United States Government Accountability Office

Report to Congressional Addressees

January 2022

CYBERSECURITY

Federal Response to SolarWinds and Microsoft Exchange Incidents

GAO-22-104746

GAO Highlights

Highlights of GAO-22-104746, a report to congressional addressees

January 2022

CYBERSECURITY

Federal Response to SolarWinds and Microsoft Exchange Incidents

Why GAO Did This Study

The risks to information technology systems supporting the federal government and the nation's critical infrastructure are increasing, including escalating and emerging threats from around the globe, the emergence of new and more destructive attacks, and insider threats from witting or unwitting employees. Information security has been on GAO's High Risk List since 1997.

Recent incidents highlight the significant cyber threats facing the nation and the range of consequences that these attacks pose. A recent such incident, involving SolarWinds, resulted in one of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and private sector. Another incident included zero-day Microsoft Exchange Server vulnerabilities that had the potential to affect email servers across the federal government and provide malicious threat actors with unauthorized remote access. According to CISA, the potential exploitation from both incidents posed an unacceptable risk to federal civilian executive branch agencies because of the likelihood of vulnerabilities being exploited and the prevalence of affected software.

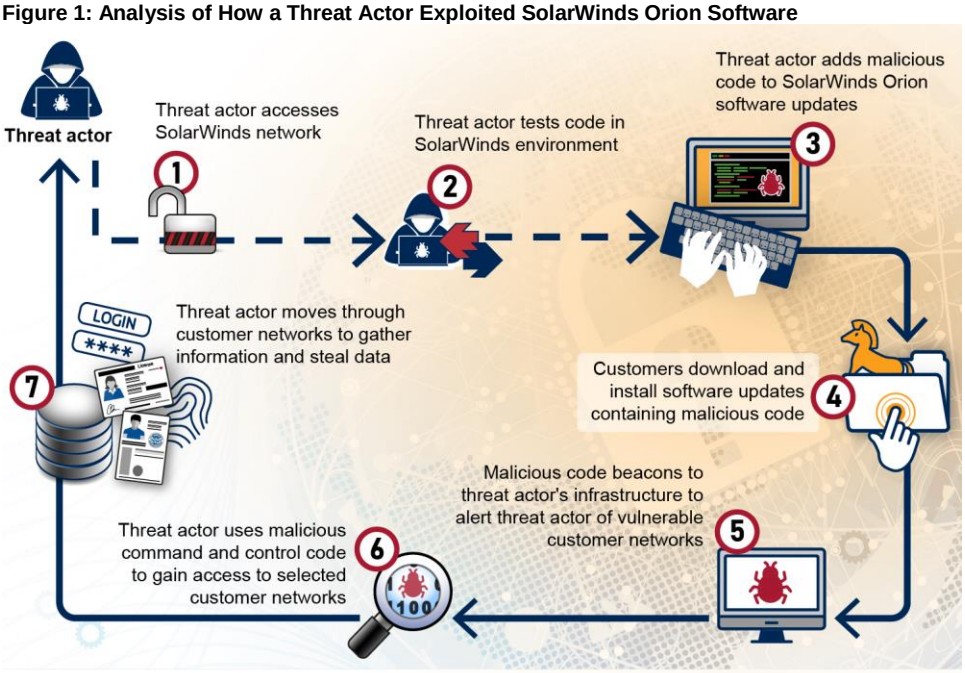
GAO performed its work under the authority of the Comptroller General to conduct an examination of these cybersecurity incidents in light of widespread congressional interest in this area. Specifically, GAO's objectives were to (1) summarize the SolarWinds and Microsoft Exchange cybersecurity incidents, (2) determine the steps federal agencies have taken to coordinate and respond to the

View GAO-22-104746. For more information, contact Nick Marinos (202) 512-9342 or marinosn@gao.gov or Jennifer Franks (404) 679-1831 or franksj@gao.gov.

What GAO Found

Beginning as early as January 2019, a threat actor breached the computing networks at SolarWinds—a Texas-based network management software company, according to the company's Chief Executive Officer. The federal government later confirmed the threat actor to be the Russian Foreign Intelligence Service. Since the company's software, SolarWinds Orion, was widely used in the federal government to monitor network activity and manage network devices on federal systems, this incident allowed the threat actor to breach several federal agencies' networks that used the software (see figure 1).

Figure 1: Analysis of How a Threat Actor Exploited SolarWinds Orion Software



Source: GAO analysis of documentation from publicly released private industry and federal agency reports; images: kras99/stock.adobe.com, anna_leni/stock.adobe.com. | GAO-22-104746

While the response and investigation into the SolarWinds breach were still ongoing, Microsoft reported in March 2021 the exploitation or misuse of vulnerabilities used to gain access to several versions of Microsoft Exchange Server. This included versions that federal agencies hosted and used on their premises. According to a White House statement, based on a high degree of confidence, malicious cyber actors affiliated with the People's Republic of China's Ministry of State Security conducted operations utilizing these Microsoft Exchange vulnerabilities. The vulnerabilities initially allowed threat actors to make authenticated connections to Microsoft Exchange Servers from unauthorized external sources. Once the threat actor made a connection, the actor then could leverage other vulnerabilities to escalate account privileges and install web shells that enabled the actor to remotely access a Microsoft Exchange Server. This in turn allowed for persistent malicious operations even after the vulnerabilities were patched (see figure 2).

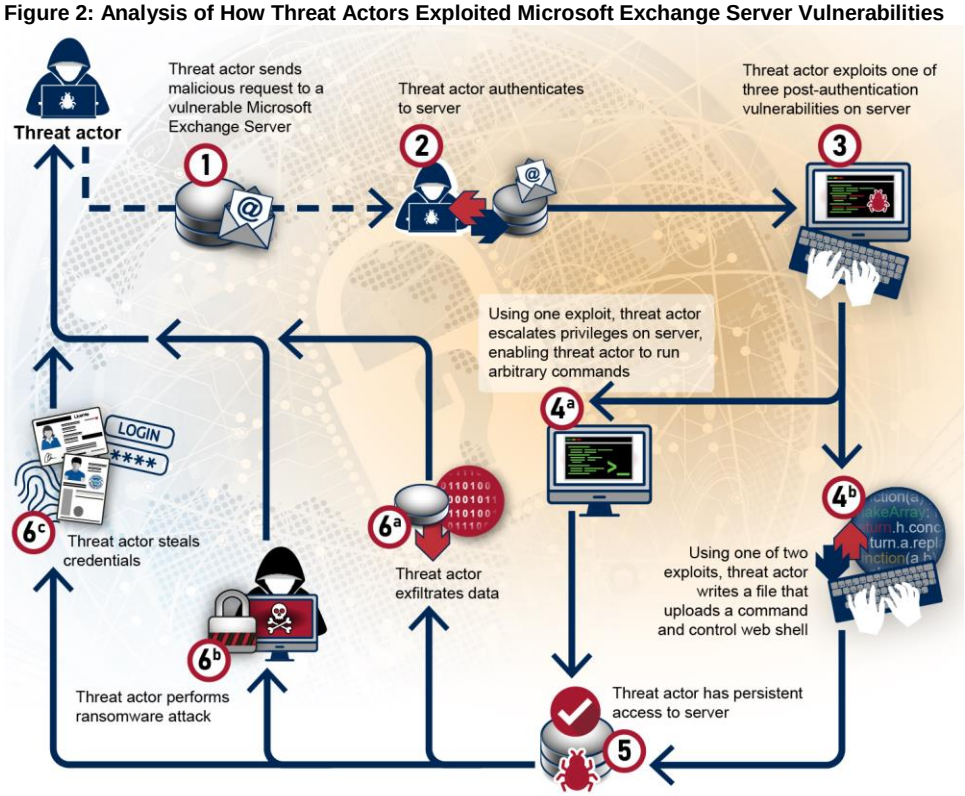
incidents, and (3) identify lessons federal agencies have learned from the incidents.

To do so, GAO reviewed documentation such as descriptions of the incidents, federal agency press releases, response plans, joint statements, and guidance issued by the agencies responsible for responding to the incidents: DHS (CISA), the Department of Justice (FBI), and ODNI with support from NSA. In addition, GAO analyzed incident reporting documentation from affected agencies and after-action reports to identify lessons learned. For all objectives, GAO interviewed agency officials to obtain additional information about the incidents, coordination and response activities, and lessons learned.

What GAO Recommends

Since 2010, GAO has made about 3,700 recommendations to agencies aimed at remedying cybersecurity shortcomings. As of November 2021, about 900 of those recommendations had not yet been fully implemented. GAO will continue to monitor federal agencies' progress in fully implementing these recommendations, including those related to software supply chain management and cyber incident management and response. Five of six agencies provided technical comments, which we incorporated as appropriate.

Figure 2: Analysis of How Threat Actors Exploited Microsoft Exchange Server Vulnerabilities



Source: GAO analysis of documentation from publicly released private industry and federal agency reports; images: kras99/stock.adobe.com, anna_leni/stock.adobe.com. | GAO-22-104746

Federal agencies took several steps to coordinate and respond to the SolarWinds and Microsoft Exchange incidents including forming two Cyber Unified Coordination Groups (UCG), one for the SolarWinds incident and one for the Microsoft Exchange incident. Both UCGs consisted of the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and the Office of the Director of National Intelligence (ODNI), with support from the National Security Agency (NSA). According to UCG agencies, the Microsoft Exchange UCG also integrated several private sector partners in a more robust manner than their involvement in past UCGs.

CISA issued emergency directives to inform federal agencies of the vulnerabilities and describe what actions to take in response to the incidents. To aid agencies in conducting their own investigations and securing their networks, UCG agencies also provided guidance through advisories, alerts, and tools. For example, the Department of Homeland Security (DHS), including CISA, the FBI, and NSA released advisories for each incident providing information on the threat actor's cyber tools, targets, techniques, and capabilities. CISA and certain agencies affected by the incidents have taken steps and continue to work together to respond to the SolarWinds incident. Agencies have completed steps to respond to the Microsoft Exchange incident.

Agencies also identified multiple lessons from these incidents. For instance,

- coordinating with the private sector led to greater efficiencies in agency incident response efforts;
- providing a centralized forum for interagency and private sector discussions led to improved coordination among agencies and with the private sector;
- sharing of information among agencies was often slow, difficult, and time consuming and;
- collecting evidence was limited due to varying levels of data preservation at agencies.

Effective implementation of a recent executive order could assist with efforts aimed at improving information sharing and evidence collection, among others.

