United States Government Accountability Office

Report to Congressional Addressees

September 2021

COVID-19

Selected Agencies Overcame Technology Challenges to Support Telework but Need to Fully Assess Security Controls

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

GAO-21-583

GAO@100 Highlights

Highlights of GAO-21-583, a report to congressional addressees

September 2021

COVID-19

Selected Agencies Overcame Technology Challenges to Support Telework but Need to Fully Assess Security Controls

Why GAO Did This Study

In response to the onset of the COVID-19 pandemic, in March 2020 the Office of Management and Budget directed federal agencies to maximize their use of telework to enable the workforce to remain safe while ensuring that government operations continue. Telework is essential to continuity of operations but also brings added cybersecurity risks.

The *CARES Act* contains a provision for GAO to monitor the federal response to the pandemic. GAO was also asked to examine federal agencies' preparedness to support expanded telework. GAO's objectives were to determine (1) selected agencies' initial experiences in providing the IT needed to support remote access for maximum telework and (2) the extent to which selected agencies followed federal information security guidance for their IT systems that provide remote access.

GAO selected 12 agencies for review that varied in their percentages of reported employee telework use and sent a questionnaire to solicit these agencies' perspectives on the use of IT in transitioning to maximum telework. GAO also reviewed the selected agencies' information security documentation and interviewed relevant officials.

What GAO Recommends

GAO is making a total of nine recommendations to six agencies to document and assess relevant controls, and to fully document remedial actions for systems supporting remote access. The agencies agreed with the recommendations.

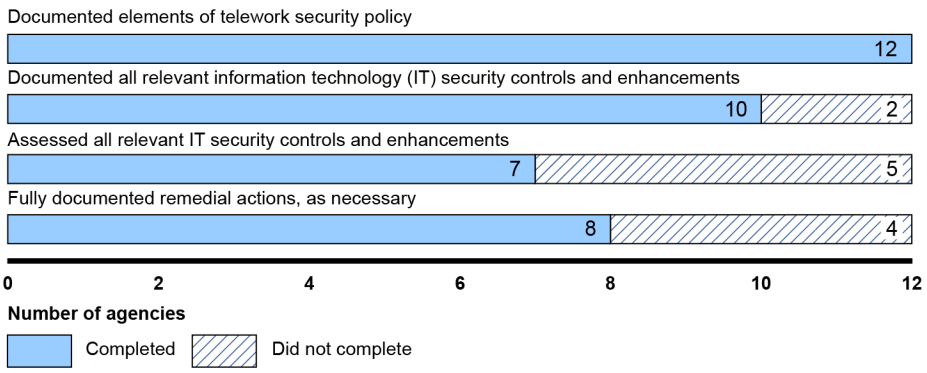
View GAO-21-583. For more information, contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov.

What GAO Found

Each of the 12 agencies GAO selected for review had information technology (IT) in place to support remote access for telework during the COVID-19 pandemic. Although the agencies initially experienced IT challenges in supporting remote access for maximum telework, they generally overcame them. For example, seven agencies were challenged in providing sufficient bandwidth to provide remote access for teleworkers, but they increased bandwidth as needed to ensure networks could handle additional remote connections. In addition, while the increased number of remote connections brings additional cybersecurity risks, all of the selected agencies reported that they continued activities intended to help ensure the security of their information and systems.

While the selected agencies had documented elements of a telework security policy, such as permitted telework devices and forms of remote access, not all agencies had fully addressed other relevant federal guidance for securing their systems that support remote access for telework (see figure). Specifically, two agencies had not fully documented relevant IT security controls to protect those systems. In addition, assessments for systems that five agencies relied upon for remote access did not address all relevant controls to ensure the controls were operating effectively. Further, four selected agencies had not fully documented remedial actions to mitigate weaknesses they had previously identified.

Extent to Which 12 Selected Agencies Followed Federal Information Security Guidance in Implementing Their IT Systems That Support Remote Access for Telework



Source: GAO analysis of agency IT security documentation. | GAO-21-583

Although one of the selected agencies subsequently resolved its shortcomings, others had not. For the agencies that did not fully follow federal information security guidance, agency IT security officials stated that these conditions existed for various reasons, such as out-of-date documentation, among others. If agencies do not sufficiently document relevant security controls, assess the controls, and fully document remedial actions for weaknesses identified in security controls, they are at increased risk that vulnerabilities in their systems that provide remote access could be exploited.

Contents

Table

Figures

Abbreviations

the Act	*Telework Enhancement Act of 2010*
BYOD	bring your own device
COVID-19	Coronavirus Disease 2019
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DOJ	Department of Justice
DOT	Department of Transportation
FBI	Federal Bureau of Investigation
FISMA	*Federal Information Security Modernization Act of 2014*
GFE	government-furnished equipment
Interior	Department of the Interior
IT	information technology
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PIV	personal identity verification
POA&M	plan of action and milestones
SEC	Securities and Exchange Commission
SP	Special Publication
SSA	Social Security Administration
VPN	virtual private network

GAO@100 U.S. GOVERNMENT ACCOUNTABILITY OFFICE
A Century of Non-Partisan Fact-Based Work

441 G St. N.W.
Washington, DC 20548

September 30, 2021

Congressional Addressees

The Coronavirus Disease 2019 (COVID-19) pandemic has resulted in a catastrophic loss of life and generated unprecedented challenges for federal agencies that must continue to carry out their missions while also ensuring that their employees are able to perform their work safely and effectively. Telework—an arrangement that allows employees to perform their work at an approved alternative worksite—can be used by agencies to accomplish their missions during periods of disruption, such as during this pandemic. In March 2020, federal agencies moved rapidly to maximize their use of telework.

To support telework, agencies rely on various technologies that provide remote access to agency networks over the internet. While these technologies have allowed agencies to continue their operations during the pandemic, remote access also brings additional cybersecurity risk to agencies' information and systems. Concerned with the risk to cybersecurity across federal government systems, we initially designated information security as a government-wide high-risk area in 1997—a designation it retains today.[1]

The *CARES Act*[2] includes a provision for GAO to report on its ongoing monitoring and oversight efforts related to the COVID-19 pandemic.[3] In addition, the chair of the Senate Subcommittee on Emerging Threats and Spending Oversight of the Committee on Homeland Security and Governmental Affairs, and the chairman of the House Committee on Homeland Security requested that we examine the federal government's

[1]See GAO, *High-Risk Series: An Overview*, GAO-HR-97-1 (Washington, D.C.: February 1997); *High-Risk Series: Information Management and Technology*, GAO-HR-97-9 (Washington, D.C.: February 1997) and *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: March 2, 2021). In 2003, we expanded this area to include computerized systems supporting the nation's critical infrastructure and, in 2015, we further expanded this area to include protecting the privacy of personally identifiable information.

[2]*CARES Act*, Pub. L. No. 116-136, § 19010, 134 Stat. 281, 579-581 (2020).

[3]We regularly issue government-wide reports on the federal response to COVID-19. For the latest report, see GAO, *COVID-19: Continued Attention Needed to Enhance Federal Preparedness, Response, Service Delivery, and Program Integrity*, GAO-21-551 (Washington, D.C.: July 19, 2021). Our next government-wide report will be issued in October 2021 and will be available on GAO's website at https://www.gao.gov/coronavirus.

preparedness to support maximum telework in response to the pandemic and whether federal agencies had maintained cybersecurity during the expansion of telework. Our specific objectives for this report were to determine (1) selected agencies' initial experiences in providing the information technology (IT) needed to support remote access for maximum telework in response to the COVID-19 pandemic and (2) the extent to which the selected agencies followed federal information security guidance for their IT systems that provide remote access to support telework.

In conducting this work, we first selected a non-probability sample of federal agencies to review. To do so, we initially identified the 28 agencies that perform national essential functions or primary mission-essential functions, as defined by Presidential Policy Directive 40, Annex A.[4] For each of the 28 agencies, we reviewed telework data from fiscal year 2018, as published by the Office of Personnel Management (OPM) in its annual *Status of Telework in the Federal Government* report to Congress for fiscal year 2018.[5]

Based on the data available in the OPM telework report, we reviewed telework data for a total of 66 agencies, which included subcomponents of the initial 28 agencies. We removed from our analysis those agencies with fewer than 1,000 employees and those with less than 20 percent of employees eligible to telework.[6] We then split the remaining agencies into

[4]The White House, *National Continuity Policy*, Presidential Policy Directive 40 (Washington, D.C.: July 2016). Annex A of this policy directive assigns executive departments and agencies to one of four categories commensurate with their continuity of operations responsibilities during a catastrophic emergency. These categories are intended to be used for continuity planning, communications and information services requirements, emergency operations capabilities, and other related requirements. Agencies identified as Category I perform "national essential functions," which are those functions necessary to lead and sustain the nation during a catastrophic emergency. Agencies identified as Category II are agencies that are not Category I, but perform "primary mission-essential functions" that support national essential functions. We removed the Central Intelligence Agency and the Office of the Director of National Intelligence from this list due to concerns about the classified nature of data at those entities.

[5]Office of Personnel Management, *Status of Telework in the Federal Government*, Report to Congress Fiscal Year 2018 (Washington, D.C.: March 2020). At the time of our agency selection, the data from fiscal year 2018 were the most recent available.

[6]We removed agencies with fewer than 1,000 employees and with less than 20 percent of employees eligible to telework because agencies with such a small number of employees eligible to telework are likely to have missions that do not facilitate the use of telework.

three tiers, to include (1) those with a small number of employees, (2) those with a medium number of employees, and (3) those with a large number of employees.[7]

Within each tier, we arranged the agencies based on the percentage of eligible employees that teleworked in fiscal year 2018 at each agency. Our final selection included the two agencies from each tier with the smallest percentage of eligible employees who teleworked and the two agencies from each tier with the largest percentage of eligible employees who teleworked.[8] We selected agencies in this manner because we wanted to perform our review at agencies with both small and large telework operations before the pandemic.

Applying these criteria, we selected the following 12 agencies for our review:

- Food and Nutrition Service at the U.S. Department of Agriculture
- Bureau of Indian Affairs and National Park Service at the Department of the Interior (Interior)
- Federal Highway Administration at the Department of Transportation (DOT)
- Federal Law Enforcement Training Centers and U.S. Secret Service at the Department of Homeland Security (DHS)
- Securities and Exchange Commission (SEC)
- Social Security Administration (SSA)
- Internal Revenue Service at the Department of the Treasury
- OPM
- Executive Office for Immigration Review and Federal Bureau of Investigation (FBI) at the Department of Justice (DOJ)

[7]The small tier contained agencies with 1,000–4,000 employees; the medium tier contained agencies with 4,001–14,000 employees; and the large tier contained agencies with more than 14,000 employees. We chose these ranges because they appeared to be a natural breakdown in the size of the agencies in our selection.

[8]In three cases, we removed agencies from our list based on conversations that we conducted with agency inspectors general. These conversations provided insight into the nature of agency telework environments that we determined made them unsuitable for our review.

