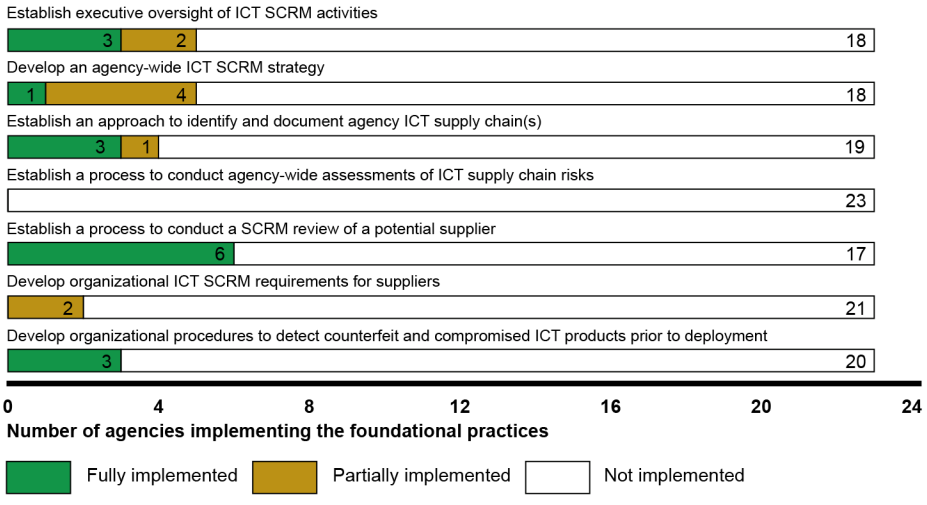
View GAO-21-594T. For more information, contact Vijay D'Souza (202) 512-6240 or dsouzav@gao.gov.

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.

Chairs Foster and Stevens, Ranking Members Obernolte and Waltz, and Members of the Subcommittees:

I am pleased to participate in today's hearing on the federal government's information and communications technology (ICT) supply chain risk management (SCRM) and recent cybersecurity incidents. The risks to information technology (IT) systems supporting the federal government and the nation's critical infrastructure are increasing, including insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, and the emergence of new and more destructive attacks.

We have designated information security as a government-wide high-risk area since 1997.[1] We expanded this high-risk area in 2003 to include the protection of critical cyber infrastructure. In September 2018, we reported that the federal government needed to take 10 specific actions to address the four major cybersecurity challenges that the federal government and other entities face: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data.[2] Since September 2018, we and others have made numerous recommendations to federal agencies and the Congress related to the 10 specific actions—including mitigating global supply chain risks—needed to address the four major cybersecurity challenges.

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

[1]See GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: March 2, 2021) and *High Risk Series: An Overview*, GAO-HR-97-1 (Washington, D.C.: February 1997). GAO maintains a high-risk program to focus attention on government operations that it identifies as high risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement or the need for transformation to address economy, efficiency, or effectiveness challenges.

[2]GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

supply chain and, thus, compromise the confidentiality, integrity, or availability of an organization's systems and the information they contain.

In September 2019, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) reported that federal agencies then faced approximately 180 different ICT supply chain-related threats. 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 persistence and significance of these threats.[3]

To address threats such as these, it is essential that agencies apply SCRM—that is, the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT products and service supply chains. Doing so is vital to agencies being effectively positioned to make risk-based decisions about how best to secure their systems.

In response to your request, my testimony today (1) describes the federal government's actions in response to the compromise of SolarWinds and (2) summarizes our prior report on the extent to which federal agencies have implemented foundational ICT SCRM practices. To prepare this statement, we reviewed our previously issued reports on major cybersecurity challenges and federal agencies' efforts to manage supply chain risks, as well as other information we have published that explains the compromise of SolarWinds and describes the federal government's efforts to coordinate and respond to the incident.[4] In addition, this statement includes updates on progress that agencies have made in implementing the recommendations made in our December 2020 supply chain report. Detailed information on the objectives, scope, and methodology of our work contributing to this statement can be found in the issued reports.