Contents

Abbreviations

APT	advanced persistent threat
CFO Act	Chief Financial Officers Act
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department Justice
FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Modernization Act
ICT	information and communications technology
IT	information technology
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSC	National Security Council
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
PII	personally identifiable information
PPD	Presidential Policy Directive
UCG	Cyber Unified Coordination Group

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

January 13, 2022

Congressional Addressees

The risks to information technology (IT) systems supporting the federal government and the nation's critical infrastructure are increasing, including escalating and emerging threats from around the globe, the emergence of new and more destructive attacks, and insider threats from witting or unwitting employees. Information security has been on our High Risk List since 1997.[1] Recent incidents highlight the significant cyber threats facing the nation and the range of consequences that these attacks pose.[2]

A recent such event resulted in one of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and private sector. The attack involved an advanced persistent threat actor that compromised the network management software suite SolarWinds Orion as part of a software supply chain cyberattack campaign.[3] The threat actor inserted a "backdoor"—a malicious program that can potentially give an intruder remote access to an infected computer—into a genuine version of that software product.[4] Beginning in early 2020 the threat actor then used this backdoor, among

[1]See GAO, *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, *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)*, (Washington, D.C.: Apr. 22, 2021). https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic (accessed May 5, 2021) and *Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness (infographic)*, (Washington, D.C.: May 18, 2021). https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic (accessed May 18, 2021).

[3]A software supply chain attack occurs when a cyber threat actor infiltrates a software vendor's network and employs malicious code to compromise the software before the vendor sends it to their customers. The compromised software then compromises the customer's data or system.

[4]Threat actors include foreign intelligence services and militaries, corporate spies, corrupt government officials, cyber vandals, disgruntled employees, radical activists, purveyors of counterfeit goods, or criminals.

other techniques, to initiate a cyberattack campaign against U.S. government agencies, critical infrastructure entities, and private sector organizations. The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) initially alerted federal agencies to the SolarWinds attack in December 2020.

Shortly following the announcement of the SolarWinds attack, in a separate incident, Microsoft reported in March 2021 that other threat actors were exploiting zero-day vulnerabilities in Microsoft's Exchange Server products used to provide on-premises[5] IT services such as email, address books, and calendars.[6] According to Microsoft, approximately 400,000 customers of these products, including federal government agencies, were at risk globally.

The threat actors exploiting the Microsoft Exchange Server products would have been able to leverage the vulnerabilities to gain access to federal government email accounts and data, as well as install malware on systems and harvest user credentials, which could have been used to gain persistent unauthorized access to other networks at an impacted agency. According to CISA, this potential exploitation posed an unacceptable risk to federal civilian executive branch agencies because of the likelihood of vulnerabilities being exploited and the prevalence of affected software in the federal enterprise. Thus, CISA determined that federal agencies must take emergency action to address the threat.

We performed our work under the authority of the Comptroller General to conduct an examination of these cybersecurity incidents in light of widespread congressional interest in this area. Specifically, our objectives were to (1) provide a summary of the SolarWinds and Microsoft Exchange cybersecurity incidents, (2) determine the steps federal

[5]CISA Emergency Directive 21-02 states that any operational Microsoft Exchange Servers hosted by or on behalf of federal agencies that had been connected to the Internet, either directly or indirectly, are considered on-premises instances. Hosted servers denote any instance of Microsoft Exchange Servers hosted by or on behalf of federal agencies on agency or third-party premises, excluding Microsoft Office 365. CISA, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*, Emergency Directive 21-02 (March 3, 2021).

[6]A zero-day vulnerability can lead to a threat actor exploiting a previously unknown hardware, firmware, or software vulnerability, which has no existing official fix or patch.

agencies have taken to coordinate and respond to the incidents, and (3) identify lessons federal agencies have learned from the incidents.

To address the first objective, we interviewed officials from the agencies comprising the Cyber Unified Coordination Groups (UCG) for these incidents: CISA, Department of Justice's (DOJ) Federal Bureau of Investigation (FBI), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA).[7] We collected and reviewed descriptions of the incidents, including timelines and entities involved, and researched blogs from cybersecurity research firms and vendors to better understand the technical aspects of the incidents. Based on the information collected from agencies and our research, we developed graphics to depict the key activities that occurred during the two incidents. We shared the graphics with the agencies to verify that we were accurately describing the incidents.

To address the second objective, we reviewed documentation such as federal agency press releases, response plans, and joint statements from the UCG agencies. In addition, we collected and analyzed emergency directives, mitigation guidance, advisories, alerts, timelines and descriptions of coordination and response activities, and malware analysis reports from UCG agencies. We reviewed transcripts and testimony statements from several hearings held on the incidents. We also interviewed officials from the UCG agencies to identify steps taken in coordinating and responding to the incidents, and work that remained to be completed.

Further, we collected and reviewed required reporting documentation submitted by the 24 major federal agencies[8] in accordance with CISA's

[7]A Cyber Unified Coordination Group can be formed to coordinate the federal response to a significant cyber incident.

[8]Major federal agencies include those for which the Chief Financial Officers (CFO) Act of 1990 established a CFO position, referred to as CFO Act agencies. The CFO Act agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, 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.

Emergency Directives associated with these incidents.[9] We also collected and reviewed any incident reporting documentation submitted by the 24 major federal agencies associated with the Office of Management and Budget (OMB) incident reporting guidance.[10] After reviewing the incident reporting documentation, we identified what steps the 24 major federal agencies took to coordinate and resolve the incidents, and what work remained to be completed.

To address the third objective, we collected information through interviews with CISA, FBI, ODNI, NSA, and the National Security Council (NSC).[11] We requested information on lessons learned from the 24 major federal agencies if they had identified any through after action reports for either incident. Through our interviews and collection, we categorized and grouped lessons federal agencies have learned from the incidents, including positive practices that resulted in improved coordination and negative practices that resulted in undesirable outcomes in the coordination and response to the incidents.

We conducted this performance audit from January 2021 to January 2022 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 information and communications technology (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

[9]CISA, *Mitigate SolarWinds Orion Code Compromise*, Emergency Directive 21-01 (Dec. 13, 2020) and CISA, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*, Emergency Directive 21-02 (March 3, 2021).

[10]OMB, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*, OMB Memorandum M-21-02 (Washington, D.C.: Nov. 9, 2020).

[11]The officials from the UCG agencies referred us to the NSC who had the responsibility to conduct the post-incident review and document the lessons learned. A 60-day review was conducted on the SolarWinds incident by the NSC. According to multiple officials, no formal review would be conducted on the Microsoft Exchange Server incident.

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. Such was the case as a threat actor maliciously accessed the networks of several federal agencies by compromising a network management suite of products developed and sold by SolarWinds—a Texas-based network management software company.

A zero-day exploit, the type used in the Microsoft Exchange incident, is an exploit that takes advantage of a security vulnerability previously unknown to the general public. By writing an exploit for the previously unknown vulnerability, an attacker creates a potent threat since the compressed time frame between public discoveries of both makes it difficult to defend against. Microsoft discovered that several versions of its enterprise email and calendar server software, Microsoft Exchange Server, were vulnerable to a number of zero-day exploits which had the potential of exposing federal agencies that had the software installed to compromise.

The emergence of increasingly sophisticated threats and the continuous reporting of cyber incidents underscores the continuing and urgent need for effective information security. Threats come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives. For example, advanced persistent threats (APT) pose increasing risks.[12] The SolarWinds and Microsoft Exchange cybersecurity incidents are examples of far-reaching and complex threats against the federal government that warrant further analysis and review. These incidents reinforce the need for a fast and effective federal response.

GAO Has Previously Reported on Federal Cybersecurity Weaknesses

We have previously reported that the federal government continues to face numerous cybersecurity weaknesses due, in large part, to ineffective information security programs. In addition, the cyber threat to critical

[12]NIST Special Publication 800-53 revision 5 defines an advanced persistent threat as an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors, including cyber, physical, and deception. These objectives typically include establishing and extending footholds within the IT infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future.

infrastructure continues to grow and represents a national security challenge.[13]

We have also reported that federal agencies had not effectively managed supply chain risks, yet the growing dependence on a globally distributed supply chain—and the lack of control over and visibility into how ICT products and services are developed, integrated, and deployed—presented an increasing amount of risk to federal agencies.[14] Successful ICT supply chain attacks by threat actors can have a range of impacts. For example, threat actors could take control of federal information systems; decrease the availability of materials or services needed to develop systems; destroy systems, causing injury and loss of life,[15] and compromising national security; or steal intellectual property[16] and sensitive information. As a result, the compromise of an agency's ICT

[13]GAO, *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 *Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements*, GAO-20-299 (Washington, D.C.: Feb. 25, 2020).

[14]GAO, *Cybersecurity: Federal Agencies Need to Implement Recommendations to Manage Supply Chain Risks*, GAO-21-594T (Washington, D.C.: May 25, 2021); *Information Security: Supply Chain Risks Affecting Federal Agencies*, GAO-18-667T (Washington, D.C.: July 12, 2018); *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018); *State Department Telecommunications: Information on Vendors and Cyber-Threat Nations*, GAO-17-688R (Washington, D.C.: July 27, 2017); *Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment*, GAO-13-652T (Washington, D.C.: May 21, 2013); and *IT Supply Chain: National Security-Related Agencies Need to Better Address Risks*, GAO-12-361 (Washington, D.C.: Mar. 23, 2012).

[15]For example, counterfeit batteries can contain volatile chemicals which may explode, counterfeit cabling and other components may lack insulation and melt during use and catch fire, and basic safety components may send dangerous electrical currents from a faulty charger directly into cell phones.

[16]In fiscal year 2018, U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement Homeland Security Investigations seized 213 shipments of computer networking equipment affixed with counterfeit trademarks with a total manufacturer suggested retail price value of nearly $15.5 million. This is a 25 percent increase in the number of seizures of computer networking equipment, and a 112 percent increase in manufacturer suggested retail price value over the previous fiscal year. The networking equipment seized allegedly violated a total of seven trademarks recorded with the Customs and Border Protection and occurred at 21 ports around the country.

supply chain can degrade the confidentiality, integrity, and availability of its critical and sensitive networks, IT-enabled equipment, and data.[17]

Since 2010, we have made more than 3,700 recommendations to agencies aimed at addressing cybersecurity challenges facing the government. While agencies have implemented a majority of our recommendations, many face challenges in safeguarding their information systems and information, in part, because many of these recommendations have not been fully implemented.

In 2018, we reported that the federal government needed to address four major cybersecurity challenges: (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. We continue to report on these challenges and the need to address them. We reiterate the importance of addressing the four major cybersecurity challenges and the 10 associated critical actions in figure 1.

[17]GAO-21-288.

Figure 1: Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges

Establishing a comprehensive cybersecurity strategy and performing effective oversight	Securing federal systems and information	Protecting cyber critical infrastructure	Protecting privacy and sensitive data
1 Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.	5 Improve implementation of government-wide cybersecurity initiatives.	8 Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).	9 Improve federal efforts to protect privacy and sensitive data.
2 Mitigate global supply chain risks (e.g., installation of malicious software or hardware).	6 Address weaknesses in federal agency information security programs.		10 Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.
3 Address cybersecurity workforce management challenges.	7 Enhance the federal response to cyber incidents.		
4 Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).			