To address the first objective, we conducted a survey of IT subject matter experts, including operations and security officials, at each of the 12 agencies selected for our review (see appendix I for a list of the survey questions).[9] We developed and administered a questionnaire, and received responses from all 12 agencies. The questionnaire asked about a number of topics, including the agency's telework environment, IT support available for teleworkers, and changes in agency remote access infrastructure due to the expansion of telework in response to the pandemic. It also included a list of several potential IT challenges that agencies may have faced during the transition to maximum telework, and asked them to indicate the extent to which they experienced these challenges.

In addition, we interviewed IT officials from each of the 12 agencies to ask additional questions and clarify questionnaire responses.[10] The experiences reflected the views of only those agencies that participated in our survey and interviews and, therefore, are not generalizable to federal agencies as a whole. We also held interviews with agency union representatives to ask questions about employees' experiences with IT during maximum telework.[11]

To address our second objective, we requested and reviewed IT security documentation associated with the systems that provide remote access to

[9]Six of the agencies in our review relied on department-level resources to provide remote access to their employees during the transition to maximum telework. In the following instances, we solicited responses from both agency and department IT officials: the Bureau of Indian Affairs and National Park Service relied on the Department of Interior for remote access for their employees; the Federal Law Enforcement Training Centers relied on the Department of Homeland Security; the Executive Office for Immigration Review relied on the Department of Justice; Food and Nutrition Service relied on the Department of Agriculture; and the Federal Highway Administration relied on the Department of Transportation.

[10]As mentioned previously, we solicited responses from both agency and department IT officials as necessary.

[11]We conducted interviews with union representatives from seven of the 12 selected agencies. During these interviews, we asked questions regarding employees' experiences during maximum telework from an IT perspective to gain insight into experiences beyond those of agency officials. Officials from the Federal Bureau of Investigation, Federal Highway Administration, and U.S. Secret Service told us that their employees were not members of a union. In addition, a union representative from the Bureau of Indian Affairs declined to comment, and a union representative from the Federal Law Enforcement Training Centers did not respond to our interview request.

support telework for the 12 selected agencies.[12] Documentation included telework security policies, system security plans, results of relevant security control assessments for the systems, and remedial action plans, as appropriate. We reviewed the documentation to determine whether agencies had addressed guidance published by the National Institute of Standards and Technology (NIST).[13] In addition, we interviewed agency IT operations and IT security officials.

During our review of the documentation, we focused on relevant security controls and enhancements cited by NIST as being of particular importance to protecting IT systems that provide remote access to support telework. The controls covered topics such as account management, remote access, identification and authentication of users, and backup of agency information. Appendix II provides more details on our objectives, scope, and methodology.

We conducted this performance audit from April 2020 to September 2021 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

In response to the onset of the COVID-19 pandemic, on March 17, 2020, the Office of Management and Budget (OMB) directed agencies to maximize their telework options for employees to enable the workforce to remain safe while ensuring that government operations continue during the pandemic.[14] In addition, OMB stated that agencies were to extend

[12]Because six of the agencies in our review relied on department-level resources to provide remote access to their employees, we reviewed documentation associated with both agencies and departments, as necessary.

[13]Guidance included, for example: National Institute of Standards and Technology, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, Special Publication 800-46 revision 2 (Gaithersburg, MD: July 2016), and National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53 revision 4 (Gaithersburg, MD: January 2015). NIST released revision 5 of Special Publication 800-53 in September 2020; however, revision 4 was in effect at the time of our review.

[14]Office of Management and Budget, *Federal Agency Operational Alignment to Slow the Spread of Coronavirus COVID-19*, M-20-16 (Washington, D.C.: March 17, 2020).

telework flexibilities to contractors whenever feasible and noted that the government was to immediately adjust operations and services to minimize face-to-face interactions.

Federal Law Requires Agencies to Develop Telework Policies

Since 1990, telework has received significant attention in Congress and in the executive branch. In October 2000, Congress and the President enacted the *Department of Transportation and Related Agencies Appropriations, 2001*, which contained a mandate requiring each executive agency[15] to establish a policy to permit eligible employees to telework to the maximum extent possible without affecting performance.[16]

Additionally, the *Telework Enhancement Act of 2010* (the Act) further requires each executive agency to notify employees of their eligibility to telework and establish telework participation goals to help measure and report results, among other things.[17] We have previously reported on federal telework programs, including key practices for ensuring the success of agencies' telework programs, the reliability of agency-reported data, the extent to which agencies have implemented telework as a tool for continuity and emergency planning, and the information available on costs and benefits of telework programs.[18]

Agencies Use Various Remote Access Technologies to Support Telework

On March 22, 2020, OMB issued a memo that directed federal agencies to use technology to the greatest extent practicable to support mission

[15]Executive agencies are defined in 5 U.S.C. § 105 as an executive department, a government corporation, and an independent establishment.

[16]Pub. L. No. 106-346, § 359, 114 Stat. 1356, 1356A-36 (2000).

[17]Pub. L. No. 111-292, 124 Stat. 3165 (Dec. 9, 2010), codified primarily at chapter 65 of title 5 of the United States Code.

[18]See GAO, *Federal Telework: Key Practices That Can Help Ensure the Success of Telework Programs*, GAO-21-238T (Washington, D.C.: November 18, 2020); *Federal Telework: Additional Controls Could Strengthen Telework Program Compliance and Data Reporting*, GAO-17-247 (Washington, D.C.: February 17, 2017); *Federal Telework: Better Guidance Could Help Agencies Calculate Benefits and Costs*, GAO-16-551 (Washington, D.C.: July 15, 2016); *Federal Telework: Program Measurement Continues to Confront Data Reliability Issues*, GAO-12-519 (Washington, D.C.: Apr. 19, 2012); *Emergency Preparedness: Agencies Need Coordinated Guidance on Incorporating Telework into Emergency and Continuity Planning*, GAO-11-628 (Washington, D.C.: July 22, 2011); and *Human Capital: Telework Programs Need Clear Goals and Reliable Data*, GAO-08-261T (Washington, D.C.: Nov. 6, 2007).

continuity during the nation's COVID-19 emergency response efforts.[19] According to NIST, agencies can do so by, among other things, leveraging one or more methods to provide teleworkers with remote access to an agency's computing resources. These methods include tunneling, application portals, remote desktop access, and direct application access. Table 1 describes each of these methods.

Table 1: Remote Access Methods Agencies Can Leverage to Provide Teleworkers with Access to Computing Resources

Tunneling	Tunneling offers an encrypted communications tunnel through which information can be securely transmitted between networks, including public networks such as the internet. A virtual private network (VPN) is a common tunneling technology that establishes an encrypted connection between a teleworker's device and the agency's network, providing the teleworker with secure access to many of the agency's computing resources.
Application portal	An application portal is a server that offers access to one or more applications through a single centralized interface. For example, a web-based portal provides a user with access to multiple applications from a single website. Another type of portal solution, called a virtual desktop infrastructure, involves the user connecting to a system that contains virtual images of standardized, non-simulated operating systems and desktops.
Remote desktop access	Remote desktop access gives a teleworker the ability to remotely control a particular workstation at the agency (most often the user's own computer at the agency's office) from a teleworker's client device, such as a laptop computer. The teleworker interacts with the remote computer and is able to access all of the applications, data, and other resources that are normally available from their agency's workstation.
Direct application access	Remote access can be accomplished without using remote access software. A teleworker can access an individual application directly, with the application providing its own security. One of the most common examples of direct application access is webmail.

Source: National Institute of Standards and Technology Special Publication 800-46. I GAO-21-583

Remote Access Comes with Increased Cybersecurity Risks

The IT systems supporting federal agencies are highly complex and dynamic, technologically diverse, and geographically dispersed. Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intentions who can intrude into those systems and use their access to obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks. While telework is an important option during the COVID-19 pandemic, the large number of additional remote connections needed to allow agencies to maintain maximum telework capabilities brings more risks to agency networks and systems.

Remote access technologies, including employee telework devices (e.g., laptop computers and other devices), often need additional protection due

[19]Office of Management and Budget, *Harnessing Technology to Support Mission Continuity*, M-20-19 (Washington, D.C.: March 2020).

to higher exposure to external threats compared to technologies located inside an agency's network boundary. In its memo directing agencies to use technology to support mission continuity during the pandemic, OMB also provided a list of areas of increased focus concerning cybersecurity and privacy.[20]

In April 2020, the Congressional Research Service reported that the increase in telework in response to the COVID-19 pandemic had increased cybersecurity risks for agencies.[21] Specifically, it reported that adversaries were, for example, using phishing attempts to try and take advantage of the pandemic to entice and trick users into downloading malicious software onto their devices.[22] Further, the increase in remote users brings additional risks, as remote users are no longer accessing agency computing resources from inside agency facilities.

Federal Agencies Provided Guidance to Address Cyber Risks

To help address the cybersecurity risks associated with remote access to agency systems, the Act requires OMB to coordinate with DHS and NIST to issue guidelines to ensure the adequacy of information and security protections for information and information systems used by employees while teleworking. In response to the Act, OMB issued security guidelines, which stated that agencies must continue to follow OMB policies and NIST standards and guidelines.[23] The OMB guidelines also referred to NIST publications and resources to assist in the protection of remote devices. In addition to OMB's reference to NIST guidance, several agencies provided additional guidance.

In addition to the security guidelines OMB provided as a result of the Act, in its March 22, 2020 memo, the agency provided additional guidance to agencies. The memo stated that agencies should, among other things,

- ensure that virtual private network (VPN) components, network infrastructure devices, and other devices used to enable remote work

[20]OMB, M-20-19.

[21]Congressional Research Service, *Federal Telework During the COVID-19 Pandemic: Cybersecurity Issues in Brief*, R46310 (Washington, D.C.: April 10, 2020).

[22]Phishing is a digital form of social engineering that uses authentic-looking, but fake, emails to request information from users or direct them to a fake website that requests information.

[23]Office of Management and Budget, *Implementing the Telework Enhancement Act of 2010: Security Guidelines*, M-11-27 (Washington, D.C.: July 15, 2011).

are updated with the latest software patches and security configurations;

- provide guidance to employees on applying appropriate information security and privacy controls when working from alternate locations or from home;
- continue to prohibit employees from forwarding federal government materials or information to personal devices; and
- continue to prohibit the unauthorized use of social media or any unauthorized devices for government business.

NIST Special Publication (SP) 800-53 revision 4 provides guidance to federal agencies on identifying the security and privacy controls needed to manage risk to their information and information systems.[24] To help agencies and information system users address cybersecurity challenges presented by teleworking and remote access, NIST issued two complementary publications on telework security. One publication[25] makes recommendations to federal agencies for securing a variety of remote access and bring your own device (BYOD) technologies.[26] The publication also recommends that agencies develop a telework security policy and identifies the security controls from NIST SP 800-53 that are most pertinent for securing enterprise telework, remote access, and BYOD technologies. The second publication provides recommendations to users for securing BYOD technologies used for remote access, as well as those directly attached to the enterprise's own networks.[27]

In response to the COVID-19 pandemic, the NIST Information Technology Laboratory issued new bulletins providing guidance to

[24]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53 revision 4 (Gaithersburg, MD: January 2015). NIST released revision 5 of this publication in September 2020; however, revision 4 was in effect at the time of our review.

[25]National Institute of Standards and Technology, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, Special Publication 800-46 revision 2 (Gaithersburg, MD: July 2016).