[3]GAO, *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)*, (Washington, D.C.: Apr. 22, 2021) and *Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness (infographic),* (Washington, D.C.: May 18, 2021).

[4]GAO, *Information and Communications Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-164SU (Washington, D.C.: Oct. 27, 2020); GAO-21-171; *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021) and *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)*, (Washington, D.C.: Apr. 22, 2021).

We conducted the work on which this statement is based 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The exploitation of ICT products and services through the supply chain is an emerging threat. ICT supply chain-related threats can be introduced in the manufacturing, assembly, and distribution of hardware, software, and services. Moreover, these threats can appear at each phase of the system development life cycle, when an agency initiates, develops, implements, maintains, and disposes of an information system. As a result, the compromise of an agency's ICT supply chain can degrade the confidentiality, integrity, and availability of its critical and sensitive networks, IT-enabled equipment, and data.

According to the Office of the Director of National Intelligence (ODNI), numerous supply chain attacks have occurred over the last several years. In response to one such recent attack, CISA issued an emergency directive and alert in December 2020 related to a cyberattack campaign that exploited software supply chain weaknesses in the SolarWinds Orion network management software.[5] Specifically, an advanced persistent threat actor used weaknesses in the software's supply chain to conduct a cyberattack campaign against U.S. government agencies, critical infrastructure entities, and private sector organizations.

To carry out the attack, the threat actor inserted a "backdoor"—a malicious program that can potentially give an intruder remote access to an infected computer—into a version of that software product. According to CISA, the malicious actor then used this backdoor, among other techniques, to initiate a cyberattack campaign against U.S. government agencies, critical infrastructure entities, and private-sector organizations. SolarWinds estimated that nearly 18,000 of its customers received a compromised software update. CISA further explained that the advanced

[5]CISA, *Mitigate SolarWinds Orion Code Compromise*, Emergency Directive 21-01 (Dec. 13, 2020); and *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations*, Alert AA20-352A (Dec. 17, 2020).

persistent threat actor had demonstrated complex intrusion techniques and that removing this threat actor from compromised IT networks would be highly complex and challenging.

Over the past several years, Congress and federal agencies have taken a number of steps aimed at mitigating ICT supply chain risks. For example:

- In December 2018, the Federal Acquisition Supply Chain Security Act of 2018 established the Federal Acquisition Security Council (FASC).[6] The FASC is a cross-agency council responsible for providing direction and guidance to executive agencies to reduce their ICT supply chain risks. According to officials in the Office of Management and Budget's (OMB) Office of the Chief Information Officer, the council finalized a strategic plan in June 2020 for addressing supply chain risks that is intended to, among other things, establish requirements for sharing relevant information about supply chain risks with all federal agencies.
- The Department of Homeland Security, through CISA, established the ICT SCRM Task Force in December 2018 as a public-private partnership to identify and develop strategies to enhance global ICT supply chain security. The task force has been extended until July 2021 to allow it to, among other things, collaborate on other ongoing public-private engagement efforts around supply chain, and support the FASC.
- The John S. McCain National Defense Authorization Act for Fiscal Year 2019 included a provision that prohibits executive branch agencies from, among other things, obtaining telecommunications equipment—or contracting with entities that use equipment—produced by Huawei Technologies Company, ZTE Corporation, or

[6]Federal Acquisition Supply Chain Security Act of 2018—Title II of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE Technology Act), Pub. L. No. 115-390, Title II, § 202(a), 132 Stat. 5173, 5178 (2018) (codified at 41 U.S.C. § 1322). The law also establishes requirements specifically for the heads of executive agencies. 41 U.S.C. § 1326.

any of their subsidiaries or affiliates.[7] In May 2019, the Department of Commerce (Commerce) added Huawei and certain non-U.S. affiliates to the Entity List[8] (with additional affiliates added in August 2019 and August 2020) as entities who may have engaged in activities that are contrary to U.S. national security or foreign policy interests and are subject to specific license requirements for the export, reexport, and/or transfer (in-country) of specified items.