Source: GAO analysis; images: peshkov/stock.adobe.com; Gorodenkoff/stock.adobe.com; metamorworks/stock.adobe.com; Monster Ztudio/stock.adobe.com. | GAO-22-104746

Presidential Policy Directive and OMB Guidance Outline the Federal Response to Cybersecurity Incidents

The Presidential Policy Directive (PPD)-41 sets forth principles to govern the federal government's response to cyber incidents (such as those described earlier) to achieve unity of effort and coordination between the public and private sectors.[18] PPD-41 states that federal agencies are to undertake three concurrent lines of effort when responding to any cyber incident:

- **Threat response activities** include conducting appropriate law enforcement and national security investigative activity at the affected entity's site, collecting evidence, and gathering intelligence. These activities also include providing attribution, linking related incidents, identifying additional affected entities, identifying threat pursuit and disruption opportunities, developing and executing courses of action to mitigate the immediate threat, and facilitating information sharing and operational coordination with asset response.
- **Asset response activities** include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents. These activities also include identifying other entities that may be at risk and assessing their risk of the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks. In addition, asset response includes facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize federal resources and capabilities in a timely, effective manner to speed recovery.
- **Intelligence support** and related activities facilitate the building of situational threat awareness and sharing of related intelligence, the integrated analysis of threat trends and events, the identification of knowledge gaps, and the ability to degrade or mitigate adversary threat capabilities.

In addition, when a federal agency is an affected entity, the directive states that the affected agency is to undertake a fourth concurrent line of effort to manage the effects of the cyber incident on its operations, customers, and workforce.

Cyber Unified Coordination Groups

In addition to the efforts that PPD-41 requires of federal agencies individually, it also provides for the formation of a UCG to coordinate a federal response to a significant cyber incident. According to PPD-41, a

[18]The White House, *United States Cyber Incident Coordination*, Presidential Policy Directive/PPD-41 (Washington, D.C.: July 26, 2016).

UCG may be formed and activated in the event of a significant cyber incident, will be incident specific, and will be formed:

- At the direction of the NSC Principals Committee (Secretary level), Deputies Committee (Deputy Secretary level), or the Cyber Response Group; [19]
- When two or more federal agencies that generally participate in the Cyber Response Group, including relevant sector specific agencies, request its formation; or
- When a significant cyber incident affects critical infrastructure owners and operators identified by the Secretary of Homeland Security for which a cyber incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

A UCG is the primary method for coordinating between and among federal agencies responding to a significant cyber incident, as well as for integrating private sector partners into incident response efforts. Further, a UCG is intended to unify the individual efforts of the agencies that comprise the UCG as they focus on their separate responsibilities, namely threat response, asset response, and intelligence gathering and coordination. PPD-41 specifically calls for a UCG to take the following actions.

- Coordinate the cyber incident response related to civilian federal networks, the Department of Defense (DOD) information network, and

[19]Per the annex to PPD-41, the Cyber Response Group is chaired by the Special Assistant to the President and Cybersecurity Coordinator, or an equivalent successor. Federal agencies and departments including relevant cyber centers, shall be invited to participate in the Cyber Response Group, as appropriate, based on given circumstances of a given incident or group of incidents. Participants shall generally include senior representatives from the Central Intelligence Agency, Department of Commerce, Department of Homeland Security and CISA, Department of Defense, Department of Energy, Department of Justice and FBI, Department of State, Department of the Treasury, Federal Communications Commission, Joint Chiefs of Staff, National Cyber Investigation Joint Task Force, NSA, ODNI, and the U.S. Secret Service. The White House, *Federal Government Coordination Architecture for Significant Cyber Incidents*, Annex for Presidential Policy Directive/PPD-41 Annex (Washington, D.C.: July 26, 2016).

the intelligence community networks in a manner consistent with the directive's principles.[20]

- Ensure all appropriate federal agencies, including sector-specific agencies, are incorporated into the incident response.
- Coordinate the development and execution of response and recovery tasks, priorities, and planning efforts, including international and cross-sector outreach, necessary to respond to and recover from an incident.
- Facilitate the rapid and appropriate sharing of information and intelligence among UCG participants on the incident response and recovery activities.
- Coordinate communications regarding the incident to affected parties and stakeholders, including the public as appropriate.
- Form a combined UCG with the lead federal agency or with any UCG established to manage physical effects of the incident when an incident includes cyber and physical effects.
- Protect intelligence and law enforcement investigations, the privacy of individuals, and sensitive private sector information.

Upon dissolution of each UCG, the Chair of the Cyber Response Group is to direct a review of the UCG's response to a significant cyber incident and create a report based on that review within 30 days. Agencies with responsibilities in PPD-41 are to modify plans and procedures based on the results of the Chair of the Cyber Response Group's review of the UCG.

The Cyber Response Group also coordinates the development and implementation of policy and strategy with respect to significant cyber incidents affecting the U.S. or its interests abroad. PPD-41 requires federal agencies, including sector-specific agencies that participate regularly in the Cyber Response Group, to establish and follow enhanced

[20]Per the annex for PPD-41, federal agencies shall respond to significant cyber incidents in accordance with the directive and applicable policies and procedures, and DHS and other federal agencies shall provide support as appropriate for civilian federal networks. The Secretary of Defense shall be responsible for managing the threat and asset response to cyber incidents affecting the DOD information networks, with support from other federal agencies as appropriate. The Director of National Intelligence shall be responsible for managing the threat and asset response for the integrated defense of the intelligence community information environment, in conjunction with intelligence community mission partners and with support from other federal agencies as appropriate.

coordination procedures for situations in which the demands of responding to significant incidents exceed its standing capacity.

OMB's Role in Cyber Incidents

The Federal Information Security Modernization Act (FISMA) of 2014 requires agencies to develop, document, and implement information security programs and have independent evaluations of those programs and practices.[21] It also assigns government-wide responsibilities for information security to OMB, DHS, and the National Institute of Standards and Technology (NIST). FISMA directs OMB to oversee agencies' information security policies and practices. Among other things, FISMA requires OMB to develop and oversee the implementation of policies, principles, standards, and guidelines on information security in federal agencies, except with regard to national security systems. The law also assigns OMB the responsibility of requiring agencies to identify and provide information security protections commensurate with assessments of risk to their information and information systems.

As part of its responsibilities, OMB defines a major incident and provides incident reporting requirements through OMB memorandum M-21-02 Fiscal Year 2020-2021, *Guidance on Federal Information Security and Privacy Management Requirements*.[22] In its memorandum, OMB defines a major incident as either

- Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or the public health and safety of the American people; or
- A breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public

[21]The Federal Information Security Modernization Act of 2014 was enacted as Pub. L. No. 113-283, 128 Stat. 3073 (2014), and amended chapter 35 of Title 44, U.S. Code.

[22]OMB, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*, OMB Memorandum M-21-02 (Washington, D.C.: Nov. 9, 2020).

confidence, civil liberties, or public health and safety of the American people.[23]

Additionally, the memorandum also states that each agency should assess each breach on a case-by-case basis to determine whether the breach meets the definition of a major incident. The memorandum requires a determination of a major incident for any unauthorized modifications, deletions, exfiltration, or access to PII of 100,000 or more people.

Furthermore, OMB instructs agencies to notify Congress in the event of a major incident. Specifically, an agency must notify the appropriate Congressional committees and its Office of Inspector General of a major incident no later than 7 days after the date on which the agency determined that it has a reasonable basis to conclude that a major incident has occurred.[24] In addition, agencies must also supplement their 7 day report to Congress with other pertinent updates and with another report no later than 30 days after the discovery of a breach constituting a major incident.

Threat Actors Exploited Vulnerabilities in SolarWinds Orion and Microsoft Exchange

SolarWinds Orion Compromise

Beginning as early as January 2019, a threat actor breached the computing networks at SolarWinds—a Texas-based network management software company, according to the company's Chief

[23]PII is defined as any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, biometric records, and any other personal information that is linked or linkable to an individual.

[24]FISMA requires notification to the House of Representatives Committees on: (1) Oversight and Government Reform; (2) Homeland Security; and (3) Science, Space, and Technology; and to the Senate Committees on: (1) Homeland Security and Governmental Affairs and (2) Commerce, Science, and Transportation; as well as to the appropriate authorization and appropriations committees. See 44 U.S.C. § 3554(b)(7)(C)(iii)(III).

Executive Officer.[25] The federal government later confirmed the threat actor to be the Russian Foreign Intelligence Service.[26] The threat actor first injected test software code into SolarWinds network management and monitoring suite of products called Orion.

Then, beginning in February 2020, the threat actor injected malicious code into a file that was later included in SolarWinds Orion software updates. The file was included in several software updates affecting multiple versions of Orion and was available for download from late March to early June, and acted as a trojan horse, hiding the threat actor's malicious code.[27] SolarWinds released the software updates to its customers not realizing that the updates were compromised with backdoor access from the threat actor.[28]

After customers installed the malicious software, the threat actor's malicious file stayed dormant for approximately 2 weeks to avoid detection. Following its dormant period, the threat actor's malicious file activated and began to inspect and gather information on affected systems. Some customers who had downloaded and installed the malicious software updates experienced their systems beaconing out, or connecting, to the threat actor's malicious infrastructure where the threat actor collected the gathered customer information, and determined whether to carry out further command and control activities.[29] Additionally,

[25]https://www.rsaconference.com/library/presentation/usa/2021/solarwinds-what-really-happened (accessed Sept. 9, 2021).

[26]https://www.whitehouse.gov/briefing-room/press-briefings/2021/04/15/background-press-call-by-senior-administration-officials-on-russia/ (accessed Oct. 14, 2021).

[27]NIST describes a trojan horse as a computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

[28]GAO, *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)*, (Washington, D.C.: Apr. 22, 2021). https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic (accessed May 5, 2021).