[26]"Bring Your Own Device" refers to a situation in which an agency allows an employee to use his or her own personal device (e.g., a personal laptop computer) to perform work-related tasks.

[27]National Institute of Standards and Technology, *User's Guide to Telework and Bring Your Own Device (BYOD) Security*, Special Publication 800-114 revision 1 (Gaithersburg, MD: July 2016).

agencies on remote access. One bulletin highlighted specific recommendations from its publication on securing agencies' remote access technologies. A second bulletin provided recommendations for securing files exchanged over the internet.[28]

DHS's Cybersecurity and Infrastructure Security Agency (CISA) provides a variety of telework security guidance for both federal agencies and non-federal organizations and for employees working remotely. For example, it has provided guidance for implementing strong authentication, securing web applications against cybersecurity threats, and avoiding social engineering[29] and phishing attacks. Other guidance has also highlighted cybersecurity principles and practices that individuals and agencies can follow to employ video conferencing tools (i.e., collaboration tools) more securely.[30]

In response to the pandemic, CISA issued additional guidance to agencies using telework. For example, one alert issued in March 2020 provided recommendations that agencies can implement to secure their VPN against cyber threats. The alert also recommended that agencies take steps to ensure that VPN connections are able to accommodate increased remote connections occurring as a result of increased telework.[31]

The National Security Agency (NSA) has also published several guides on telework and network security topics, including, among others, securing mobile devices, home networks, and web browsers against cyber threats; safely using social media; configuring VPNs securely; and

[28]National Institute of Standards and Technology Information Technology Laboratory, *Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions* (Gaithersburg, MD: March 2020) and *Security Considerations for Exchanging Files Over the Internet* (Gaithersburg, MD: August 2020).

[29]An attack using personal information to build trust with a user in order to gain unauthorized access to sensitive information, systems, and networks or to engage in identity fraud, among other things.

[30]Resources on telework security from the Cybersecurity and Infrastructure Security Agency can be found at https://www.cisa.gov/telework.

[31]Cybersecurity and Infrastructure Security Agency, *Enterprise VPN Security*, Alert AA20-073A, accessed March 13, 2020, https://www.us-cert.gov/ncas/alerts/aa20-073a.

evaluating security features for collaboration tools.[32] For example, in November 2020, NSA issued guidance outlining security features to consider when selecting a collaboration tool, such as a video meeting application, and steps to take to use the services securely. The guidance also included a list for comparing the security features of 17 commercial collaboration tools.[33]

Further, in response to the pandemic, NSA and CISA jointly developed a best practices guide for telework. This guide is intended to help federal teleworkers protect federal information and information systems from cybersecurity threats while working remotely.[34]

Selected Agencies Supported Remote Access and Overcame IT Challenges during Maximum Telework

The 12 agencies selected for review reported that they had IT in place to allow employees to remotely access agency resources during the pandemic. As they transitioned to maximum telework, the agencies reported that they experienced IT challenges, which they generally overcame. Further, the selected agencies were able to continue activities intended to help ensure the cybersecurity of their information systems during maximum telework.

Selected Agencies Had Technology in Place to Support Remote Access during the Pandemic

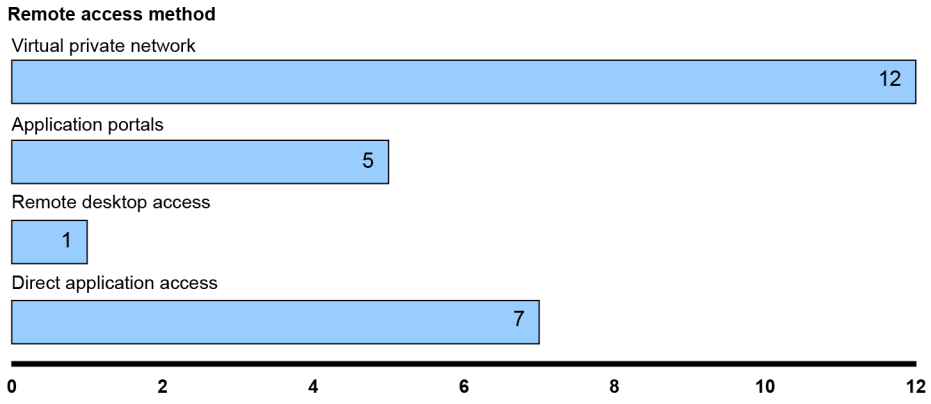
Each of the selected agencies reported that they had technology in place to support employees' remote access to agency resources during the pandemic. For example, all of the agencies used a VPN, and some also used other technologies, such as application portals, remote desktop access, and direct application access to enable employees to connect remotely to agency resources. The extent of the selected agencies' uses of these various technologies to achieve remote access for telework is shown in figure 1.

[32]National Security Agency, *Telework and Mobile Security Guidance*, accessed March 29, 2021, https://www.nsa.gov/What-We-Do/Cybersecurity/Telework-and-Mobile-Security-Guidance/.

[33]National Security Agency, *Selecting and Safely Using Collaboration Services for Telework–UPDATE* (Fort Meade, MD: November 2020).

[34]National Security Agency and Cybersecurity and Infrastructure Security Agency, *Telework Best Practices*, April 29, 2020; available at https://www.nsa.gov/What-We-Do/Cybersecurity/Telework-and-Mobile-Security-Guidance/ and https://www.cisa.gov/publication/telework-best-practices.

Figure 1: Remote Access Technologies Used by 12 Selected Agencies during the Pandemic to Support Telework



Source: GAO analysis of agency survey results. | GAO-21-583

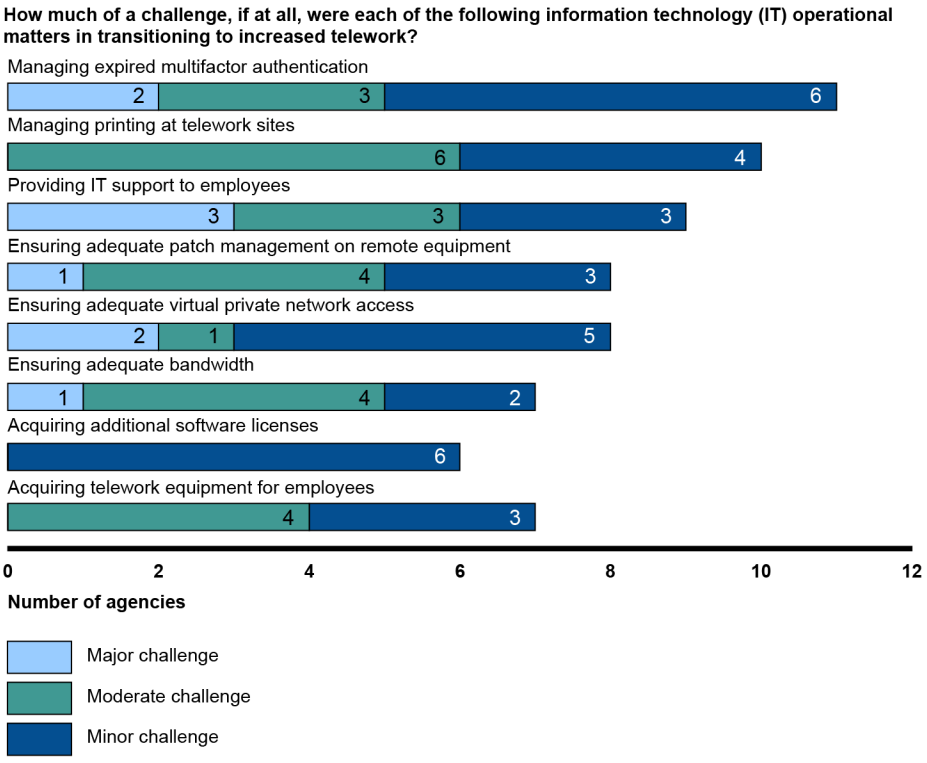
Further, six of the 12 selected agencies reported that they allowed their employees to use personally owned devices (e.g., employees' personal laptops) during telework, and all 12 agencies had established methods to enable their employees to log in to agency systems and services remotely. To do so, they enabled employees to use personal identity verification (PIV) or other methods, such as a secure token.[35]

[35]Department of Homeland Security, *Policy for a Common Identification Standard for Federal Employees and Contractors,* Homeland Security Presidential Directive 12 (HSPD-12) (Washington, D.C.: August 2004*).* This directive mandates a federal standard for secure and reliable forms of identification, including for rapid electronic authentication, which includes a personal identity verification card. A secure token is a physical object a user possesses and controls that is used to authenticate a user's identity, such as a hardware device that can generate information that the verifier knows can only come from that device.

Selected Agencies Faced, but Generally Overcame, IT Challenges Associated with the Transition to Maximum Telework

All of the agencies in our review reported that they had experienced challenges in ensuring that their IT would support the transition to maximum telework. At least half of the agencies reported experiencing some degree of (i.e., major, moderate, or minor) challenge in eight areas while implementing maximum telework. These challenges ranged from managing expired multifactor authentication to acquiring equipment. Further details on the challenges are provided in figure 2 and in the discussion that follows the figure.

Figure 2: Extent of IT Challenges Identified by Selected Agencies in Implementing Maximum Telework



Source: GAO analysis of agency survey data. | GAO-21-583

Managing expired multifactor authentication

Multifactor authentication credentials, such as PIV cards, are required for employees to log in to agency systems and services, including for remote access. In the event that an employees' PIV card expires, the agency has

to either come up with an alternative solution for employee log in, or provide an updated PIV card to the employee.

Officials from 11 agencies told us that they experienced challenges regarding the expiration of multifactor authentication credentials, such as PIV cards, in a maximum telework environment. Officials from the 11 agencies told us that they had alleviated the problems with card expiration. For example, five of those agencies created temporary credentials, such as a combination of username and password, for employees to use in the event that they could not physically obtain a new card. In addition, three of those agencies allowed employees to perform a temporary online renewal of the PIV credential to enable the employee to continue to use the card without going into the office for renewal.

Managing printing at telework sites

Employees may be accustomed to having access to printers or, in some cases, may need to print documents in order to perform their jobs. Officials from 10 of the selected agencies identified the need for employees to print documents at their telework sites as a challenge in a maximum telework environment.

However, officials from eight of those 10 agencies told us that their agencies had overcome the challenge.[36] One of the agencies decided to disallow wireless printing, but to allow employees to print using a wired connection, because allowing remote users to print over a home wireless network can expose an agency's systems to security threats. In addition, five of the 10 agencies chose to not allow employees to print from home in most cases. For example, one of those five agencies was concerned that additional IT help desk support would be required to assist employees in managing the process of connecting their printers at home.

Providing IT support to employees

IT support services, including help desks, are critical for helping employees access computer systems and software, providing technical support for software applications and computer equipment, and troubleshooting and identifying software, hardware, network, or telecommunications problems experienced by end users, among other

[36]The two additional agencies did not provide descriptions of the challenge associated with managing printing at telework sites, and therefore did not tell us whether or not they had overcome the challenge.

things. Officials from nine of the selected agencies told us that they experienced challenges in providing IT support to all of their employees during the transition to maximum telework. For example, officials from one of the nine agencies told us that their agency was challenged by an initial spike in support requests as employees who were not familiar with teleworking attempted to connect using the agency's VPN for the first time.