- Also in May 2019, the President issued an executive order prohibiting transactions involving ICT and services provided by foreign adversaries or their agents, and which pose an undue risk to critical infrastructure or to U.S. national security.[9]
- In 2020, the Federal Communications Commission (FCC) published a final rule in response to ongoing concerns about the integrity of the communications supply chain.[10] The rule prohibits the use of money from the Universal Service Fund to purchase or obtain equipment or services from any communications equipment or service provider identified by the FCC's Public Safety and Homeland Security Bureau as posing a national security risk to communications networks or the communications supply chain, such as Huawei Technologies Company and ZTE Corporation.[11]

[7]The John S. McCain National Defense Authorization Act for Fiscal Year 2019 prohibits executive branch agencies from procuring, obtaining, extending, or renewing a contract to procure or obtain any equipment, system, or service that uses "covered telecommunications equipment or services" as a substantial or essential component of any system, or as critical technology as part of any system. Pub. L. No. 115-232, § 889(a)(1)(A), 132 Stat. 1636, 1917 (2018). Executive branch agencies are also prohibited from entering, renewing, or extending contracts with entities that use equipment containing "covered telecommunications equipment or services." *Id.*, at § 889(a)(1)(B). The act defines "covered telecommunications equipment or services" to include telecommunications equipment produced by Huawei Technologies Company (Huawei), ZTE Corporation, or any of their subsidiaries or affiliates. *Id.*, at § 889(f)(3)(A).

[8]The Entity List can be found at Supplement No. 4 to Part 744 of the Export Administration Regulations.

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

[10]See 47 C.F.R. § 54.9 (2020).

[11]To support broadband deployment in unserved areas, FCC provides billions through the Universal Service Fund's high-cost program to telecommunications carriers that offer broadband and voice services in areas that are costly to serve. These areas are typically rural or remote and increase carriers' infrastructure costs due to challenges, such as difficult terrain and longer distances between consumers. These areas also often have fewer consumers overall, further limiting carriers' abilities to offset infrastructure costs with end-user revenue.

- The President signed into law the Secure and Trusted Communications Networks Act of 2019 in March 2020, which prohibits the use of certain federal funds to obtain or maintain communications equipment or services from a company that, as determined by the FCC, poses an unacceptable risk to U.S. national security or the security of U.S. persons.[12]
- In February 2021, the President issued an executive order requiring the Secretaries of Commerce and Homeland Security to submit a report by February 2022 on supply chains for critical sectors of the ICT industrial base, including the industrial base for the development of software, data, and associated services.[13]
- In May 2021, CISA announced the publication of an ICT SCRM toolkit to assist organizations with information on how to secure ICT and related supply chains.

Despite these measures, we have previously reported that federal agencies have not effectively managed supply chain risks (which we further discuss later in this statement).[14] Similarly, we have previously reported on supply chain ICT risks to our nation's critical infrastructure sectors. For example:

- In June 2019, we reported that more than 2.7 million miles of pipeline that transports and distributes the natural gas, oil, and other hazardous liquids that U.S. citizens and businesses depend on, increasingly rely on sophisticated networked computerized systems and electronic data, which may be vulnerable to cyberattack or intrusion if not adequately protected.[15] In December 2018, we reported on weaknesses in the Transportation Security Administration's (TSA) management of its pipeline security efforts, including that the quantity of TSA's reviews of corporate and critical facilities security had varied considerably. So far, TSA has fully addressed 7 of our 10 recommendations for improving their oversight of pipeline security. However, 3 recommendations related to pipeline

[12]Pub. L. No. 116-124, §§ 2-3, 134 Stat. 158-159 (2020).

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

[14]GAO-21-171.