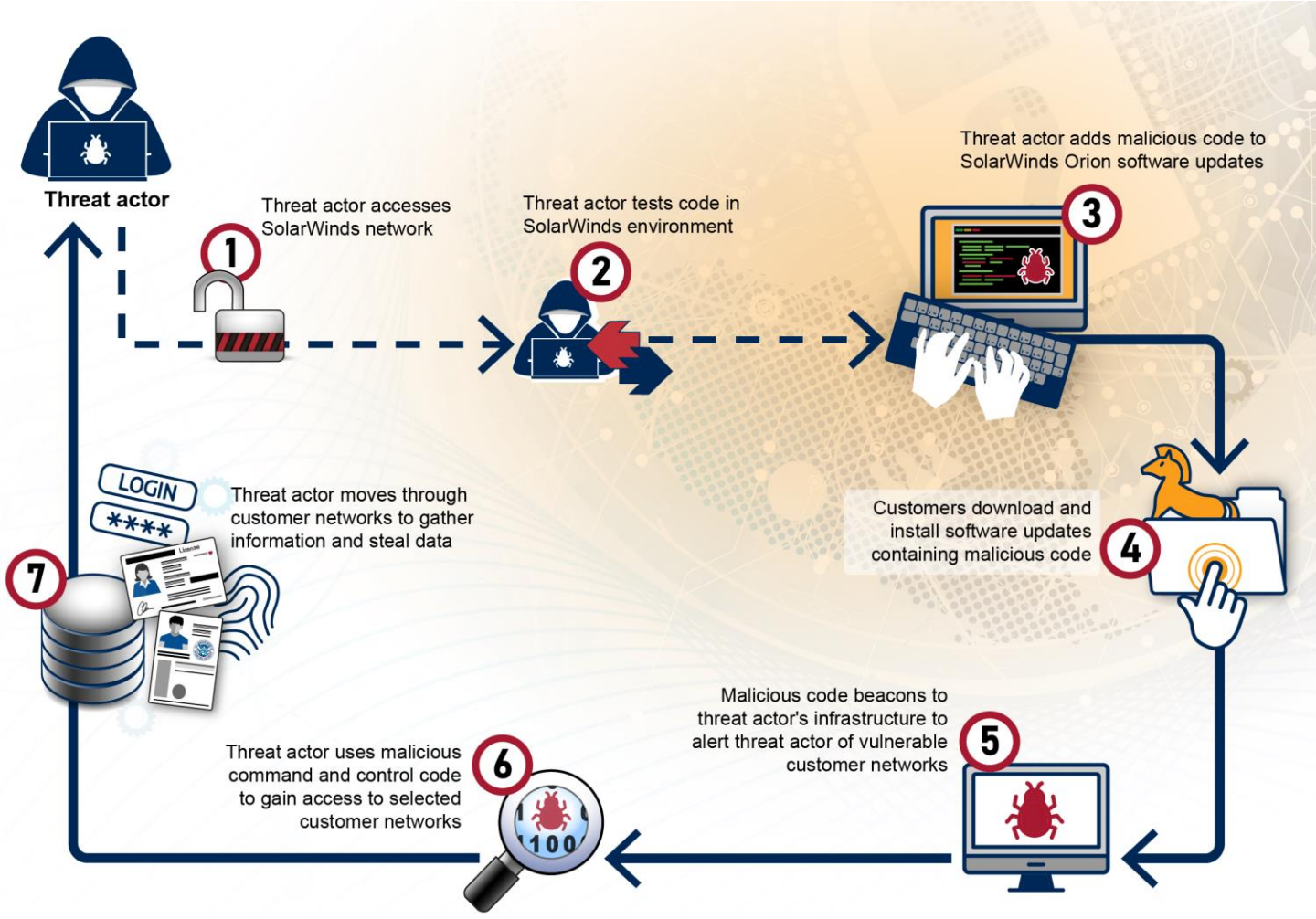
[29]According to the MITRE Corporation, command and control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection. There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses. https://attack.mitre.org/tactics/TA0011/ (accessed Jan. 4, 2022).

the threat actor used the backdoor to send and install additional malware on customer systems that could be used in post-intrusion activities.

A cybersecurity firm initially discovered evidence of this campaign in November 2020 and publicly acknowledged it in December 2020. Federal and private sector entities subsequently identified attempts by the threat actor to gain long-term access through legitimate credentials, accounts, and applications, accessing systems and data for several months before indications of a breach were identified.

Figure 2 depicts an analysis of how the threat actor exploited SolarWinds Orion software.

Figure 2: Analysis of How a Threat Actor Exploited SolarWinds Orion Software



Source: GAO analysis of documentation from publicly released private industry and federal agency reports; images: kras99/stock.adobe.com, anna_leni/stock.adobe.com. | GAO-22-104746

Since SolarWinds was widely used in the federal government to monitor network activity and manage network devices on federal systems, this incident allowed the threat actor to breach and infect several federal agencies' information systems. According to an official from the NSC, nine federal agencies were compromised by this attack. SolarWinds estimated that nearly 18,000 of its worldwide customers could have received a compromised software update. However, SolarWinds further estimated that fewer than 100 customers were actually compromised by

the threat actor. The smaller subset of impacted customers was comprised of high intelligence value customers, including several federal government agencies, exploited for the primary purpose of espionage.

Even though CISA's efforts to work with agencies have provided a degree of confidence that the threat actor is no longer present, the threat actor may have established undiscovered persistent access within affected agencies and private companies' networks. Failure to perform comprehensive and thorough remediation activity will expose those networks and potentially cloud environments to substantial risk for long-term undetected APT activity. Compromised agencies will risk further loss of sensitive data and the erosion of public trust in their networks. In addition, despite the primary purpose of the attack on the federal government being espionage, with the access gained, the threat actor had the ability to carry out far more destructive operations.

Microsoft Exchange Server Vulnerability

While the response and investigation into the SolarWinds breach was still ongoing, Microsoft publicly disclosed another major cybersecurity incident in early March 2021. It had the potential to have serious, widespread impacts to private sector and government systems if not quickly addressed.

According to a Joint Cybersecurity Advisory released by CISA and FBI, Microsoft reported the exploitation or misuse of zero-day vulnerabilities used to gain access to Microsoft Exchange Server versions 2013, 2016, and 2019 that organizations hosted on their premises.[30] Further, the Joint Cybersecurity Advisory stated that the zero-day exploits had been used by threat actors as early as January 2021. According to a White House statement, based on a high degree of confidence, malicious cyber actors affiliated with the People's Republic of China's Ministry of State Security conducted operations utilizing these Microsoft Exchange vulnerabilities.[31]

The vulnerabilities initially allowed threat actors to make authenticated connections to Microsoft Exchange Servers from unauthorized external

[30]CISA and FBI Joint Cybersecurity Advisory, AA21-069A, *Compromise of Microsoft Exchange Server,* (Mar. 10, 2021) and CISA, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities* , Emergency Directive 21-02 (Mar. 3, 2021).

[31]https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/ (accessed July 29, 2021).

sources.[32] Once a connection was successfully made, the threat actor could leverage other vulnerabilities to escalate account privileges and install web shells on the affected server.[33] The web shells allowed the threat actor to remotely access a Microsoft Exchange Server, allowing for persistent malicious operations even after the vulnerabilities were patched.

According to the advisory, after the initial exploitation of the zero-day vulnerabilities, the threat actors could gain persistent and privileged escalation of accounts to access files and mailboxes on the Microsoft Exchange Server as well as potentially pivot to access other systems and networks within that agency. Further, the persistent access could enable the threat actor to steal credentials and information including PII, encrypt data for ransom, and carry out other types of attacks.[34] According to a CISA Emergency Directive, without patching and remediating affected systems, the threat actors could continue to access networks for potential later actions and gain control of an enterprise network.[35]

Figure 3 depicts an analysis of how the threat actors exploited Microsoft Exchange Server vulnerabilities.

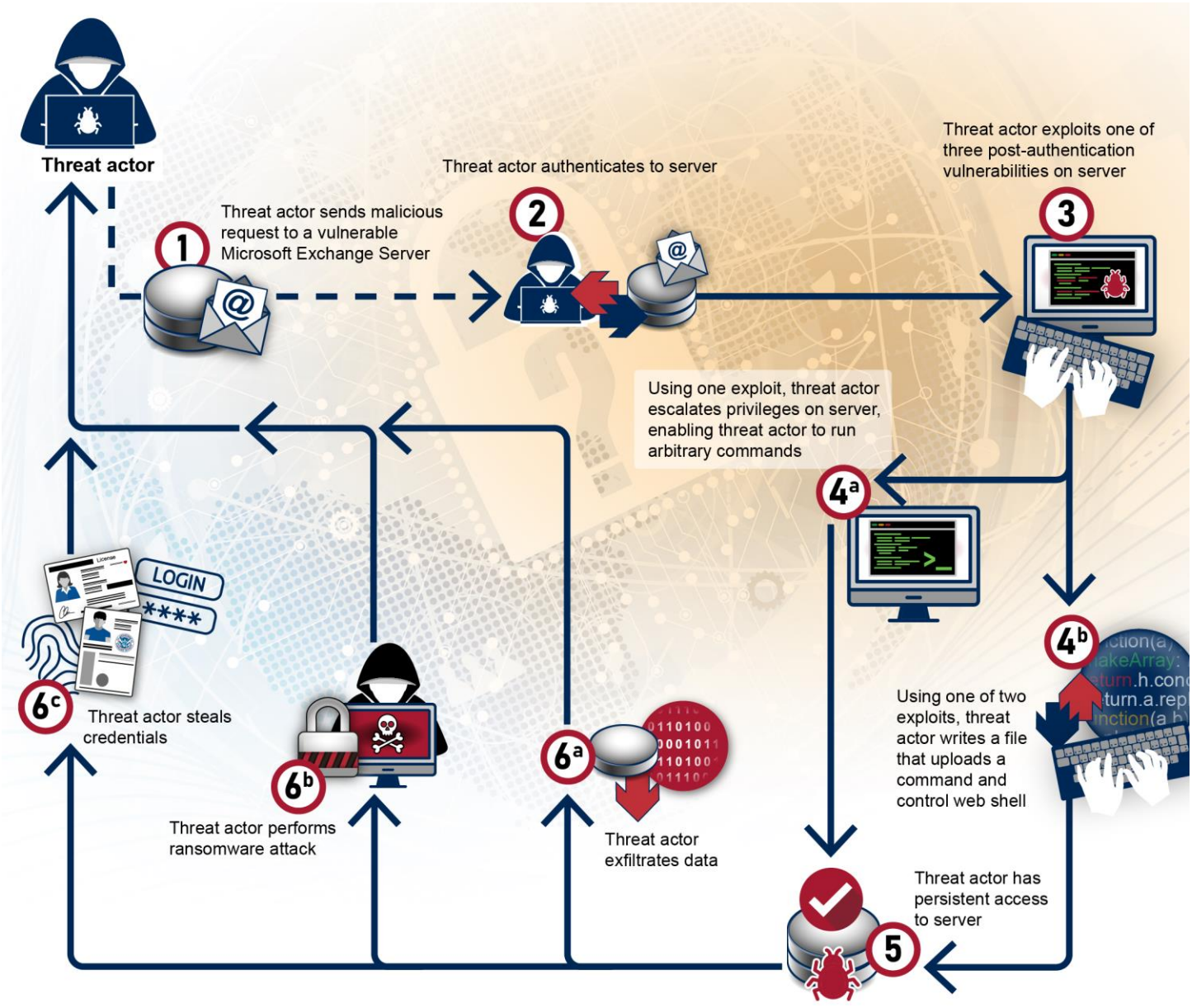
[32]The initial vulnerability allowed a threat actor to send arbitrary HTTP requests to a vulnerable Microsoft Exchange Server and authenticate as the server, making an untrusted connection. This vulnerability served as the initial step in the attack chain. CISA, Alert (AA21-062A), *Mitigate Microsoft Exchange Server Vulnerabilities,* (Mar. 3, 2021).