Officials from six of the nine agencies stated that they had overcome the challenges associated with providing IT support for teleworkers.[37] For example, officials from three of those six agencies told us that they had expanded IT support by either adding more support staff or extending IT help desk hours available to employees. However, union representatives from two of those six agencies told us that timely resolution of IT support issues was still a problem for employees at least 7 months after the expansion to maximum telework.

Ensuring adequate patch management on remote equipment

Patch management is an important element in mitigating the risks associated with known vulnerabilities. When vulnerabilities are discovered, the software vendor may release an update, called a patch, to mitigate the risk. Unless the patch is applied in a timely manner, an attacker may exploit a vulnerability that is not yet mitigated, enabling unauthorized access to information systems or enabling users to have access to greater privileges than authorized.

Officials from eight of the selected agencies told us that certain aspects of ensuring that government-furnished equipment (GFE) were sufficiently patched became more difficult in an expanded telework environment with a large number of employees working from home offices instead of agency offices. For example, officials told us that it was difficult to maintain adequate patches on GFE because patches are easiest to apply overnight when employees are not using their laptops. However, during maximum telework, employees at home did not always maintain remote connections on their laptops to the agency's network at the end of the work day. In these instances, the agency would have a smaller window of opportunity for agency IT staff to patch the laptops remotely.

[37]Officials from the other three agencies did not comment on whether the challenge associated with IT support services had decreased or not.

Officials from the eight agencies stated that IT security staff generally were able to work around the patching challenge. For example, to ensure that GFE could be kept up to date with needed patches, officials from four agencies told us that IT staff communicated in advance with employees to ensure that laptops remained remotely connected to agency networks at the end of the work day. An official from another agency told us that, upon first connecting to the VPN in the morning, users would be prompted to install any necessary updates either at lunchtime or the end of the work day.

Overcoming infrastructure limitations with VPN access, bandwidth, and software licenses

Due to the increase in employees accessing agency services remotely when they transitioned to maximum telework, officials from 11 of the selected agencies told us that they experienced challenges concerning the infrastructure comprising their systems that provide remote access to employees, including VPN access, bandwidth, and software licenses. For example:

- VPNs are important components of remote access because they provide for secure connections between remote devices and an agency's information systems. Eight agencies' officials stated that they experienced challenges in ensuring adequate VPN service to support maximum telework. They added that they upgraded or expanded this service in order to enable employees to securely connect to agency resources. Specifically, agencies had to add additional infrastructure or obtain additional VPN licenses for use by employees.
- Agencies need sufficient bandwidth to ensure quality performance as their employees access agency networks remotely. Officials from seven agencies told us that they experienced challenges in ensuring adequate bandwidth to support increased traffic on their networks. The agencies reported that they monitored the bandwidth and increased it as necessary in order to ensure that their networks could handle the additional teleworkers.
- Agencies require software licenses to enable employees to use externally acquired software on laptop computers or elsewhere in the telework environment. Officials from six agencies told us that they had been challenged to ensure that they had an adequate number of software licenses to support the increased number of teleworkers. For example, the agencies had to add or expand the number of software

licenses, such as licenses for software that enables IT help desk staff to interact remotely with employees' laptop computers.

Acquiring telework equipment for employees

Not all agencies allow employees to use personally owned devices (e.g., personal laptops) when teleworking and, instead, provide them with GFE, including laptops and peripherals, such as headsets. As a result of increased telework, nine selected agencies said they had to acquire additional GFE for employees.

Officials from seven of the selected agencies reported that they experienced challenges in procuring additional telework equipment for employees. For example, officials from five of the seven agencies told us that they experienced delays in acquiring GFE to be used by employees during maximum telework. Specifically, officials at three of those agencies told us that they experienced delays of between 2 weeks and 1 month in procuring additional GFE; officials from two other agencies reported that they experienced delays of more than 1 month in procuring the additional equipment. Officials from three of the five agencies told us that problems with acquiring GFE had subsided over time.

Agency officials told us that the delay in GFE acquisitions were due to high demand across government and the private sector for equipment to be used by teleworkers. A union representative from one of the selected agencies told us that employees could not access email without GFE, and that employees without it had to use weather and safety leave[38] until they obtained needed equipment.

Five of the Selected Agencies Reported an Increase in Cyberattacks and All Continued Cybersecurity Activities

Officials from five of the selected agencies told us that they experienced an increase in certain types of cyberattacks during maximum telework. For example, officials from four of the five agencies stated that they saw an increase in phishing attacks.

Notwithstanding these reported increases in cyberattacks, all of the agencies in our review stated that they had continued activities intended to help ensure the security of their information and systems, as they had done prior to maximum telework. For example, officials from 10 of the selected agencies told us that their security operations centers were

[38]Agencies may grant weather and safety leave due to a condition that prevents the employee or group of employees from safely traveling to, or performing work at, an approved location.

operating remotely and could do the majority of their tasks remotely. As such, the security operations centers' activities and operational capacity had not changed due to the transition to maximum telework. In addition, several agencies reduced cybersecurity risk by increasing employee awareness. For example, officials from seven of the selected agencies told us that they had provided additional security guidance to employees as the number of teleworkers increased.

Selected Agencies Generally Followed Federal Information Security Guidance, but Gaps Remained

NIST has issued federal information security guidance that recommends that agencies develop a telework security policy. NIST also recommends that agencies document IT security controls and enhancements relevant to securing their systems that support telework; assess the controls and enhancements; and document risk associated with, and remedial actions for, controls and enhancements assessed to be other than satisfactory.

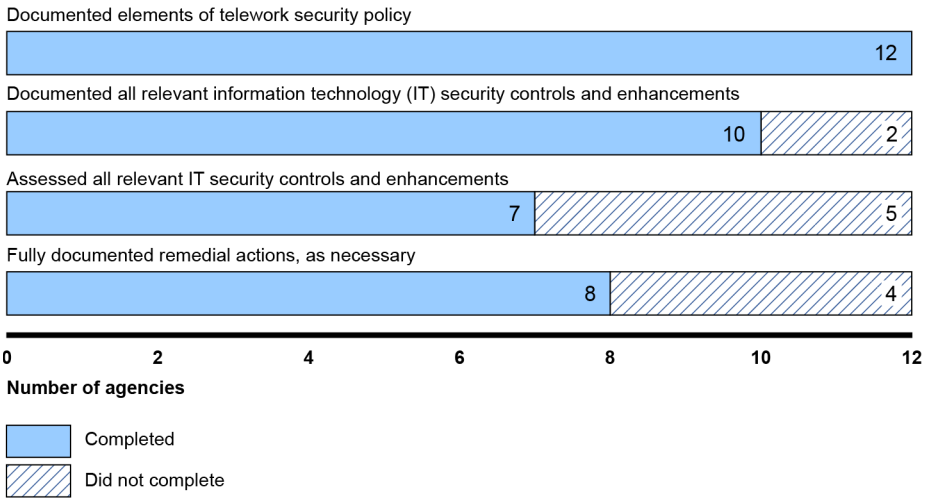
The selected agencies generally followed federal information security guidance for their IT that supports remote access for telework.[39] For example, these agencies documented elements of a telework security policy. The agencies also had, except in limited cases:

- documented IT security controls and enhancements relevant to securing their systems that support telework,
- assessed the controls and enhancements, and
- documented any risks associated with, and remedial actions for, controls and enhancements assessed to be other than satisfactory.

Figure 3 provides a summary of the extent to which the agencies had followed information security guidance for their IT that provides remote access for telework.

[39]Our evaluation consisted of an assessment of documentation provided to us by the selected agencies to determine the extent to which they had documented the required elements of a telework security policy, documented IT controls and enhancements relevant to securing their systems that support telework, assessed the controls and enhancements, and documented any risks associated with, and remedial actions for, controls and enhancements assessed to be other than satisfactory. We did not perform any on-site or technical testing of security controls to determine whether agencies had or had not implemented controls effectively.

Figure 3: Extent to Which Selected Agencies Followed Federal Information Security Guidance for Their IT that Supports Remote Access for Telework



Source: GAO analysis of agency IT security documentation. | GAO-21-583

All Selected Agencies Documented Elements of a Telework Security Policy

NIST SP 800-46, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* recommends that agencies create telework security policies. According to NIST, an agency's telework security policy should define, among other things:

- the forms of remote access the agency permits,
- the types of telework devices that are permitted to use each form of remote access, and
- how user account provisioning should be handled.

Only one agency in our review had created a specific telework security policy document. However, each of the 12 selected agencies had documented these elements of a telework security policy in various sources, including telework policies, remote access policies, and system security plans.

Most Selected Agencies Had Documented and Assessed Controls and Documented Remedial Actions, but Gaps Remained

NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, identifies security controls and enhancements that are to be used by agencies to protect their systems and recommends that agencies describe them in system security documentation.[40] Specifically, it outlines the basic controls that agencies should implement based on the documented impact a system has on agency operations, as determined in NIST Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.[41] Further, NIST SP 800-46 identifies relevant controls from NIST SP 800-53 that are especially important for securing systems that support remote access for telework.[42]

Ten of the selected agencies had documented in system security plans, all relevant security controls and enhancements for protecting their systems that provide remote access to support telework. Among others, these agencies had documented controls related to account management, remote access, access control for mobile devices, use of external information systems, internal system connections, information

[40]NIST SP 800-53. According to NIST, control enhancements either add functionality or specificity to a base control or increase the strength of a base control. Control enhancements are used in systems and environments of operation that require greater protection than the protection provided by the base control.

[41]National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication 199 (Gaithersburg, MD: February 2004). This publication establishes security categories for both information and information systems based on the potential impact on an agency if certain events occur that jeopardize the information and information systems needed by the agency to accomplish its assigned mission. The potential impacts are defined as low, moderate, and high. The information systems we reviewed at the 12 selected agencies were all at the moderate- or high-impact level, as determined by agency officials.

[42]NIST SP 800-46 includes 12 controls that it deems to be of particular importance for remote access security. Further, NIST SP 800-53 includes a set of IT security controls and enhancements that are important for securing moderate- and high-impact systems. We determined the IT security control and enhancements relevant to our review through a combination of the two NIST documents and agency impact determination as described. In total, there are 34 relevant controls and enhancements for systems determined to be at the moderate-impact level, and 46 relevant controls and enhancements for systems determined to be at the high-impact level. The controls cover topic areas such as account management, remote access, access control for mobile devices, use of external information systems, internal system connections, information system backup, identification and authentication (agency users), device identification and authentication, risk assessment, boundary protection, and transmission confidentiality and integrity.

system backup, identification and authentication, risk assessment, boundary protection, and transmission confidentiality and integrity.