[15]GAO, *Critical Infrastructure Protection: Key Pipeline Security Documents Need to Reflect Current Operating Environment*, GAO-19-426 (Washington, D.C.: June 5, 2019).

security workforce and risk management have yet to be fully addressed.[16]

- In August 2019,[17] we reported that the Federal Energy Regulatory Commission (FERC)[18] had approved a new standard in October 2018 to bolster SCRM protections for the nation's bulk power system.[19] However, we found that this and other FERC-approved cybersecurity standards only partially addressed NIST's guidance for improving critical infrastructure cybersecurity. In particular, the standards fully addressed associated subcategories for establishing SCRM processes, security measures in contracts with suppliers and third-party partners, and evaluations of suppliers and third-party partners to ensure they meet their contractual obligations. However, the standards did not address subcategories for response and recovery planning and testing with suppliers and third-party providers, and for using the SCRM process to identify, prioritize, and assess suppliers and third-party partners.
- In October 2020, we reported that vulnerabilities can be introduced to avionics systems at multiple points within an insecure supply chain.[20] To date, extensive cybersecurity controls have been implemented and there have not been any reports of successful cyberattacks on an airplane's avionics system. However, the increasing connections between airplanes and other systems, combined with the evolving cyber threat landscape, could lead to increasing risks for future flight safety.

[16]GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, GAO-19-48 (Washington, D.C.: Dec. 18, 2018).

[17]GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO-19-332 (Washington, D.C.: Aug. 26, 2019).

[18]FERC is the regulator for the interstate transmission of electricity with responsibility to review and approve standards for the reliable operation of the bulk power system.

[19]The term "bulk power system" refers to (1) facilities and control systems necessary for operating the interconnected electric transmission network and (2) the output from certain generation facilities needed for reliability. FERC oversees the North American Electric Reliability Corporation, the federally designated U.S. electric reliability organization responsible for conducting reliability assessments and developing and enforcing mandatory standards to provide for reliable operation of the bulk power system.

[20]GAO, *Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks*, GAO-21-86 (Washington, D.C.: Oct. 9, 2020).

- In November 2020, we reported that the global reach of the 5G supply chain, as well as the technological complexity of the components of 5G technologies, presented the risk that components from suppliers whose quality and security could not be fully guaranteed may be used in 5G networks.[21] According to an April 2019 Defense Innovation Board report, a compromised 5G supply chain could pose a serious threat to national security by introducing vulnerabilities into networks and systems.[22]

In addition to our findings, the Cyberspace Solarium Commission[23] has also made recommendations related to the challenge of mitigating supply chain risks.[24] For example, the Commission has recommended that:

- Congress direct the U.S. government to develop and implement an ICT industrial base strategy to ensure more trusted supply chains.
- Congress appropriate consistent funding and task the executive branch to develop and implement research and development priorities in emerging technologies.
- Congress and the executive branch identify and budget the funds necessary to achieve the goals of the Cyber Moonshot Initiative.[25]
- The Supply Chain and Counterintelligence Risk Management Task Force within ODNI explore additional avenues to expand its support to critical infrastructure.
- The executive branch strengthen the capacity of the Committee on Foreign Investment in the United States.

[21]GAO, *5G Wireless: Capabilities and Challenges for an Evolving Network*, GAO-21-26SP (Washington, D.C.: November 24, 2020).

[22]Defense Innovation Board, *The 5G Ecosystem: Risks & Opportunities for DOD* (Washington, D.C.: April 2019).

[23]John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1652, 132 Stat. 1636, 2140 (2018) established the Cyberspace Solarium Commission, a federal commission made up of members of Congress and appointees, as well as officials from the Office of the Director of National Intelligence, the Department of Homeland Security, the Department of Defense, and the Federal Bureau of Investigation.

[24]U.S. Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report* (Washington, D.C.: March 2020).

[25]In 2018, the President's National Security Telecommunications Advisory Committee called for a "moonshot" initiative to address the action needed to address the "progressively worsening cybersecurity threat environment" facing our public safety, economic prosperity, and national security. The President's National Security Telecommunications Advisory Committee, *NSTAC Report to the President on a Cybersecurity Moonshot* (Nov. 14, 2018).