[33]A web shell is a script that can be maliciously uploaded to a compromised web server to enable remote administration of the machine. Web shells can then be used to upload additional malware or perform other exploits.

[34]CISA, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities,* Emergency Directive 21-02 (Mar. 3, 2021); CISA, Alert, AA21-062A, *Mitigate Microsoft Exchange Server Vulnerabilities* (Mar. 3, 2021); and CISA, FBI. Joint Cybersecurity Advisory, AA21-069A, *Compromise of Microsoft Exchange Server* (Mar. 10, 2021).

[35]CISA, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*, Emergency Directive 21-02 (Mar. 3, 2021).

Figure 3: Analysis of How Threat Actors Exploited Microsoft Exchange Server Vulnerabilities



Source: GAO analysis of documentation from publicly released private industry and federal agency reports; images: kras99/stock.adobe.com, anna_leni/stock.adobe.com. | GAO-22-104746

Federal Agencies Have Been Taking Action in Response to Significant Cyber Incidents

Federal agencies took action to coordinate and respond to the SolarWinds and Microsoft Exchange incidents. For example,

- Two UCGs coordinated the government-wide response to the SolarWinds and Microsoft Exchange incidents, respectively. The UCG efforts included threat and asset response activities, such as issuing directives and guidance, including advisories, alerts, and tools to agencies.
- Federal agencies reported to CISA the actions they took to mitigate the threats introduced by the SolarWinds and Microsoft Exchange incidents as well as additional information regarding network activity and each incident's impact.

The UCGs for both incidents dissolved in April 2021. CISA and certain agencies affected by the incidents have taken steps and continue to work together to respond to the SolarWinds incident. Agencies have completed steps to respond to the Microsoft Exchange incident.

In addition to the actions taken by the UCGs, in May 2021, the President issued Executive Order 14028 that was prompted, in part, by the compromise of the SolarWinds software supply chain.[36] The executive order identifies a broad range of cybersecurity areas in need of improvement across the federal government and addresses, among other things, short and mid-term challenges highlighted by the incident.

Federal Agencies Coordinated Efforts in Response to the SolarWinds and Microsoft Exchange Incidents

Two UCGs coordinated the federal governments' response to the SolarWinds and Microsoft Exchange cybersecurity incidents. Specifically, the NSC and participating agencies announced the formation of a UCG for SolarWinds on December 16, 2020. For the Microsoft Exchange incident, the UCG first met on March 16, 2021. Each UCG consisted of CISA, FBI, and ODNI, with support from the NSA. According to these agencies, the Microsoft Exchange UCG also included participation from several private sector partners in a more robust manner than their involvement in past UCGs. The following describes the agencies and private sector partners' UCG responsibilities:

- The NSC hosted weekly meetings with UCG entities and received daily reports from ODNI.

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

- The FBI was responsible for taking the federal lead in threat response activities. Specifically, the agency was responsible for investigating and gathering intelligence in order to attribute, pursue, and disrupt the responsible threat actor; identifying victims, collecting evidence, and analyzing evidence to determine attribution; sharing relevant information; and investigating results to provide indicators of compromise to network defenders and intelligence to government and private sector partners to enable further actions.[37] According to a Deputy Assistant Director in FBI's Cyber Division, the agency provided direct incident response assistance. For example, FBI's Cyber Action Team, comprised of agency and professional staff employees trained in gathering forensics, were deployed to collect evidence in connection with national security threats of criminal activity for the SolarWinds incident.
- CISA was responsible for acting as a point of contact and federal lead for asset response activities for government, private sector, and international partners. This included providing technical assistance upon request. In addition, the agency facilitated information sharing and operational coordination through its release of numerous alerts, advisories, and tools, including details on indicators of compromise. Further, CISA engaged with public and private stakeholders across relevant critical infrastructure communities to promote dissemination of information and ensure steps were being taken to identify and mitigate compromises.[38]
- ODNI was responsible for taking the federal lead for intelligence support and related activities. In addition, the Director of National Intelligence was responsible for managing threat and asset response for intelligence community networks and systems, with support from other agencies as needed. Further, the agency's role was to provide situational awareness for stakeholders and coordinate intelligence

[37]According to NIST, indicators of compromise are forensic artifacts from intrusions that are identified on organizational systems at the host or network level. These indicators provide valuable information on systems that have been compromised. The rapid distribution and adoption of indicators of compromise can improve information security by reducing the time that systems and organizations are vulnerable to the same exploit or attack.

[38]For a significant cyber incident, OMB, in coordination with lead agencies for threat and asset response, is responsible for providing affected agencies a consolidated, timely written recommendation, caveats, and conditions, to help inform agencies on whether to restart affected civilian federal networks and systems. Further, the Secretary of Homeland Security, in consultation with the Director of OMB, administers the implementation of information security policies and practices, and operates the federal information security incident center.

collection activities to address knowledge gaps and support interagency attribution efforts. According to an official in the ODNI Office of Legislative Affairs, the agency hosted weekly phone conferences with the intelligence community to discuss intelligence updates and planned intelligence community publications.

- NSA provided intelligence, cybersecurity expertise, and actionable guidance to UCG partners, as well as national security systems, DOD, and Defense Industrial Base system owners. Further, NSA engaged with UCG and industry partners to assess the scope and scale of incidents, and provide technical mitigation guidance.
- According to a Senior Technical Director in CISA's Cybersecurity Division, about 10 private sector partners were integrated into the incident response efforts for the Microsoft Exchange incident. According to a White House briefing, private sector partners were to assist with the methodology used to track incidents. Ultimately, they worked with the UCG to modernize cyber defenses and enhance the nation's ability to rapidly respond to significant cyber incidents.[39] An official in ODNI's Cyber Executive Office stated that the private sector partners were able to help identify challenges and roadblocks that needed to be addressed and provide information on the full extent of the incident.

Figure 4 identifies the key entities that comprised the UCGs for the SolarWinds and Microsoft Exchange incidents.

[39]https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/17/statements-by-press-secretary-jen-psaki-deputy-national-security-advisor-for-cyber-anne-neuberger-on-microsoft-exchange-vulnerabilities-ucg/ (accessed Mar. 23, 2021).

Figure 4: Key Entities of the Cyber Unified Coordination Groups for the SolarWinds and Microsoft Exchange Incidents

Source: GAO analysis of agency documentation; images: kras99/stock.adobe.com. | GAO-22-104746

[a]Private sector partners participated in both UCGs. However, private sector partners were integrated as formal partners only for the Microsoft Exchange incident.

The coordination and response from the UCGs and the respective federal agencies included (1) issuing emergency directives and (2) providing guidance through advisories, alerts, and tools.

Issuing emergency directives. Initially, CISA issued emergency directives to federal agencies to inform them about the vulnerabilities and describe what actions to take. For example, in response to the SolarWinds compromise, in December 2020, CISA issued Emergency Directive 21-01, which outlined the required mitigations for federal

agencies to prevent further exploitation of federal information systems resulting from the SolarWinds compromise.[40]

The emergency directive and its supplemental guidance and direction required agencies that had affected SolarWinds Orion versions to perform a number of actions, including to (1) disconnect or power down devices running affected versions of SolarWinds;[41] (2) harden systems, rebuild infrastructure and reset accounts, or upgrade versions of SolarWinds and server operating systems; and (3) follow guidance to fully remove threat actors from affected networks.[42] Agencies were also required to provide periodic status reports to CISA based on a template.

CISA required agencies to submit additional details on the incident and steps they took to remediate the vulnerabilities. For example, CISA required agencies to report whether they detected any unusual network activity, had enough log data to support troubleshooting and threat analysis, and performed forensic analysis of systems.[43]

CISA also issued an emergency directive for the Microsoft Exchange incident. On March 3, 2021, CISA issued Emergency Directive 21-02, which outlined mitigation techniques and required agencies that had certain affected versions of Microsoft Exchange Server to disconnect the affected equipment.[44] The emergency directive and its supplemental

[40]CISA, *Mitigate SolarWinds Orion Code Compromise*, Emergency Directive 21-01 (Dec. 13, 2020).

[41]CISA defines "disconnect" as disconnecting devices from the network and leaving powered on if the agency has the capability to collect forensics images (system memory, host storage, network) off the host or virtual machine, or disconnecting devices from the network and powering off if no such capability exists.

[42]According to NIST, hardening systems is a process intended to eliminate a means of attack by patching vulnerabilities and turning off nonessential services. In addition, hardening includes securely configuring a system to reduce security weaknesses.

[43]According to Appendix A "Required Forensics Investigation Actions" within Emergency Directive 21-01 and its Supplemental Guidance version 3, agencies with affected versions of SolarWinds Orion were to collect and analyze images from system memory, host storage, network, and cloud environments, and hunt for indicators of compromise or other evidence of threat actor activity. Analysis actions also included analyzing new user or service accounts and stored network traffic. CISA, *Mitigate SolarWinds Orion Code Compromise*, Emergency Directive 21-01 (Dec. 13, 2020) and Supplemental Guidance version 3 (Jan. 6, 2021).

[44]CISA, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*, Emergency Directive 21-02 (Mar. 3, 2021) and Supplemental Direction (Mar. 31, 2021).

guidance required agencies that had affected on-premises Microsoft Exchange Server instances to patch and harden their systems or disconnect their servers; forensically triage their networks; and scan for potential threat activity.[45] Agencies were also required to provide periodic status reports based on a template provided by CISA.

The status reports that CISA required agencies to submit requested additional details on the incident and steps taken to remediate the vulnerabilities. For example, the status reports required agencies to report the number of affected servers. Agencies were also required to report on:

- whether the servers were disconnected from the network, updated with the latest software versions, and scanned for potential signs of threat activity;
- the status of firewalls; and
- whether logging was enabled on the servers and was monitored by a Security Operations Center.[46]

This information is required for each affected server.

Providing guidance to federal agencies. To aid organizations in conducting their own investigations and securing their networks, UCG agencies also provided guidance through advisories, alerts, and tools.