However, two other agencies' system security plans did not include all relevant controls or enhancements. Specifically:

- Although SEC documented most of the relevant security controls and enhancements in the security plan documents for its system that provided remote access, in four instances, the agency did not document all relevant controls. Specifically, as of May 2021, the agency had not documented one security control and two security control enhancements; in addition, it had incorrectly described another security control enhancement. SEC IT security officials told us that they were in the middle of a regular assessment cycle for the components associated with this system and, therefore, had not made adjustments to documentation, as applicable, based on the results of the assessment.
- SSA did not document all relevant security controls and enhancements in the system security plan for its system that provided remote access. For example, as of May 2021, the agency had not documented about half of the relevant controls and enhancements in the plan. SSA IT security officials told us that the agency was reorganizing the components that make up the system that provided remote access to the agency's employees, and that, due to the reorganization, they had not updated the system security plan since 2016. SSA asserted, however, that the controls and enhancements were in place. Nevertheless, the agency had not documented the controls in an updated system security plan.

Until SEC and SSA consistently document the controls and enhancements relevant to protecting their systems that provide remote access to support telework, these agencies are at increased risk that cybersecurity officials will not have the necessary information to make credible, risk-based decisions regarding their information systems.

Five Selected Agencies Relied on Systems for Remote Access That Had Not Been Fully Assessed

The *Federal Information Security Modernization Act of 2014* (FISMA) requires that agencies periodically test the effectiveness of information security controls.[43] Similarly, NIST SP 800-53 recommends that an agency assess the controls in a system and its environment of operation to determine the extent to which the controls have been implemented

[43]*Federal Information Security Modernization Act of 2014*, Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014).

correctly, are operating as intended, and are producing the desired outcome with respect to meeting established security and privacy requirements.

Although seven of the selected agencies had documented that they assessed all of the relevant security controls and enhancements for protecting their systems that provided remote access to support telework, four of the systems that provided remote access for five selected agencies had not been fully assessed. Specifically:

- The Federal Highway Administration relies on DOT to provide a remote access solution to employees. However, DOT had not assessed one of the relevant security control enhancements as of January 2021. Department officials told us that the team responsible for their controls assessment had overlooked the enhancement during their review. As of February 2021, the department had created a remedial action plan to track the enhancement and ensure that it includes the enhancement in its next assessment. However, until DOT assesses the remaining control enhancement, it will be at increased risk that the enhancement is not working as intended.
- In 2020, SEC assessed the relevant controls and enhancements for a subset of components associated with its system that supports telework. For the remaining components, although SEC had documented assessments in prior years, the documentation was not detailed enough to demonstrate whether all relevant controls had been assessed. For example, the agency did not link assessment results to specific controls in its assessment documentation. The agency has plans to assess the controls and enhancements for the components again in calendar years 2021 and 2022. Until the agency completes these assessments and associates the results to specific relevant controls, it lacks assurance that relevant controls for remote access are operating as intended.
- SSA assessed controls and enhancements as part of its annual FISMA assessment, including conducting both internal and external penetration testing,[44] as of March 2021.[45] Officials in SSA's Office of the Deputy Commissioner of Systems asserted that this level of

[44]Penetration testing is a test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.

[45]FISMA requires agencies to report the status of their information security program to OMB and requires inspectors general to conduct annual independent assessments of those programs.

testing covered all of the relevant controls and enhancements, and emphasized that, from an operations perspective, they believe regular reviews and testing of information security controls are effective. However, the agency's documentation was not detailed enough to demonstrate that it had assessed about half of the relevant controls and enhancements for its system that provided remote access to support telework. For example, SSA did not always link assessment results to specific controls in its assessment documentation. As a result, the agency lacks assurance that relevant controls for remote access are operating as intended.

- The Bureau of Indian Affairs and National Park Service both rely on the Department of the Interior to provide a remote access solution to employees. However, Interior had not assessed eight of the relevant security controls and enhancements as of May 2021. Interior's Office of the Chief Information Officer (OCIO) officials told us that the controls were not included in the prior assessment schedule.

  Further, assessments for another 10 of the security controls and enhancements had been in progress since 2018. Department officials stated that the controls were not assessed in 2018 due to staffing and resource issues. The officials asserted that they have addressed staffing and resource issues and will assess the controls in the department's current assessment period. In May 2021, after we informed Interior of these shortcomings, the department reassessed the 18 controls and enhancements. We verified that the department addressed all 18 controls and enhancements in its updated assessment.

Selected Agencies Had Not Always Assigned Risk Levels or Documented Remedial Actions Appropriately

FISMA requires that agencies periodically assess the risk that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support agency operations. FISMA also requires agencies to document remedial actions to address any deficiencies. Similarly, NIST SP 800-53 recommends that agencies periodically assess the risks to their systems in the event that they discover new threats or vulnerabilities. In addition, NIST SP 800-37 recommends that agencies create plans of action and milestones (POA&M) to identify the actions planned to correct weaknesses discovered in their information security controls.[46] NIST also recommends that POA&Ms include scheduled completion dates for milestones and

[46]National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations*, Special Publication 800-37 revision 2 (Gaithersburg, MD: December 2018).

tasks associated with addressing the weaknesses. The guidance further states that POA&Ms are to be used to monitor progress toward completing the tasks.

Based on their assessments of relevant controls and enhancements, all of the agencies in our review had identified weaknesses in their systems that support remote access. However, four agencies could not demonstrate that they had consistently monitored progress toward completing the remedial actions. In addition, one of these four agencies could not demonstrate that it had documented the risks associated with the identified weaknesses. Specifically:[47]

- The Federal Law Enforcement Training Centers rely on DHS to provide a remote access solution to employees who are teleworking. However, DHS did not always consistently monitor its progress toward completing the remedial actions for weaknesses identified in its control assessments. For example, DHS had documented planned remedial actions to reduce the risks from weaknesses identified in nine relevant security controls and enhancements. Nevertheless, as of May 2021, the remedial actions associated with these weaknesses had passed their scheduled completion dates by just over 2 years. DHS OCIO officials told us that the remediation work for the two POA&Ms took longer than expected and, as a result, they had put waivers in place to allow more time to fully address the concerns.
- As of May 2021, DOT could not demonstrate that it had consistently monitored its progress toward completing remedial actions because the POA&Ms it created did not include estimated completion dates. Agency officials told us that the department's OCIO had been assuming operational and management responsibilities for technology and services transferred to it from other component agencies within the department. The officials explained that, during the transfer, OCIO inherited POA&Ms from the component agencies and did not initially

[47]Subsequent to our initial request for documentation (as of July 31, 2020), but before providing documentation to us, three agencies developed plans of action and milestones (POA&Ms) for relevant controls assessed as not fully implemented. Specifically, the Department of Justice (providing remote access service for the Executive Office of Immigration Review) developed a POA&M in October 2020 and the U.S. Department of Agriculture (providing remote access to the Food and Nutrition Service) developed POA&Ms in August 2020. In addition, the Securities and Exchange Commission, which had completed assessments through August 2020, developed POA&Ms through May 2021.

assess the planned actions due to COVID-19 response efforts, evolving priorities, and resource challenges.[48]

- Although the FBI had documented remedial actions and risks for weaknesses found with three relevant security control enhancements, the agency could not demonstrate that it had consistently monitored its progress in completing two of the three remedial actions. Specifically, the two remedial actions were still in progress at least 12 months beyond their estimated completion dates. FBI OCIO officials told us that staff responsible for remediation activities had made an administrative error and had not updated estimated completion dates associated with the two remedial actions; the officials added that FBI IT security personnel were properly tracking the remedial actions as well as the overall security posture of the system.
- Although OPM had documented remedial actions for weaknesses discovered by control assessments, it did not demonstrate that it always consistently monitored its progress toward completing the actions. For example, the agency had identified 16 remedial actions to correct weaknesses found in the relevant security controls and enhancements in calendar year 2019. However, 14 of the 16 remedial actions were in "draft" or "initial" status, and one did not have a status listed. Additionally, the agency had not estimated a date for completing any of the remedial actions. Further, OPM had not documented the risks for any of these weaknesses. OPM OCIO officials did not offer an explanation as to why these shortcomings in the documentation of risks and remedial actions existed.[49]

If these agencies do not consistently document risks and remedial actions and adequately monitor the progress toward completing those actions, they are at an increased risk that vulnerabilities in their systems that provide remote access connections could be exploited.

[48]In May 2021, subsequent to our analysis of agency documentation, Department of Transportation officials told us that the Office of the Chief Information Officer had taken corrective actions to review plans of action and milestones on a monthly basis, including an assessment of estimated completion dates and adherence to planned milestones. We plan to review the department's corrective actions as we follow up with agencies regarding the status of our recommendations to them.

[49]According to OPM OCIO officials, the agency had assessed the risk for each of the weaknesses, but did not communicate this information to us. We will verify OPM's actions as part of our recommendation follow-up process.

Conclusions

Officials from the 12 selected agencies reported that they had IT in place to allow employees to remotely access agency resources during the COVID-19 pandemic. While the selected agencies reported that they faced challenges in providing the IT needed to support remote access for maximum telework in response to the pandemic, they also reported that they had overcome most of the challenges quickly and were successfully supporting maximum telework.

In order to protect their systems in a time of increased cybersecurity risks associated with teleworking, the selected agencies generally followed federal information security guidance in implementing the systems that support remote access for telework. However, not all of the selected agencies assessed all relevant security controls to determine if they were operating as intended. In addition, not all of the selected agencies fully documented the risks and planned remedial actions intended to mitigate the gaps discovered during an assessment of the controls. Until the selected agencies fully assess all security controls and complete remedial actions for those controls assessed to not be operating as intended, their systems could be vulnerable to exploits.

Recommendations

We are making a total of nine recommendations to six agencies, including two to SEC, two to SSA, one to DHS, two to DOT, one to FBI, and one to OPM. Specifically:

The Chair of SEC should ensure that the agency documents relevant IT security controls and enhancements in the security plan for the system that provides remote access for telework. (Recommendation 1)

The Commissioner of SSA should ensure that the agency documents relevant IT security controls and enhancements in the security plan for the system that provides remote access for telework. (Recommendation 2)

The Secretary of Transportation should ensure that the agency assesses all relevant IT security controls and enhancements for the system that provides remote access for telework. (Recommendation 3)

The Chair of SEC should ensure that the agency assesses and sufficiently documents the assessment of relevant IT security controls and enhancements for the system that provides remote access for telework. (Recommendation 4)

The Commissioner of SSA should ensure that the agency assesses and sufficiently documents the assessment of relevant IT security controls and enhancements for the system that provides remote access for telework. (Recommendation 5)

The Secretary of Homeland Security should ensure that the agency consistently monitors progress toward the completion of remedial actions for the system that provides remote access for telework. (Recommendation 6)

The Secretary of Transportation should ensure that the agency consistently monitors progress toward the completion of remedial actions by including estimated completion dates in its plan of action and milestones for the system that provides remote access for telework. (Recommendation 7)

The Director of the FBI should ensure that the bureau consistently monitors progress toward the completion of remedial actions for relevant IT security controls and enhancements for the system that provides remote access for telework. (Recommendation 8)

The Director of OPM should ensure that the agency documents risks and monitors progress toward the completion of remedial actions by including estimated completion dates in plans of action and milestones and keeping them up to date with current information for the system that provides remote access for telework. (Recommendation 9)

Agency Comments and Our Evaluation

We requested comments on a draft of this report from the 12 agencies selected for our review. In response, the six agencies to which we made recommendations provided comments agreeing with the recommendations. In addition, one agency to which we did not make a recommendation provided comments on the draft report. The remaining agencies did not provide any comments on the draft report.