Recent events have illustrated that the nation's critical infrastructure continues to face growing and increasingly sophisticated cyber threats, as demonstrated by the SolarWinds incident, as well as the ransomware attack that led to a shutdown of a major U.S. fuel pipeline in early May 2021.[26]

Federal Agencies Have Taken Actions to Respond to the Recent Compromise of Widely Used Network Management Software

In response to the recent compromise of a widely used network management software—SolarWinds Orion—several federal agencies have taken action. Specifically, in December 2020, CISA issued an emergency directive requiring agencies to take action and an alert explaining that an advanced persistent threat actor, later determined to be the Russian Foreign Intelligence Service, had been observed leveraging, among other techniques, a software supply chain compromise of the SolarWinds software.[27] As emphasized in the directive, this threat posed a grave risk to federal, state, local, tribal, and territorial governments, as well as critical infrastructure entities and other private sector organizations.

Also in December 2020, the National Security Council (NSC) staff formed a Cyber Unified Coordination Group (UCG), in accordance with Presidential Policy Directive-41, to coordinate the government response to the cyberattack. The UCG is composed of the Federal Bureau of Investigation (FBI), CISA, and ODNI, with support from the National Security Agency (NSA).

In response to the incident, the UCG was tasked with, and took, a number of steps to help organizations identify and remove the threat actor. These steps included gathering intelligence and developing tools and guidance. Specifically, the FBI identified the scale and scope of the incident and engaged with affected entities. In addition, NSA and CISA released cybersecurity advisories that detailed adversary techniques and provided mitigation actions for system owners.

[26]Ransomware is a type of malware used to deny access to IT systems or data and hold the systems or data hostage until a ransom is paid.

[27]CISA, Emergency Directive 21-01 and Alert AA20-352A.

The UCG also undertook a number of other efforts. For example:

- The UCG reported in January 2021, that fewer than 10 U.S. government agencies were compromised for the primary purpose of espionage.
- In March 2021, CISA released the CISA Hunt and Incident Response Program, a software tool that helps network defenders find indicators of compromise associated with malicious activity for on-premises systems.
- In April 2021, CISA, the FBI, and NSA jointly confirmed that the Russian Foreign Intelligence Service was responsible for the SolarWinds incident. In addition, to aid organizations in conducting their own investigations and security their networks, the Department of Homeland Security, including CISA, and the FBI released an advisory providing information on the Russian Foreign Intelligence Service's cyber tools, targets, techniques, and capabilities.
- Also in April 2021, the NSC stated that lessons learned from this incident will be identified and used to improve future federal government responses to significant cyber incidents.[28]

Subsequent to these actions, in April 2021, the Deputy National Security Advisor for Cyber and Emerging Technology announced the deactivation of the Cyber UCG for the SolarWinds incident. According to the Deputy National Security Advisor, the group was deactivated after the UCG completed its initial surge efforts.

In addition to the actions taken by the UCG, in April 2021, the President issued Executive Order 14024. The executive order declared a national emergency to address the threat of harmful foreign activities of the Government of the Russian Federation, including engaging in and facilitating malicious cyber-enabled activities against the United States and its allies and partners.[29]

Also, in May 2021, the President issued Executive Order 14028 that was prompted, in part, by the compromise of the SolarWinds software supply chain. Among other things, the executive order directed the Secretary of Homeland Security, in consultation with the Attorney General, to establish

[28]https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/19/statement-by-deputy-national-security-advisor-for-cyber-and-emerging-technology-on-solarwinds-and-microsoft-exchange-incidents/ (accessed Apr. 20, 2021).