For example, DHS, including CISA, the FBI, and NSA released advisories for each incident providing information on the threat actor's cyber tools, targets, techniques, and capabilities. In addition, the advisories listed techniques agencies could use to detect indicators of compromise and various mitigation strategies for vulnerabilities. For instance, CISA and FBI released a Joint Cybersecurity Advisory that described the Chinese cyber threat actor's tactics and techniques used to exploit vulnerabilities

[45]According to Emergency Directive 21-02, forensic triage includes using forensic tools to collect and analyze system memory, event logs, registry hives, and web log artifacts to look for indications of compromise. CISA, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*, Emergency Directive 21-02 (Mar. 3, 2021).

[46]According to NIST, a Security Operations Center defends and monitors an organizations systems and networks on an ongoing basis. A Security Operations Center is also responsible for detecting, analyzing, and responding to cybersecurity incidents in a timely manner.

and gain unauthorized access to networks.[47] The joint advisory also provided information on ways to identify indicators of compromise associated with the Chinese cyber threat actor, along with ways to mitigate and remediate the threats and unauthorized access.

UCG agencies also issued alerts to provide additional information about threat actors and adversary techniques for each incident. For instance, CISA released an alert that provided guidance on mitigating the Microsoft Exchange Server vulnerabilities, identifying indicators of compromise, and tactics, techniques, and procedures associated with the malicious activity.[48] In addition, CISA released multiple cybersecurity alerts associated with the SolarWinds Orion compromise that detailed adversary techniques and provided mitigation guidance for system owners.

In addition to issuing advisories and alerts, UCG agencies provided tools to assist federal agencies with identifying malicious activity on their networks. For example, in December 2020, CISA released a tool called "Sparrow" to be used by incident responders to detect unusual and malicious activity following the compromise of SolarWinds Orion. Further, in March 2021, CISA released the CISA Hunt and Incident Response Program, a software tool that helps agencies find indicators of compromise associated with malicious activity for on-premises systems.

Appendix I provides additional detail on the timelines of steps taken by the UCGs in response to the SolarWinds and Microsoft Exchange incidents.

Agencies Reported on Mitigation Efforts and Severity of the Incidents

In response to CISA's Emergency Directives 21-01 for the SolarWinds incident and 21-02 for the Microsoft Exchange incident, federal agencies reported information to CISA regarding their mitigation efforts. These efforts included reporting on:

[47]CISA and FBI, *Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department*, Alert AA21-200A (July 19, 2021).

[48]CISA, *Mitigate Microsoft Exchange Server Vulnerabilities*, Alert AA21-062A (Mar. 3, 2021).

- anomalous activity identified in their networks,[49]
- whether the agencies had performed forensic analysis on their systems, and
- if the agencies were able to generate and maintain enough telemetry information to understand if the threat actor had compromised the network environments in the past 180 days.[50]

Additionally, per OMB guidance, if agencies determined a major incident occurred, agencies must report the incident to the OMB Office of the Federal Chief Information Officer, CISA, and Congress.

A CISA official reported that the majority of agencies with affected versions of SolarWinds completed the required steps and reported their statuses to CISA. Specifically, based on the self-reported data from the 23 civilian Chief Financial Officers (CFO) Act of 1990 agencies that provided information on Emergency Directive 21-01, agencies reported the following information:[51]

- **Anomalous activity.** Five agencies reported that they had observed anomalous activity on their networks. Four agencies reported they did not have any networks where anomalous activity could have occurred and therefore reported “not applicable” or did not provide a response

[49]CISA defines anomalous activity as including both routine and unexpected events that can compromise security and might require a response to maintain functionality and security. Examples include credential dumping, lateral movement, persistence mechanisms, or other follow on exploitation activity.

[50]CISA defines telemetry information as minimally processed data collected by a capability (e.g., collected by an endpoint detection and response agent).

[51]We requested incident reporting data from major cybersecurity incidents from 23 of the 24 CFO Act agencies. DOD is not required to provide this reporting to CISA, pursuant to these emergency directives.

for observed anomalous activity.[52] The remaining 14 agencies stated that they had not observed anomalous activity.

- **Forensic analysis.** Eighteen agencies reported that they performed forensic analysis on their networks. Five agencies did not provide a response.
- **Telemetry information.** Eleven agencies reported that they had networks where anomalous activity could have occurred (category 2 or category 3 networks) and were able to generate and maintain enough telemetry information to understand actions that had potentially occurred in cloud environments in the past 180 days. One agency stated that it was unable to provide CISA with an answer. Five agencies reported "not applicable" or did not provide a response. Six agencies stated that they were unable to generate and maintain enough telemetry information to effectively determine what actions had occurred on their networks.

Federal agencies also reported on their mitigation efforts in response to the Microsoft Exchange incident as required by CISA's Emergency Directive 21-02. Specifically, a Senior Technical Director from CISA's Cybersecurity Division reported that agencies with affected versions of Microsoft Exchange completed the required steps and reported to CISA the results from their system scans, as required. Additionally, based on the self-reported data from the 23 civilian CFO Act agencies, all agencies performed the forensic triage required by CISA in the initial release of the emergency directive.[53] In addition, all 23 agencies either patched their affected Microsoft Exchange Servers with updates to the zero-day

[52]According to CISA, category 1 networks did not utilize, or never had, affected versions of SolarWinds Orion. Category 2 networks utilize or utilized affected versions of SolarWinds Orion but have forensically demonstrated that, at most, only initial beaconing activity occurred, and the threat actor conducted no follow-on activity. Category 3 networks utilized affected versions of SolarWinds Orion and have evidence of follow-on threat actor activity. Both category 2 and 3 networks would have required agencies to report definitively whether the agencies observed anomalous activity on their networks because they had used affected versions of SolarWinds Orion. However, agencies with category 1 networks were likely to report "not applicable" or did not provide a response for observing anomalous activity on their networks because they never used affected versions of the product.

[53]CISA, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*, Emergency Directive 21-02 (Mar. 3, 2021).

vulnerabilities or disconnected the affected servers from agency networks.[54]

Further, federal agencies provided incident reporting of cybersecurity events to Congress. Five of the 24 CFO Act agencies reported SolarWinds as a major incident per OMB reporting guidance for such incidents.[55] For the remaining 19, two of the 19 agencies stated that they did not declare a major incident because there was no compromise of information or successful exploitation of systems. One of the 19 agencies evaluated its systems for indicators of compromise and determined that a major incident did not occur as defined by OMB. Sixteen of the 19 agencies stated that they did not declare a major incident and did not elaborate further. None of the 24 agencies reported a major incident related to the Microsoft Exchange vulnerabilities.

Several Agencies Have Taken Steps and Are Continuing to Respond to the Incidents

While the Deputy National Security Advisor for Cyber and Emerging Technology reported that the UCGs dissolved by April 19, 2021, after they completed their initial surge efforts, CISA and several affected agencies continue to work together to fully respond to the incidents.[56] In June 2021, CISA reported that there were still response actions to be completed per Emergency Directive 21-01 for several agencies. Specifically, for SolarWinds, CISA was still engaging with agencies that had evidence of follow-on threat actor activity to assist with implementing CISA's supplemental direction for removing the threat actor.[57] As of August 2021, four agencies reported completing pre-eviction guidance

[54]According to Emergency Directive 21-02 and its Supplemental Directive version 2, agencies were to deploy Microsoft updates to all affected Microsoft Exchange Servers. Affected servers that could not be updated within CISA's deadline were to be immediately removed from agency networks. CISA, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*, Emergency Directive 21-02 (Mar. 3, 2021) and Supplemental Direction version 2 (Apr. 13, 2021).

[55]OMB, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*, OMB Memorandum M-21-02 (Washington, D.C.: Nov. 9, 2020).

[56]The annex for PPD-41 states that a Cyber UCG shall dissolve when enhanced coordination procedures for threat and asset response are no longer required or the authorities, capabilities, or resources of more than one federal agency are no longer required to manage the remaining facets of the federal response to an incident.

[57]CISA *Mitigate SolarWinds Orion Code Compromise,* Emergency Directive 21-01 (Dec. 13, 2020) and Supplemental Direction version 4, (Apr. 22, 2021). This supplemental direction provides additional required actions for agencies with networks that used affected versions of SolarWinds Orion and have evidence of follow-on threat actor activity.

and, for relevant networks, had either completed or planned to complete eviction guidance with deviations.[58] In addition, four agencies reported completing pre-eviction guidance only and, based on these reports, were not required per the terms of the supplemental direction to complete subsequent sections. A Senior Technical Director from CISA's Cybersecurity Division stated that CISA was reviewing responses and engaging agencies as necessary to ensure submission and adequate completion of the required actions.

Officials from the NSA, FBI, and ODNI noted that, from their respective roles within the UCG, there were no remaining coordination or response steps to be completed. However, these officials stated that their agencies will continue to look for indicators of compromise or further adversary activity that may be linked to the SolarWinds incident. Lastly, NSA and FBI officials stated that these agencies will continue to pursue foreign intelligence leads that may trace back to the Microsoft Exchange incident.

Recent Executive Order Calls for Additional Federal Actions to Improve Cybersecurity and Incident Response Practices

In May 2021, the President issued Executive Order 14028, *Improving the Nation's Cybersecurity*,[59] that was prompted, in part, by the compromise of the SolarWinds software supply chain.[60] Among other things, the executive order directed the Secretary of Homeland Security, in consultation with the Attorney General, to establish a Cyber Safety Review Board to review and assess the threat activity, vulnerabilities, and mitigation activities of, and agency responses to, significant cyber incidents. The board's initial review is to be focused on the compromise of SolarWinds and is to include recommendations to the Secretary of

[58]Pre-eviction guidance outlines steps for agencies to, among other things, detect and identify the threat actor in affected networks, and define the scope of the intrusion. Eviction guidance outlines steps for agencies to, among other things, isolate affected networks, remove the threat actor from networks, apply mitigations, and rebuild and reimage impacted systems. CISA, Analysis Report AR21-134A, *Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise*, (May 14, 2021).

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

[60]In addition, in April 2021, the President issued Executive Order 14024, *Blocking Property With Respect To Specific Harmful Foreign Activities of the Government of the Russian Federation*. 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. 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).

Homeland Security for improving cybersecurity and incident response practices. The executive order does not provide a timeline for when the board should be established after an incident. As of December 2021, a board had not yet been established. However, DHS was collaborating with federal interagency partners to establish the board and nominate appointees.

The executive order also included a provision for the Secretary of Homeland Security to develop a standard set of operational procedures or playbook to be used in planning and responding to cybersecurity vulnerabilities and incidents. According to an official from CISA's Cybersecurity Division, the agency published the document in November 2021.[61] The document contains two playbooks, one for incident response and one for vulnerability response and provides federal agencies with a set of procedures to identify, coordinate, remediate, recover, and track successful mitigations from incidents and vulnerabilities affecting federal systems, data, and networks. According to the executive order, the Director of OMB shall issue guidance to federal agencies on the use of the playbook.