Via email, an audit liaison at DOT, which provides remote access service to the Federal Highway Administration, stated that the department concurred with our recommendation.

Via email, an audit liaison at DOJ stated that the department concurred with our recommendation to FBI.

DHS provided written comments on behalf of the Federal Law Enforcement Training Centers and the U.S. Secret Service. In its

comments, DHS stated that it agreed with our recommendation to the department related to providing remote access service to the Federal Law Enforcement Training Centers. DHS also believed that it has implemented the recommendation. We plan to follow-up to validate the department's actions regarding the recommendation. DHS's comments are reprinted in appendix III.[50] The department also provided a technical comment, which we have incorporated into this report as appropriate.

SEC provided written comments in which it agreed with our two recommendations. Regarding our recommendation that SEC ensure that it documents relevant IT security controls and enhancements in the security plan for the system that provides remote access for telework, the agency stated that it was tracking the issue and expects to complete actions to address it by December 2021.

Regarding our recommendation that the agency ensure that it assesses and sufficiently documents the assessment of relevant IT security controls and enhancements for the system that provides remote access for telework, SEC stated that it was currently performing a new assessment of the components that support the agency's remote access solutions. SEC added that it expects to complete the assessment by the second quarter of fiscal year 2022 and that the assessors are expected to fully document their findings. The agency further noted that it plans to continue to frequently assess the security posture of its remote access capabilities. SEC's comments are reprinted in appendix IV.

In written comments, SSA stated that it agreed with our recommendations. The agency added that it was finalizing the security plan for its system that provides remote access for telework. SSA's comments are reprinted in appendix V.

In written comments, OPM agreed with our recommendation. The agency stated that it intended to document risks and monitor the progress of remedial actions. In addition, the agency said it will include estimated completion dates and current information to keep the plans of action and milestones up to date for its systems that provide remote access for telework. OPM's comments are reprinted in appendix VI.

[50]We did not include a second page of the department's letter reprinted in appendix III because it contained sensitive information. The second page included details specific to actions taken by DHS to address our recommendation.

While we did not make recommendations to IRS, in written comments, the agency described actions it had taken to ensure that IRS could continue its mission-critical activities while responding to the COVID-19 pandemic. For example, the agency said it quickly scaled up its infrastructure and equipped customer service representatives with laptops and peripheral equipment to support telework. The agency added that in expanding telework, IRS followed cybersecurity recommendations for federal agencies, as well as applicable guidance from NIST bulletins and OMB. IRS's comments are reprinted in appendix VII.

In addition to the aforementioned responses, officials from the remaining agencies sent emails stating that they did not have any comments on the draft report. Specifically, we received emails from liaisons at the Department of Justice, which provides remote access service to the Executive Office of Immigration Review; the Department of Agriculture, which provides remote access service to Food and Nutrition Services; and the Department of the Interior, which provides remote access service to the Bureau of Indian Affairs and the National Park Service.

We are sending copies of this report to the appropriate congressional committees; the Secretaries of Agriculture, Homeland Security, Interior, and Transportation; the Attorney General of the United States; the Directors of the Executive Office of Immigration Review, the FBI, the Federal Law Enforcement Training Centers, the National Park Service, OMB, OPM, and the U.S. Secret Service; the chair of SEC; the Commissioners of the Internal Revenue Service and SSA; the Principal Deputy Secretary for Indian Affairs; the Administrator of the Federal Highway Administration; offices of the chief information officer of agencies selected for our review; inspectors general of agencies selected for our review; and other interested congressional parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me 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 key contributions to this report are listed in appendix VIII.

Jennifer R. Franks
Director
Information Technology and Cybersecurity

List of Addressees

The Honorable Patrick Leahy
Chairman
The Honorable Richard Shelby
Vice Chairman
Committee on Appropriations
United States Senate

The Honorable Ron Wyden
Chairman
The Honorable Mike Crapo
Ranking Member
Committee on Finance
United States Senate

The Honorable Patty Murray
Chair
The Honorable Richard Burr
Ranking Member
Committee on Health, Education, Labor, and Pensions
United States Senate

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

The Honorable Margaret Wood Hassan
Chair
Subcommittee on Emerging Threats and Spending Oversight
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Rosa L. DeLauro
Chairwoman
The Honorable Kay Granger
Ranking Member
Committee on Appropriations
House of Representatives

The Honorable Frank Pallone, Jr.
Chair
The Honorable Cathy McMorris Rodgers
Republican Leader
Committee on Energy and Commerce
House of Representatives

The Honorable Bennie G. Thompson
Chairman
The Honorable John Katko
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Carolyn B. Maloney
Chairwoman
The Honorable James Comer
Ranking Member
Committee on Oversight and Reform
House of Representatives

The Honorable Richard Neal
Chair
The Honorable Kevin Brady
Republican Leader
Committee on Ways and Means
House of Representatives

Appendix I: IT Telework Questions Sent to Selected Agencies

This appendix contains the introduction and survey questions sent to the 12 selected agencies to obtain their perspectives regarding their initial experiences in providing the IT needed to support remote access for maximum telework in response to the pandemic. We sent the survey to agency liaisons in order to provide it to agency IT subject matter experts. See appendix II for our full scope and methodology. We received responses from all 12 agencies.

Survey Introduction

GAO is gathering information about the experience of implementing or expanding telework (working remotely) from an IT perspective as a result of the coronavirus (COVID-19) pandemic. We are doing this work at the request of the Congress and under the authority of the *CARES Act*.

If another agency or entity is responsible for the question content, please coordinate with the appropriate officials. For example, it may be appropriate to consult with CIO officials at the Departmental level. Please invite the relevant officials to assist in providing responses to these questions on behalf of <Name of agency/entity>.

Throughout this questionnaire, we use the term telework to mean when employees or contractors work remotely to access agency systems and applications to perform their work tasks.

Survey Questions

Do teleworkers (employees or contractors) using *government-furnished equipment* connect to the necessary agency systems and applications in the following ways? [*yes/no/not sure*]

- Virtual Private Network – VPN? (e.g., IPSec or SSL Tunnel)
- Application portals? (e.g., Virtual Desktop Infrastructure – VDI)
- Remote desktop access? (e.g., direct access to a device, such as an internal workstation through means other than VPN or VDI)
- Direct application access? (e.g., direct access to an application such as webmail via HTTPS)
- Other? (please describe)

How do teleworkers (employees or contractors) authenticate when accessing the network remotely using *government-furnished equipment*? [*yes/no/not sure*]

- PIV authentication?
- Other multi-factor authentication?

- Password alone?
- Other method? (please describe)

Are teleworkers (employees or contractors) allowed to use *personally-owned devices* to connect (directly or virtually) to agency systems and applications necessary to perform their work tasks? [*yes/no*]

[If personally-owned devices are allowed]
Are any of the following *personally-owned devices* allowed or not? [*allowed/not allowed*]

- Laptop/notebook computers?
- Smartphones?
- Tablets?
- Other? (please describe)

[If personally-owned devices are allowed]
Do teleworkers (employees or contractors) using *personal devices* connect to agency systems and applications in the following ways? [*yes/no/not sure*]

- Virtual Private Network – VPN? (e.g., IPSec or SSL Tunnel)
- Application portals? (e.g., Virtual Desktop Infrastructure – VDI)
- Remote desktop access? (e.g., direct access to a device, such as an internal workstation through means other than VPN or VDI)
- Direct application access? (e.g., direct access to an application such as webmail via HTTPS)
- Other? (please describe)

[If personally-owned devices are allowed]
How do teleworkers (employees or contractors) authenticate when accessing the network remotely using *personal devices*? [*yes/no/not sure*]

- PIV authentication?
- Other multi-factor authentication?
- Password alone?
- Other method? (please describe)

Did your agency procure additional *government-furnished equipment* for teleworkers in response to the telework expansion? [*yes/no*]

[If government-furnished equipment was procured]
Was any of the following additional equipment procured in response to the telework expansion? [*not procured/procured*] If so, how many? [indicate whether an estimate or exact amount]

- Laptop/notebook computers?
- Smartphones?
- Tablets?
- Peripherals (monitors, cameras, keyboards, headsets, mice, docking stations, etc.)?
- Other? (please describe)

Does your agency have any ongoing procurement of additional *government-furnished equipment* in response to the telework expansion? [*yes/no/not sure*]

Did your agency *expand existing* IT infrastructure capacity (e.g., hardware, software licenses, or services) to support the telework expansion? [*yes/no/not sure*]

[If existing IT infrastructure capacity was expanded]
Did you *expand* the following existing IT infrastructure capacity or not? [*yes/no/not sure*]

- Bandwidth?
- VPN access?
- Cloud services?
- Software licenses?
- Other infrastructure? (e.g., servers, firewalls, network devices, etc.)
- Other? (please describe)

Did your agency *add new* IT infrastructure capacity (e.g., hardware, software, licensing, or services) to support the telework expansion? [*yes/no/not sure*]

[If new IT infrastructure capacity was added]
Did your agency *add* the following *new* IT infrastructure capacity or not? [*yes/no/not sure*]

- Bandwidth?
- VPN access?
- Cloud services?
- Software licenses?
- Other infrastructure? (e.g., servers, firewalls, network devices, etc.)
- Other? (please describe)

How much of a challenge, if at all, were each of the following IT operational matters in transitioning to increased telework? [*major challenge/moderate challenge/minor challenge/not a challenge/not sure or no basis to judge*]

- VPN?
- Bandwidth?
- Software or application licenses?
- Connecting remotely to legacy IT?
- PIV expirations requiring alternative authentication?
- Printing remotely?
- Providing government-furnished equipment?
- Service or Help Desk support?
- Other? (please describe)

What vendor delays, if any, did your agency experience in acquiring the following in transitioning to increased telework? [*major delay (more than 1 month)/moderate delay (2 weeks to a month)/minor delay (less than 2 weeks)/no delay/not sure or no basis to judge*]

- VPN access?
- Bandwidth?
- Cloud services?
- Software licensing?

- Government-furnished equipment?
- Other? (please describe)

Has your agency provided additional security training or guidance to teleworkers since mid-March 2020? [*yes/no/not sure*]

- Additional security training?
- Additional security guidance?
- Other? (please describe)

Has your agency experienced an increase, no change, or a decrease in the following activities related to cyberattacks or exploits since the telework expansion? [*increase/no change/decrease/not sure*]

- Denial of service?
- Phishing/spear-phishing
- Other? (please describe)

How much of a challenge, if at all, were the following IT security activities as a result of the expansion in telework? [*major challenge/moderate challenge/minor challenge/not a challenge/not sure or no basis to judge*]

- Deployment of patches and/or patch management?
- Oversight and enforcement of relevant security policies and procedures?
- Ensuring teleworker awareness of cyber threats?
- Incident response?
- Other? (please describe)

Considering your agency's telework in response to the pandemic, is there anything else you would like to offer from an IT perspective?

Appendix II: Objectives, Scope, and Methodology

The objectives for this review were to determine (1) selected agencies' initial experiences in providing the IT needed to support remote access for maximum telework in response to the COVID-19 pandemic and (2) the extent to which the selected agencies followed federal information security guidance for their IT systems that provide remote access to support telework.