[29]The White House, *Blocking Property With Respect To Specified Harmful Foreign Activities of the Government of the Russian Federation*, Executive Order 14024 (Washington, D.C.: Apr. 15, 2021).

a Cyber Safety Review Board to review and assess the threat activity, vulnerabilities, and mitigation activities of, and agency responses to, significant cyber incidents.[30]

The Board's initial review is to be focused on the compromise of SolarWinds and is to include recommendations to the Secretary of Homeland Security for improving cybersecurity and incident response practices. To address software supply chain security, the executive order directed, among other things, the Director of the National Institute of Standards and Technology's (NIST) to publish guidelines that include criteria to evaluate the security practices of developers and suppliers of critical software and guidance identifying practices that enhance the security of the software supply chain.[31]

We have ongoing work examining federal agencies' responses to SolarWinds and any lessons that they have identified from the compromise. We plan to issue a report detailing our findings later this Fall 2021.

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

The recent compromise of SolarWinds highlights the significance of threats to the ICT supply chain. In December 2020, we reported on the 23 civilian agencies'[32] implementation of foundational practices for managing ICT supply chain risks.[33] In that report, we identified and selected the

[30]The White House, *Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021).

[31]The executive order defines critical software as software that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources).

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

[33]GAO-21-171.

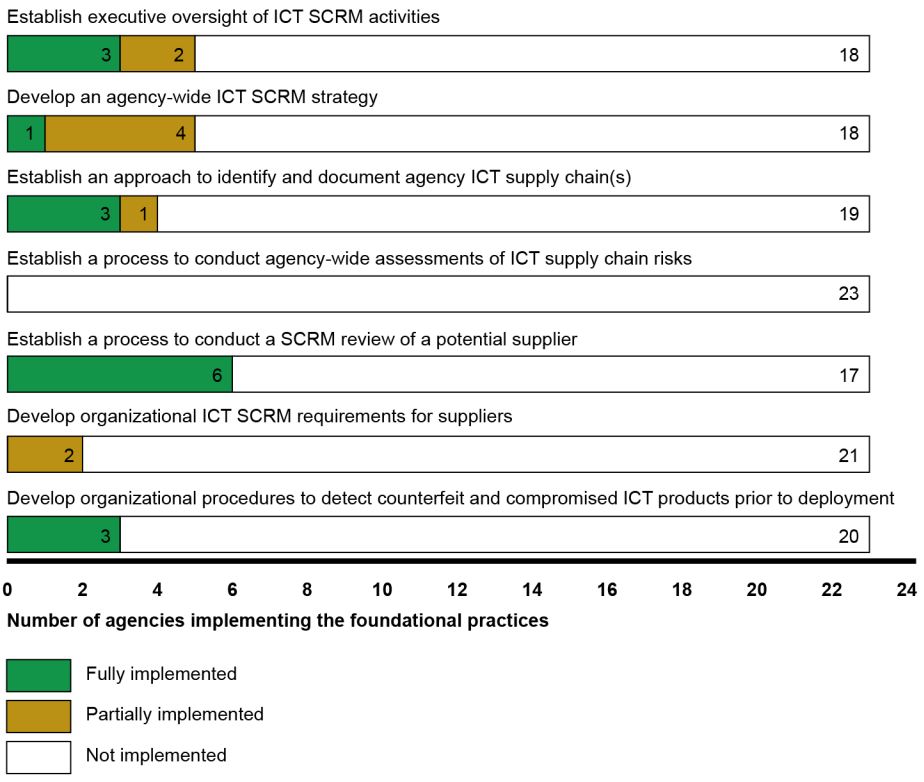
seven practices from NIST's guidance that are considered foundational for an organization-wide approach to ICT SCRM.[34] These selected foundational practices are:

- 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.

However, as we discussed in our report, none of the 23 agencies had fully implemented all of the supply chain risk management practices. Further, 14 of the 23 agencies had not implemented any of the practices. Figure 1 summarizes the extent of the agencies' implementation of the practices.

[34]See NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, v. 1.1 (Apr. 16, 2018); *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, SP 800-161 (Gaithersburg, Md.: Apr. 2015); *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST SP 800-37, Rev. 2 (Gaithersburg, Md.: Dec. 2018); and *Managing Information Security Risk: Organization, Mission, and Information System View*, SP 800-39 (Gaithersburg, Md.: Mar. 2011).