In addition, to address software supply chain security, the executive order directed, among other things, the Director of NIST to publish guidelines that include criteria to evaluate the security practices of developers and suppliers of software, and guidance that identifies practices that enhance the security of the software supply chain. In July 2021, NIST, in consultation with NSA, issued guidelines on the recommended minimum standards for vendors' testing of their software source code. In accordance with the executive order, the guidelines recommend minimum standards for vendors' testing of their software source code. Further, in July 2021, NIST issued the guidance outlining security measures for critical software use after consulting with CISA and OMB.

To improve the government's investigative and remediation capabilities, the executive order directed OMB, in consultation with DHS, to formulate policies for agencies to establish requirements for logging, log retention, and log management, to ensure centralized access and visibility for each agency. In August 2021, OMB issued a memorandum, *Improving the Federal Government's Investigative and Remediation Capabilities*

[61]https://www.cisa.gov/news/2021/11/16/cisa-releases-incident-and-vulnerability-response-playbooks-strengthen (accessed Nov. 17, 2021).

Related to Cybersecurity Incidents, that establishes a maturity model consisting of four tiers of event logging ranging from "not effective" to "advanced," in which advanced means that logging requirements at all criticality levels are met.[62] The tiers are intended to assist agencies in prioritizing resources to ultimately achieve full compliance. The memorandum establishes requirements for agencies to first assess the maturity of their event logging capabilities and then work toward incremental deadlines for achieving the advanced level.

Further, the executive order addresses the challenges of sharing threat information between the federal government and IT service providers. Service providers often have unique access and insight into cyber threat and incident information on federal information systems. However, contract restrictions may limit the ability of service providers to share threat and incident information with federal agencies, specifically those agencies such as CISA, FBI, and others in the intelligence community responsible for investigating and remediating cyber incidents. The order calls for, among other things, the Secretary of Homeland Security and the Director of OMB to take appropriate steps to ensure to the greatest extent possible that service providers share data with agencies, CISA, and the FBI to assist them in responding to cyber threats and incidents. As of October 2021, an official from CISA's Cybersecurity Division stated that the agency had made recommendations to the Federal Acquisition Regulatory Council to remove contractual barriers to information sharing from federal contractors that included proposed standardized contract language for appropriate cybersecurity requirements. Further, the official noted that CISA created standard operating procedures to share contractors' reported information appropriately among agencies.

[62]OMB, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents,* OMB Memorandum M-21-31 (Washington, D.C.: Aug. 27, 2021).

Federal Agencies Learned Lessons from Efforts Coordinating and Responding to the SolarWinds and Microsoft Exchange Incidents

Our prior work has noted that assessing and documenting lessons learned can help agencies collect and analyze information to determine operational or programmatic changes.[63] Collecting information after an event or at the close of a program allows agencies to identify, for example, positive practices that resulted in desirable outcomes or negative practices that resulted in undesirable outcomes. The agency can analyze the information collected to determine root causes and identify appropriate actions to resolve the issues.

Officials from the NSC, agencies that comprise the UCGs, and several major federal agencies identified lessons from the federal government's coordination and response to the SolarWinds and Microsoft Exchange incidents, which included positive and negative practices in the coordination and response to these incidents.[64] In addition, the NSC, with input from UCG agencies, conducted an after action review of the SolarWinds incident, which may offer solutions to address several of the challenges that agencies identified.

Federal Agencies' Coordination with the Private Sector and Each Other Reportedly Led to Desirable Outcomes

Federal agencies identified several practices that officials believe led to benefits or desirable outcomes in the coordination and response to the SolarWinds and Microsoft Exchange incidents. Specifically, three UCG agency officials stated that coordinating with the private sector led to greater efficiencies in their incident response efforts. For example, they noted that information sharing with the private sector

- allowed the federal government to identify the scale of the SolarWinds incident and respond quickly;
- provided increased visibility on the status of patching and exploitation in the case of the Microsoft Exchange vulnerabilities; and

[63]GAO, *Grants Management: OMB Should Collect and Share Lessons Learned from Use of COVID-19-Related Grant Flexibilities*, GAO-21-318 (Washington, D.C.: Mar. 31, 2021); *DOD Utilities Privatization: Improved Data Collection and Lessons Learned Archive Could Help Reduce Time to Award Contracts*, GAO-20-104 (Washington, D.C.: Apr. 2, 2020); *Project Management: DOE and NNSA Should Improve Their Lessons-Learned Process for Capital Asset Projects*, GAO-19-25 (Washington, D.C.: Dec. 21, 2018); and *Federal Real Property Security: Interagency Security Committee Should Implement A Lessons-Learned Process*, GAO-12-901 (Washington, D.C.: Sept. 10, 2012).

[64]Although all 24 major federal agencies responded to our data request seeking information on responses to and lessons learned collected through after action reports from the incidents, only 12 agencies had completed and provided after action reports at the time of our request.

- provided the opportunity for the federal government to build trust with the private sector, which may lead to increased coordination for future significant cyber incidents.

In addition to coordinating with the private sector, officials from three of the four UCG agencies stated that interagency coordination among the UCG agencies led to positive results during their response to the SolarWinds and Microsoft Exchange incidents. The officials told us that the UCG's role as a centralized forum for interagency communication enhanced the participating agencies' coordination efforts. Specifically, agency officials stated that the regular cadence of meetings was an effective way to share information because the meetings allowed the UCG members to coordinate and streamline information sharing. Initially, the UCGs met daily and then changed the frequency of meetings to a few times a week based on operational needs. Furthermore, an FBI official stated that the UCG's interagency communication allowed the agency to quickly collaborate with other agencies. This enabled the FBI to provide victims in the public and private sectors with security advisories, including technical advisories developed with other federal agencies that assisted in remediating relevant vulnerabilities.

Federal Agencies' Information Sharing Restrictions and Limited Evidence Collection Reportedly Led to Undesirable Outcomes

Federal agencies also identified practices related to information sharing and evidence collection that led to challenges or undesirable outcomes in coordinating and responding to the SolarWinds and Microsoft Exchange incidents. For example, officials from two UCG agencies stated that sharing information among agencies and private sector partners was a challenge and a slow process due to restrictions on sharing information. Specifically, an official from ODNI's Cyber Executive Office told us that information sharing among law enforcement, private sector, and intelligence groups was difficult and time consuming, as there were different classification levels for information. In addition, a Senior Technical Director from CISA's Cybersecurity Division told us that sharing data received from law enforcement with other agencies and the private sector was challenging. Both officials said that it would have been beneficial to have a shared channel (outside of email) to share information among federal agencies, as well as private sector partners. Furthermore, the ODNI official stated that information dissemination should have been an automated process rather than the manual process that was used in responding to these incidents.

Agency officials also told us that the varying levels of data log preservation among agencies and a lack of data collection tools limited evidence collection for the incidents. Although all 24 major agencies did

not provide information on lessons learned from the incidents, eight of the 12 agencies that did stated that the gaps in network and log coverage prevented them from quickly responding to the incidents. In addition, five agencies stated that they were unable to respond to the incidents using their existing tools and needed to acquire new tools or perform configuration changes to respond to either incident. According to agency officials, there were significant gaps in agencies' log data due to differences in how much data is retained and for how long, noting that while some agencies held log data for 90 or 180 days, others maintained no log data. One official further noted that log retention was a particular challenge for investigators responding to the SolarWinds incident as the threat actor was in agencies' networks months before it was detected and evidence may not have existed at all agencies based on an agency's log preservation activities.

Efforts underway may help improve evidence collection. Specifically, OMB's August 2021 memorandum on improving the federal government's investigative and remediation capabilities is intended to improve visibility into cybersecurity incidents through information from logs of federal information systems by requiring agencies to work to achieve advanced data logging requirements.

Further, in August 2021, CISA announced the standup of the Joint Cyber Defense Collaborative. This is a new effort to lead the development of cyber defense operations plans and to execute those plans in coordination with partners from the federal interagency; private sector; and state, local, tribal, and territorial government stakeholders to reduce risk before an incident and to unify defensive actions should an incident occur.[65]

Federal Agencies' Conducted a Review of the SolarWinds Incident to Identify Ways to Improve Coordination and Incident Response

According to an NSC official, the NSC, with input from the UCG agencies, conducted a review of the SolarWinds incident after the UCG dissolved. The official described areas of focus based on this review that may address several of the challenges experienced during the coordination and response of the incident, and may help with preventing and

[65]https://www.cisa.gov/news/2021/08/05/cisa-launches-new-joint-cyber-defense-collaborative (accessed Sept. 22. 2021).

responding to future cybersecurity incidents.[66] The review identified the following areas, among others:

- **Align technology investments with operational priorities.** The review identified that the federal government should invest resources to increase its capabilities to identify, detect, protect, and respond to significant cybersecurity incidents.
- **Improve public-private engagement.** The federal government should improve its coordination and information sharing with the private sector.
- **Improve threat intelligence acquisition, sharing, and use among federal agencies.** The federal government should improve information sharing with its partners.

The NSC official stated that the areas of focus from the review are intended to be a companion to Executive Order 14028 and many of the areas detailed in the review are captured in the executive order for action. Further, while the executive order addresses short and mid-term challenges the areas from the review also identify longer-term challenges. If implemented effectively, the areas from the NSC review and the executive order could help to address several of the challenges identified for both the SolarWinds and Microsoft Exchange incidents.

Agency Comments

We provided a draft of this report to DHS, DOJ, NSA, NSC, ODNI and OMB for comment. DHS, NSA, NSC, ODNI, and OMB provided technical comments orally or via email, which we have incorporated, as appropriate. DOJ told us that it had no comments on the draft report.

We are sending copies of this report to appropriate congressional committees and to the Attorney General, the Directors of National Intelligence and the National Security Agency, Executive Office of the President, Executive Secretary of the National Security Council and the Secretary of Homeland Security. In addition, the report will be available at no charge on GAO's website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov, or Jennifer R.

[66]NSC acknowledged documenting lessons learned in an after action review. However, the content of that review is considered limited official use only and therefore we could not disclose its contents in full detail in our publicly available report. As an alternative, we interviewed key contributors to the document and sought from them relevant lessons learned information not considered sensitive.

Franks at (404) 679-1831 or franksj@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 major contributions to this report are listed in appendix II.