In conducting the review, we first selected a non-probability sample of agencies to review. To do so, we initially identified the agencies listed in categories I and II in *National Continuity Policy*, Presidential Policy Directive 40, Annex A.[1] The agencies listed in Annex A perform mission essential functions that support national essential functions, and therefore, must be able to continue their operations in the event of an emergency or other continuity of operations event. In this first step, we chose 28 agencies from the list of agencies in Annex A.[2]

Next, we reviewed telework data about each of the 28 agencies from fiscal year 2018, as published by the Office of Personnel Management (OPM) in its annual *Status of Telework in the Federal Government* report to Congress.[3] This report includes, among other things, data regarding the number of employees at each agency, the number of employees eligible for telework, and the percentage of eligible employees who teleworked during the fiscal year.

[1]The White House*, National Continuity Policy,* Presidential Policy Directive 40 (Washington, D.C.: July 2016). Annex A of this policy directive assigns executive departments and agencies to one of four categories commensurate with their continuity of operations responsibilities during a catastrophic emergency. These categories are intended to be used for continuity planning, communications and information services requirements, emergency operations capabilities, and other related requirements. Agencies identified as Category I perform "national essential functions," which are those functions necessary to lead and sustain the nation during a catastrophic emergency. Agencies identified as Category II are agencies that perform "primary mission essential functions" that support national essential functions.

[2]We removed the Central Intelligence Agency and the Office of the Director of National Intelligence from this list due to concerns about the classified nature of data at those entities. Excluding the Central Intelligence Agency and the Director of National Intelligence, this list contains 28 agencies.

[3]Office of Personnel Management, *Status of Telework in the Federal Government,* Report to Congress Fiscal Year 2018 (Washington, D.C.: March 2020). The data from fiscal year 2018 were the most recent available for us to use at the time we selected agencies for our survey.

To perform this analysis, we subdivided the 28 agencies selected from Annex A into subcomponent agencies, as applicable.[4] We did so because, in some cases, employee telework infrastructure and policies would be managed at the subcomponent agency level, rather than at the department level. Based on the data available in the OPM telework report, we reviewed telework data from 66 agencies, which included subcomponent agencies from the initial 28 agencies.

We assessed the reliability of the data in the OPM report by reviewing the documentation of the methodology the agency used in preparing the report. We determined these data were sufficiently reliable for categorizing agencies by telework usage as part of the selection process for the agencies we reviewed.

We removed from our analysis, those agencies that had fewer than 1,000 employees and those where less than 20 percent of their employees were eligible to telework. We did so because agencies with so few employees eligible to telework are likely to have a mission that does not facilitate the use of telework. We then split the remaining agencies into three tiers, to include (1) those with a small number of employees, (2) those with a medium number of employees, and (3) those with a large number of employees.[5]

Within each tier, we arranged the agencies based on the percentage of eligible employees that teleworked in fiscal year 2018 at each agency. Our final selection included the two agencies from each tier with the smallest percentage of eligible employees who teleworked and the two agencies from each tier with the largest percentage of eligible employees who teleworked.[6] We selected agencies in this manner because we

[4]Some federal agencies are "federated," which means that they consist of multiple components. In this report, we use "agency" to refer to both an agency and its components.

[5]The small tier contained agencies with 1,000–4,000 employees; the medium tier contained agencies with 4,001–14,000 employees; and the large tier contained agencies with more than 14,000 employees. We chose these ranges because they appeared to be a natural breakdown in the size of the agencies in our selection.

[6]In three cases, we removed agencies from our list based on conversations that we conducted with agency inspectors general. These conversations provided insight into the nature of agency telework environments that we determined made them unsuitable for our review.

wanted to perform our review at agencies with both small and large telework operations before the pandemic.

Applying these criteria, we selected the following 12 agencies for our review:

- Food and Nutrition Service at the U.S. Department of Agriculture
- Bureau of Indian Affairs and National Park Service at the Department of the Interior
- Federal Highway Administration at the Department of Transportation
- Federal Law Enforcement Training Centers and U.S. Secret Service at the Department of Homeland Security
- Securities and Exchange Commission
- Social Security Administration
- Internal Revenue Service at the Department of Treasury
- OPM
- Executive Office for Immigration Review, and Federal Bureau of Investigation at the Department of Justice

To address the first objective, we conducted a survey of agency IT subject matter experts, including operations and IT security officials, at each of the 12 agencies selected for our review.[7] We developed and administered a questionnaire to, and received responses from, all 12 agencies. The questionnaire included questions about topics including the agency's telework environment, the process by which agencies expanded their systems that support telework in response to the COVID-19 pandemic, and changes in agency telework infrastructure due to the expansion of telework. It also included a list of several potential IT challenges that agencies may have faced during their transition to

[7]We collected questionnaire results from knowledgeable officials at each of the 12 agencies in our review. However, in some cases, agency components relied on telework infrastructure at the department level, such as a department-wide virtual private network. Accordingly, we requested that agency officials forward the questionnaire to knowledgeable parties at the department level, as applicable. We collected the contact information for those individuals who filled out the questionnaire to understand which responses reflected the perspectives of the components in our scope, and which reflected the agency's perspectives.

maximum telework, and asked them to indicate the extent to which they experienced these challenges.[8]

The practical difficulties of developing and administering a survey may introduce errors, including how a particular question is interpreted, for example. Therefore, we included steps in developing and administering the questionnaire to minimize such errors. We conducted two pretests of the questionnaire with IT subject matter experts from two agencies by telephone to check that (1) the questions were clear and unambiguous, (2) terminology was used correctly, (3) the questionnaire did not place an undue burden on agency officials, (4) the information could be obtained, and (5) the survey was comprehensive and unbiased.

We reviewed the results of the completed questionnaires and used the responses to tailor follow-up interviews at each of the 12 agencies to ask additional questions of the IT subject matter experts and clarify questionnaire responses. In addition to clarifying questions, our interviews included questions about

- the agency's telework environment,
- the process by which the agency expanded its telework environment in response to the COVID-19 pandemic,
- IT support available for teleworkers, security policies, and communication of cyber threats to teleworkers,
- cybersecurity and threat management, and
- lessons learned by the agency throughout its transition to maximum telework.

We also held interviews with employee union representatives from seven of the 12 agencies.[9] We conducted these interviews to ask questions

[8]Guidance included documentation from both the Cybersecurity and Infrastructure Security Agency and the National Institute of Standards and Technology (NIST) regarding securing federal telework solutions and the transition to maximum telework from an IT perspective. We met with officials from NIST to ensure that we had included the most pertinent guidance in our questionnaire.

[9]Officials from the Federal Bureau of Investigation, Federal Highway Administration, and U.S. Secret Service told us that their employees were not members of a union. In addition, a union representative from the Bureau of Indian Affairs declined to comment, and a union representative from the Federal Law Enforcement Training Centers did not respond to our interview request. At the seven agencies in which we interviewed union representatives, some of the agencies had a single union representative, while others had multiple union representatives.

regarding employees' experiences during maximum telework in response to the pandemic from an IT perspective to gain insight into their experiences beyond that of agency officials. We asked questions regarding any challenges conveyed by employees to their union representatives during maximum telework from an IT perspective, as well as questions about what went well in the same time frame.

In conjunction with the survey results, we reviewed the results of the interviews of agency IT subject matter experts and union representatives to understand what agencies' initial experiences were in providing the IT needed to provide remote access to support maximum telework in response to the pandemic. The experiences reflected the views of only those agencies that participated in our survey and interviews, and, therefore, are not generalizable to federal agencies as a whole. Regardless of this limitation, the solicited perspectives provided insight into the experiences and views of the selected agencies.

To address the second objective, in addition to interviews of the agency officials, we requested and reviewed IT security documentation associated with the systems that support remote access for telework for the 12 selected agencies.[10] Specifically, the documentation we requested was based on NIST guidance for securing federal information systems, including those systems that provide remote access to support telework at agencies, and included the following:[11]

[10]We requested documentation from the agencies as of July 31, 2020. However, in some cases, agencies did not provide us with documentation until much later (e.g. February 2021). Further, some of the documentation provided to us by the agencies included information that had been updated after July 31, 2020.

[11]National Institute of Standards and Technology, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security,* Special Publication 800-46 revision 2 (Gaithersburg, MD: July 2016) and *Security and Privacy Controls for Federal Information Systems and Organizations,* Special Publication 800-53 revision 4 (Gaithersburg, MD: January 2015), provide guidance for the security of agency IT systems, including those systems that support telework. NIST released revision 5 of Special Publication 800-53 in September 2020; however, revision 4 was in effect at the time of our review.

- agency telework security policies,
- system security plans for the systems that provide remote access to support telework at agencies,[12]
- security and risk assessment documentation for the systems that provide remote access at agencies, and
- any remedial actions created as a result of the assessment of security controls for the systems that support remote access at agencies.

We reviewed the agency documentation to evaluate whether the agencies had included the following elements of a telework security policy, per NIST Special Publication (SP) 800-46, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*:

- which forms of remote access would be permitted by the agency for employees,[13]
- types of telework devices permitted for each form of remote access, and
- how user account provisioning should be handled.

We also reviewed how agencies had documented and assessed relevant IT security controls intended to protect agency systems that support telework.[14] Specifically, we reviewed security controls most relevant to protecting agency telework environments based on guidance in NIST SP 800-46 and NIST SP 800-53 revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. Further, we reviewed how agencies had documented remedial actions as warranted, in

[12]We defined a system that provides remote access to support telework at the selected agencies as the system that contains the method by which employees connect to agency resources, such as a virtual private network. Because of this, in some cases, we reviewed department-level documentation because the connection method was implemented and managed at the department level and not at the component level.

[13]In most cases, remotely accessing agency systems and services is required to enable an employee to telework.

[14]Our evaluation consisted of an assessment of documentation provided to us by the selected agencies. We did not perform any on-site or technical testing of IT security controls to determine whether agencies had designed or implemented these controls effectively or not.

accordance with NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations*.[15]

NIST SP 800-46 includes a list of security controls that it deems most relevant to securing systems that support remote access for telework. In addition, NIST SP 800-53 revision 4 suggests that agencies implement a set of control baselines based on the Federal Information Processing Standard Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* impact assessment of their system.[16] The baselines include additional enhancements to the controls that are intended to provide increased security.[17] Based on the NIST SP 800-46 list of controls and the NIST SP 800-53 revision 4 control baselines, we reviewed agency documentation associated with the following controls and control enhancements:[18]

- **AC-2, account management:** Involves managing single-factor or multifactor authentication for remote access users, such as passwords, digital certificates, and/or hardware authentication tokens. This control has four enhancements at the moderate-impact baseline and eight enhancements at the high-impact baseline.
- **AC-17, remote access:** Dedicated to documenting remote access requirements, authorizing remote access prior to allowing

[15]National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations,* Special Publication 800-37 revision 2 (Gaithersburg, MD: December 2018).

[16]National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standard Publication 199 (FIPS-199) (Gaithersburg, MD: February 2004). FIPS-199 defines three levels of potential impact on agencies or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or reliability) for its information systems. The levels are low impact, moderate impact, and high impact. NIST SP 800-53 security control baselines represent a starting point in determining the security controls for information systems based on their impact level, as determined by FIPS-199.