Figure 1: Extent to Which 23 Civilian Agencies Implemented Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM) Practices



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

As a result of not fully implementing these selected foundational practices, the agencies are 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. 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 had limited their implementation of the selected foundational practices for managing supply chain risks. The most commonly cited factor was the lack of

federal SCRM guidance. For example, 11 agencies reported that they were waiting for federal guidance to be issued from the FASC before implementing one or more of the selected foundational practices. At the time that our report was issued, according to OMB officials, the council expected to complete this effort by December 2020. As of May 2021, we have not yet received further information from OMB regarding the council's progress on this effort.

Nevertheless, while the additional direction and guidance from the council could further assist agencies with the implementation of the selected foundational practices, federal agencies currently have guidance they can already use to assist with managing their ICT supply chain risks. Specifically, NIST issued ICT SCRM-specific guidance in 2015[35] and OMB has required agencies to implement ICT SCRM since 2016.[36]

NIST is currently updating its guidance, with a final version expected by April 2022. According to NIST, the revised guidance, among other things, is expected to capture leading cyber SCRM practices from government and industry and integrate related SCRM concepts and processes from other NIST publications.

In a sensitive report issued in October 2020, we made 145 recommendations to the 23 agencies to fully implement selected foundational practices in their organization-wide approaches to ICT SCRM.[37] 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 believe that all of the recommendations are warranted.

In May 2021, we received updates from six of the 23 agencies regarding actions taken or planned to address our recommendations. We are currently evaluating evidence provided by these six agencies to determine the extent to which implementation of recommendations has occurred. However, to date, none of the agencies have yet fully

[35]NIST SP 800-161.

[36]OMB, Managing Information as a Strategic Resource, Circular No. A-130 (July 28, 2016).

[37]GAO-21-164SU.

addressed recommendations to implement foundational practices in their organization-wide approach to ICT SCRM. We intend to continue monitoring agencies' progress in implementing them.

In summary, as our work has emphasized, the need for agencies to make risk-based ICT supply chain decisions about how to secure their systems is urgent. Recent events, such as the compromise of SolarWinds Orion, highlight the importance of implementing SCRM to protect against threats posed by malicious actors. In the absence of foundational risk management practices, malicious actors may continue to exploit vulnerabilities in the ICT supply chain, causing further disruption to mission operations, harm to individuals, or theft of intellectual property.

Chairs Foster and Stevens, Ranking Members Obernolte and Waltz, and Members of the Subcommittees, this completes my prepared statement. I would be pleased to respond to any questions that you may have.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Vijay A. D'Souza, Director of Information Technology and Cybersecurity, at (202) 512-6240 or dsouzav@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Edward R. Alexander, Jr. (Assistant Director), Josh Leiling (Assistant Director), Season Burris (Analyst-in-Charge), Linda Erickson, Rebecca Eyler, Keith Kim, Katherine Noble, Niti Tandon, and Scott Pettis. Other staff who made key contributions to the reports cited in the testimony were Anna Bennett, Kiana Beshir, Donald Baca, Christopher Businsky, Donna Epler, John deFerrari, Jennifer Franks, Carol Harris, Kaelin Kuhn, Hoyt Lacy, Catherine Maloney, Nick Marinos, Carlo Mozo, Sukhjoot Singh, Angela Watson, and Eric Winter.

Vijay D'Souza a Director of Information Technology and Cybersecurity at the US Government Accountability Office (GAO) where he leads a diverse set of evaluations of government cybersecurity and IT issues. Current areas of work include ransomware, the SolarWinds breach, use of the NIST Cybersecurity Framework and IT modernization efforts at USDA. Vijay also leads GAO's Center for Enhanced Cybersecurity, which provides advanced technical support for GAO's cybersecurity audits. He previously led GAO's data analytics activities and worked for GAO's Health Care Team. Vijay has been at GAO since 2001. Prior to GAO, he worked in the international development area, and before that as a developer of technology training. Mr. D'Souza has an M.B.A from the University of California Berkeley and a B.S. in Engineering from the University of Maryland, College Park.