Nick Marinos
Managing Director, Information Technology and Cybersecurity

Jennifer R. Franks
Director, Information Technology and Cybersecurity

List of Addressees

The Honorable James M. Inhofe
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Ron Wyden
Chairman
Committee on Finance
United States Senate

The Honorable Gary C. Peters
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Mark R. Warner
Chairman
The Honorable Marco Rubio
Vice Chairman
Select Committee on Intelligence
United States Senate

The Honorable Mike Rounds
Ranking Member
Subcommittee on Cybersecurity
Committee on Armed Services
United States Senate

The Honorable Cynthia Lummis
Ranking Member
Subcommittee on Space and Science
Committee on Commerce, Science, and Transportation
United States Senate

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

The Honorable Carolyn B. Maloney
Chairwoman
Committee on Oversight and Reform
House of Representatives

The Honorable Eddie Bernice Johnson
Chairwoman
The Honorable Frank D. Lucas
Ranking Member
Committee on Science, Space, and Technology
House of Representatives

The Honorable Adam Schiff
Chairman
Permanent Select Committee on Intelligence
House of Representatives

The Honorable Jim Langevin
Chairman
The Honorable Jim Banks
Ranking Member
Subcommittee on Cyber, Innovative Technologies, and Information Systems
Committee on Armed Services
House of Representatives

The Honorable Ruben Gallego
Chairman
The Honorable Trent Kelly
Ranking Member
Subcommittee on Intelligence and Special Operations
Committee on Armed Services
House of Representatives

The Honorable Yvette D. Clarke
Chairwoman
Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation
Committee on Homeland Security
House of Representatives

The Honorable Haley Stevens
Chairwoman
The Honorable Michael Waltz
Ranking Member
Subcommittee on Research and Technology
Committee on Science, Space, and Technology
House of Representatives

The Honorable Elise Stefanik
House of Representatives

Appendix I: Detailed Timelines of Steps Taken by Cyber Unified Coordination Group Agencies in Response to the SolarWinds and Microsoft Exchange Incidents

The following tables provide detailed timelines of the steps taken by the Cyber Unified Coordination Group agencies—Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA), Department of Justice's Federal Bureau of Investigation (FBI), and Office of the Director of National Intelligence (ODNI)—with support from the National Security Agency (NSA)—in response to the SolarWinds and Microsoft Exchange incidents. The steps taken by these agencies include a variety of activities such as issuing initial and supplemental technical directives and providing guidance through advisories, alerts, and tools.

Table 1: Detailed Timeline of Steps Taken by Cyber Unified Coordination Group Agencies in Response to the SolarWinds Incident

Date	Step taken
December 13, 2020	Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 21-01, *Mitigate SolarWinds Orion Code Compromise*, which outlined required mitigations for federal agencies to prevent further exploitation of federal information systems resulting from the SolarWinds compromise.
December 16, 2020	CISA, Federal Bureau of Investigation (FBI), and the Office of the Director of National Intelligence (ODNI) released a joint statement announcing the formation of a Cyber Unified Coordination Group (UCG) to coordinate a government-wide response to the SolarWinds incident.
December 17, 2020	CISA released Alert AA20-352A, which provided information on the advanced persistent threat (APT) that compromised some SolarWinds supply chain products. (Last updated April 15, 2021.)
December 17, 2020	National Security Agency (NSA) released an advisory that provided guidance on techniques used to detect and protect against follow-on threat activity from the SolarWinds compromise, leading to the abuse of authentication mechanisms to access cloud resources.
December 18, 2020	CISA issued the first Emergency Directive 21-01 Supplemental Guidance, which included additional information on affected versions of SolarWinds, guidance for affected agencies using third-party service providers, and clarity on required actions.
December 21, 2020	FBI, in coordination with the UCG, released a Private Industry Notification, *Advanced Persistent Threat Actors Leverage SolarWinds Vulnerabilities*, which provided information to cyber security professionals and system administrators to help determine whether advanced persistent threat actors exploited SolarWinds vulnerabilities on their systems.
December 23, 2020	CISA released *CISA Insights* "What Every Leader Needs to Know About the Ongoing APT Cyber Activity" to provide background information on the ongoing APT cyber activity that compromised SolarWinds Orion software supply chain. *CISA Insights* are informed by intelligence and real-world events and provide background information on particular cyber or physical threats to the nation's critical infrastructure, as well as a ready-made set of mitigation activities that nonfederal partners can implement.
December 24, 2020	CISA released "Sparrow," a tool to detect unusual and malicious activity in Azure/Microsoft Office 365 environments. This tool is intended to be used by incident responders to focus on recent tactics, techniques, and procedures used by the recent attacks.
December 30, 2020	CISA issued the second Emergency Directive 21-01 Supplemental Guidance, which included additional guidance on minimum versions of SolarWinds software that could be used by agencies.
January 5, 2021	CISA, FBI, NSA, and ODNI released a joint statement with updates on the SolarWinds incident. The UCG stated that the APT is likely Russian in origin and is responsible for the incident.

Date	Step taken
January 6, 2021	CISA issued the third Emergency Directive 21-01 Supplemental Guidance, which updated the list of affected versions and outlined additional hardening and forensic analysis requirements, conditions for operating SolarWinds, guidance for affected agencies using third-party service providers, and agency reporting requirements.
January 8, 2021	CISA released Alert AA21-008A. The alert describes the tactics, techniques, and procedures the APT actor uses and offers an overview of, and guidance on, available open-source tools—including a CISA-developed tool, Sparrow—for network defenders to analyze their Microsoft Azure Active Directory, Office 365, and M365 environments to detect potentially malicious activity.
February 8, 2021	CISA released Malware Analysis Report AR21-039A. This report provides a detailed analysis of the SUNBURST malware associated with SolarWinds compromise.
February 8, 2021	CISA released Malware Analysis Report AR21-039B. This report provides a detailed analysis of the TEARDROP malware associated with SolarWinds compromise.
March 9, 2021	CISA released guidance on remediating networks affected by the SolarWinds and Active Directory/M365 compromise to provide actionable guidance to organizations affected by this APT activity.
March 9, 2021	CISA released *CISA Insights* “Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise: Risk Decisions for Leaders” providing actions to perform for organizations with affected versions of SolarWinds Orion and evidence follow-on threat actor activity.
March 18, 2021	CISA released CISA Hunt and Incident Response Program tool to find indicators of compromise associated with the SolarWinds and Active Directory/M365 compromise in an on-premises enterprise environment.
March 18, 2021	CISA released Alert AA21-077A with the release of the CISA Hunt and Incident Response Program. CISA described the technical details of the tool and how to run it to detect post-compromise threat activity.
April 8, 2021	CISA released the Aviary dashboard to assist organizations visualize and analyze outputs when using the Sparrow tool.
April 15, 2021	CISA, FBI, and NSA released a joint advisory describing the threat activities associated with the Russian Foreign Intelligence Service. The group stated that the Russian Foreign Intelligence Service compromised SolarWinds Orion software updates, and has exploited other vulnerabilities to gain unauthorized access to networks.
April 15, 2021	CISA and the Cyber National Mission Force of U.S. Cyber Command released Malware Analysis Report AR21-105A to provide detailed analysis of several malicious samples and artifacts associated with the supply chain compromise of SolarWinds Orion network management software.
April 22, 2021	CISA issued the fourth Emergency Directive 21-01 Supplemental Direction, which provides additional required actions for agencies with networks that used affected versions of SolarWinds Orion and have evidence of follow-on threat actor activity.
April 26, 2021	DHS and FBI released a joint advisory AA21-116A, describing the techniques the Russian Foreign Intelligence Service used in its cyberattacks as well as recommendations to prevent and mitigate these threats.
May 7, 2021	CISA, FBI, NSA, and United Kingdom’s National Cyber Security Centre released joint advisory on Russian Foreign Intelligence Service activity and additional tactics, techniques, procedures, and other details of follow-on activity after the initial SolarWinds Orion software compromise.
May 14, 2021	CISA released Analysis Report AR21-134A. This report describes the full process CISA recommends to evict the potential APT. This guidance contains pre-eviction tasks, tasks to evict the actor, and post-eviction steps to document actions taken and return to normal operation. This guidance contains the most up to date information and all agencies that have evidence of follow-on threat actor activity must complete the eviction by July 16, 2021, or within 90 days of discovery.

Source: GAO analysis of agency documentation. | GAO-22-104746.

Table 2: Detailed Timeline of Steps Taken by Cyber Unified Coordination Group Agencies in Response to the Microsoft Exchange Incident

Date	Step taken
March 3, 2021	The Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 21-02, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*, which outlined mitigation techniques for those agencies that had affected on-premises Microsoft Exchange Server instances.
March 3, 2021	CISA issued Alert AA21-062A, Mitigate Microsoft Exchange Server Vulnerabilities, and seven Malware Analysis Reports, which provided further guidance on mitigating the vulnerabilities, identifying indicators of compromise, and tactics, techniques, and procedures associated with the malicious activity.
March 10, 2021	CISA and Federal Bureau of Investigation (FBI) released a Joint Cybersecurity Advisory AA21-069A, Compromise of Microsoft Exchange Server. The joint advisory provided additional guidance on the associated tactics, techniques, and procedures associated with the malicious activity, as well as the techniques agencies could use to detect indicators of compromise and various mitigation strategies for vulnerabilities.
March 13, 2021	CISA added seven additional malware analysis reports to Alert AA21-062A, related to the web shell associated with the exploitation of vulnerabilities in compromised Microsoft Exchange server products.
March 31, 2021	CISA issued the first Emergency Directive 21-02 Supplemental Direction, which outlined digital forensics triage and server hardening requirements, as well as reporting requirements for those agencies that have on-premises Microsoft Exchange Server products.
April 9, 2021	The Department of Justice obtained a warrant to remove web shells from U.S.-based victim servers that had been compromised pursuant to the Microsoft Exchange Server software vulnerability.
April 12, 2021	CISA released two additional malware analysis reports, related to Alert AA21-062A, on the ransomware and web shells associated with the Microsoft Exchange Server compromise.
April 13, 2021	CISA issued the second Emergency Directive 21-02 Supplemental Direction, which included additional requirements for updating Microsoft Exchange servers.
July 19, 2021	CISA and FBI released advisory AA21-200A, which discussed the overserved tactics, techniques, and procedures associated with the Chinese threat actors attributed to the Microsoft Exchange incident.
July 19, 2021	CISA, FBI, and National Security Agency released advisory AA21-200B, which provided information on the tactics, techniques, and procedures used by the Chinese threat actors associated with the Microsoft Exchange incident.

Source: GAO analysis of agency documentation. | GAO-22-104746.

Note: A web shell is a script that can be maliciously uploaded to a compromised web server to enable remote administration of the machine. Web shells can then be used to upload additional malware or perform other exploits.

Appendix II: GAO Contacts and Staff Acknowledgments

GAO Contacts

Nick Marinos, (202) 512-9342 or marinosn@gao.gov
Jennifer R. Franks, (404) 679-1831 or franksj@gao.gov

Staff Acknowledgments

In addition to the contact named above, Edward Alexander, Jr. and Josh Leiling (Assistant Directors), Season Burris (Analyst in Charge), Jake Backer, Chris Businsky, Vijay D'Souza, Linda Erickson, Rebecca Eyler, Camille Garcia, Keith Kim, Katherine Noble, Scott Pettis, and Umesh Thakkar made key contributions to this report.