[17]Enhancements to baseline security controls are used to supplement security controls. For example, control AC-2 focuses on how agencies manage user accounts for their information systems, and the first enhancement suggests that agencies additionally employ automated mechanisms to support management of information system accounts. Agencies have flexibility in applying baseline security controls from NIST SP 800-53 and can tailor their relevant security control baseline so that it more closely aligns with their mission and business requirements and environments of operation.

[18]NIST SP 800-46 also includes control IA-11 in its appendix of relevant security controls. However, IA-11 does not appear in the NIST SP 800-53 baseline of controls for either moderate-impact or high-impact systems, so we did not review agencies' implementation of it.

connections, monitoring and controlling remote access, encrypting remote access, etc. This control has four enhancements at both the moderate and high-impact baselines.

- **AC-19, access control for mobile devices:** Includes requirements for agency-controlled mobile devices and authorization to connect mobile devices to agency systems, such as through remote access. This control has one enhancement at moderate- and high-impact baselines.
- **AC-20, use of external information systems:** Involves the use of external information systems, such as personally owned client devices and third-party-controlled client devices that may process, store, or transmit agency-controlled data. This control has two enhancements at moderate- and high-impact baselines.
- **CA-9, internal system connections:** Involves connections between a system and its components, including mobile devices and laptops. This control has no enhancements at either baseline.
- **CP-9, information system backup:** Telework devices need to have their data backed up either locally or remotely. This control has one enhancement at the moderate-impact baseline and four enhancements at the high-impact baseline.
- **IA-2, identification and authorization (agency users):** Involves using single factor or multifactor authentication for remote access users, such as passwords, digital certificates, and/or hardware authentication tokens. This control has six enhancements at the moderate-impact baseline and eight enhancements at the high-impact baseline.
- **IA-3, device identification and authentication:** Mutual authentication is recommended whenever feasible to verify the legitimacy of a remote access server before providing authentication credentials to it. This control has no enhancements at either baseline.
- **RA-3, risk assessment:** A risk assessment should be performed as part of selecting a remote access method. This control has no enhancements at either baseline.
- **SC-7, boundary protection:** Involves segmenting a network to keep publicly accessible components off internal networks and monitoring and controlling communications at key boundary points. This control has four enhancements at the moderate-impact baseline, and seven enhancements at the high-impact baseline.
- **SC-8, transmission confidentiality and integrity:** The various remote access methods discussed in NIST SP 800-46 protect the

confidentiality and integrity of transmissions through the use of cryptography. This control has one enhancement at both the moderate- and high-impact baselines.

For each of the relevant security controls and associated enhancements, we evaluated whether a selected agency had:

- documented the implementation of controls intended to protect their systems that support telework in their system security plans,
- assessed the implementation for these controls,
- identified risks to their systems based on the assessments, and planned remedial action activities to be taken based on the results of control assessment activities (a plan of action and milestones), and
- monitored progress toward completion of remedial actions (i.e., documented and met internal completion dates).

We also determined that the control activities component of internal control was significant to this objective, along with the underlying principles that management should implement control activities through policy and design information system and related control activities to achieve objectives and respond to risks. As previously noted, we assessed whether selected agencies' telework security policies aligned with elements recommended by NIST. In addition, we reviewed agency documentation to determine whether they had documented relevant security controls in a security plan, assessed the controls, and assigned a risk level to controls that they determined to not be fully implemented.

Further, we determined that the monitoring component of internal control was significant to the objective, along with the underlying principle that management should remediate identified control deficiencies on a timely basis. As previously noted, we assessed whether selected agencies documented remedial action plans for security controls that they assessed to not be fully implemented and whether the agencies met time frames specified in the plans for addressing the deficiencies.

We conducted this performance audit from April 2020 through September 2021 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.

Appendix III: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

September 17, 2021

Jennifer R. Franks
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report, GAO-21-583 "COVID-19: Selected Agencies Overcame Technology Challenges to Support Telework but Need to Fully Assess Security Controls"

Dear Ms. Franks:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition that DHS's Cybersecurity and Infrastructure Security Agency (CISA) provides a variety of telework security guidance for both federal agencies and non-federal organizations for employees working remotely. For example, CISA provided guidance for implementing strong authentication, securing web applications against cybersecurity threats, and avoiding phishing attacks. DHS is committed to protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

The draft report contains nine recommendations, including one for DHS with which the Department concurs. Attached find our detailed response to the recommendation. DHS previously submitted technical comments addressing accuracy and other issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions.

Sincerely,

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2021.09.17 11:07:43 -04'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

Appendix IV: Comments from the Securities and Exchange Commission

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

September 16, 2021

Jennifer R. Franks
Director
Cybersecurity and Information Management
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Franks,

Thank you for the opportunity to review and comment on the draft Government Accountability Office (GAO) report "*Selected Agencies Overcame Technology Challenges to Support Telework but Need to Fully Assess Security Controls*." I appreciate GAO's thorough work analyzing the SEC's telework program and agree with the importance GAO placed in its report on telework security. The SEC has continued to prioritize the security of our remote access capabilities. We concur with the two areas GAO has cited for improvement.

I would like to share some additional context regarding GAO's two recommendations. First, with respect to GAO's findings of three missing control descriptions in the System Security Plan (SSP) covering the agency's remote access systems, the Office of Information Technology (OIT) has been tracking this issue as a result of a previous independent security assessment completed in September 2020. The estimated completion date remediating this issue is December 2021.

Second, regarding GAO's second recommendation on assessment documentation, independent assessors are currently performing a new assessment of the components that support the agency's remote access solutions. They expect to complete testing by the second quarter of fiscal year 2022 and will fully document their findings. OIT will continue to assess frequently the security posture of the agency's remote access capabilities, including through vulnerability scanning and participation in the Cybersecurity and Infrastructure Security Agency's (CISA) Cyber Hygiene Program.

Thank you once again for the professionalism and courtesies that you and the GAO team demonstrated throughout this audit. We intend to pursue these corrective actions as a top priority, and look forward to working with your office to confirm our actions fully address the issues identified in your report. If you have any other questions, please do not hesitate to contact me at (202) 551-5703.

Sincerely,

Bottom, David Digitally signed by Bottom, David Date: 2021.09.16 09:23:42 -04'00'

David Bottom
Chief Information Officer

Appendix V: Comments from the Social Security Administration

SOCIAL SECURITY
Office of the Commissioner

September 17, 2021

Jennifer R. Franks
Director, Information Technology and Cybersecurity Issues
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Director Franks:

Thank you for the opportunity to review the draft report "COVID-19: Selected Agencies Overcame Technology Challenges to Support Telework but Need to Fully Assess Security Controls" (GAO-21-583) and the accompanying enclosure. We agree with the recommendations.

We are finalizing our security plan for our system that provides remote access for telework. In addition, we are documenting the extensive control testing we conduct to ensure the security of our systems.

If you have any questions, please contact me at (410) 965-2611. Your staff may contact Trae Sommer, Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

Scott Frey
Chief of Staff

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

Appendix VI: Comments from the Office of Personnel Management

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Chief Information Officer

Ms. Jennifer R. Franks
Director
Information Technology and Cybersecurity Issues
US Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Franks:

Thank you for providing us the opportunity to respond to the Government Accountability Office (GAO) draft report, *COVID-19: Selected Agencies Overcame Technology Challenges to Support Telework but Need to Fully Assess Security Controls*, GAO-21-583, GAO job code 104260.

Our response to your recommendation is provided below.

Recommendation 9: The Director of the Office of Personnel Management should ensure that the agency documents risks and monitors progress toward the completion of remedial actions by including estimated completion dates in plans of action and milestones and keeping them up to date with current information for the system that provides remote access for telework.

Management Response: Concur. OPM will document risks and monitor the progress of remedial actions in the POA&Ms. OPM will include estimated completion dates and current information to keep the POA&Ms up to date for the systems that provide remote access to telework.

We appreciate the opportunity to respond to this draft report. If you have questions regarding our response, please contact Larry Allen, larry.allen@opm.gov or 202-230-2229.

Sincerely,

Guy Cavallo
Digitally signed by Guy Cavallo
Date: 2021.09.20 13:57:04 -04'00'

Guy V. Cavallo
Chief Information Officer
U.S. Office of Personnel Management

www.opm.gov Recruit, Retain, and Honor a World Class Workforce to Serve the American People www.usajobs.gov

Appendix VII: Comments from the Internal Revenue Service

DEPUTY COMMISSIONER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

September 16, 2021

James R. McTigue, Jr.
Director, Tax Policy and Administration
Strategic Issues Team U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. McTigue:

Thank you for the opportunity to comment on the draft report entitled COVID-19: Selected Agencies Overcame Technology Challenges to Support Telework but Need to Fully Assess Security Controls (GAO-21-583). Responding to the COVID-19 Pandemic was an enormous undertaking as the IRS delivered Economic Impact Payments in record time while simultaneously keeping the annual filing season on track and expanding telework capabilities to help protect the health and safety of taxpayers and IRS employees.

The IRS Information Technology (IT) organization successfully expanded telework capabilities by quickly adjusting in-flight plans and scaling up the agency's infrastructure. The IRS remote access solution was previously sized to support an immediate increase and the infrastructure was designed to easily and quickly accommodate double the available capacity if needed. By September 2020, the number of IRS employees teleworking had more than doubled since the onset of the pandemic, with nearly 60,000 employees simultaneously connecting to the IRS network remotely. To meet this expansion, IRS IT also mobilized to equip the IRS workforce with the equipment needed to telework. We equipped IRS customer service representatives with laptops and peripheral equipment bundles in preparation for telework, provided a variety of support and self-help services, and took unprecedented steps to ship laptops directly to employees' home addresses. By the end of FY 2020, more than 15,000 laptops and peripheral equipment bundles were provisioned across 28 sites around the country, and more than 2,000 employees received equipment at home. These actions helped ensure the continuity of mission critical activities.

In expanding telework, the IRS followed cybersecurity recommendations for federal agencies, along with the applicable guidance from the National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) bulletins and Office of Management and Budget (OMB). The Continuous Diagnostics and Mitigation (CDM) program, which helps in identifying and tracking our security posture, enabled the IRS to have greater certainty that the increased number of devices connecting remotely to the IRS network were in compliance and regularly updated.

If you have any questions, please contact me, or a member of your staff may contact Nancy A. Sieger, Chief Information Officer, at 202-317-5000.

Sincerely,

Jeffrey J. Tribiano

Digitally signed by Jeffrey J. Tribiano
Date: 2021.09.16 16:23:39 -04'00'

Jeffrey J. Tribiano
Deputy Commissioner for
Operations Support

Appendix VIII: GAO Contact and Staff Acknowledgments

GAO Contact

Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov

Staff Acknowledgments

In addition to the individual named above, Jeffrey Knott (Assistant Director), William Cook (Analyst-in-Charge), Christopher Businsky, Nancy Glover, Ronald La Due Lake, Richard Sayoc, Kevin Smith, Priscilla Smith, and Haley Weller made key contributions to this report. West Coile, Sailaja Ledalla, Monica Perez Nelson, and Adam Vodraska also provided valuable assistance.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548