Federal Telework During the COVID-19 Pandemic: Cybersecurity Issues in Brief

April 10, 2020

Congressional Research Service
https://crsreports.congress.gov
R46310

CRS REPORT
Prepared for Members and
Committees of Congress

Contents

Figures

Contacts

Introduction

President Trump declared the Coronavirus Disease 2019 (COVID-19) a national emergency in March 2020.[1] In an effort to slow the transmission of COVID-19, the Office of Management and Budget (OMB) ordered federal agencies to "maximize telework across the nation for the Federal workforce (including mandatory telework, if necessary), while maintaining mission-critical workforce needs."[2] Private sector companies are taking similar measures.[3]

This report provides information on telework in practice at federal agencies and potential effects of telework on our communications infrastructure, data, and security.[4]

Telework in Practice

This section discusses how employees may access an organization's digital resources and potential effects that may have on communications infrastructure.

Working Onsite at an Organization's Facilities

For many organizations, employees perform their work at an organization-controlled facility, such as an office which affords access to both digital and physical resources. Workers access company information on equipment owned by the organization (e.g., a laptop), and use software the company approves (e.g., a word processor). Typically, organizations provide email services, internet access, and other communication services (e.g., chat). In this model, the organization controls data access, and provides cybersecurity safeguards to protect their information, the employees, and the organization itself.

Some of the cybersecurity safeguards an organization may provide include:

- anti-malware software at both the device and network level (prevents malicious software from executing unauthorized commands on the system);
- intrusion protection systems (detects and blocks malicious internet traffic coming into and going out of the organization's network);
- firewalls (blocks certain internet traffic based on preset rules);
- regular patching and secure configurations (minimizes opportunities for hackers to exploit vulnerabilities in a system); and
- event logging (allows security professionals to investigate and identify attacks).

[1] Executive Office of the President, "Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak," 85 *Federal Register* 15337-15338, March 18, 2020. For more information on the novel coronavirus (COVID-19), see https://www.cdc.gov/coronavirus/2019-nCoV/index.html.

[2] Office of Management and Budget, "Federal Agency Operational Alignment to Slow the Spread of Coronavirus COVID-19," M-20-16, March 17, 2020, at https://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf.

[3] Jena McGregor, "How IBM, Goldman Sachs, PwC, and Others are Responding to the Coronavirus Threat to the Global Workplace," *The Washington Post*, February 28, 2020, at https://www.washingtonpost.com/business/2020/02/28/workplace-coronavirus-work-from-home/.

[4] For general information on federal telework policy in response to coronavirus, see CRS In Focus IF11454, *Telework in Executive Agencies: Background, OPM Guidance, and 116th Congress Legislation Following Coronavirus*, by Barbara L. Schwemle.

These safeguards may still apply if employees telework. For a discussion of the effect of cybersecurity tools when employees telework, see the "Increased Telework" section of this report.

Working Remotely

With the increased adoption of information communications technologies (ICT) that support mobile computing (e.g., wireless networking and video teleconferencing), more organizations and employees are embracing remote working arrangements.

Telework is "the ability for an organization's employees, contractors, business partners, vendors, and other users to perform work from locations other than the organization's facilities."[5] Federal agencies have used telework as workplace flexibility, a tool to ease transportation congestion, and a perk for recruiting and retaining a workforce. Over the years it has also been used as a tool to benefit the government, such as maintaining productivity during emergencies (e.g., inclement weather) and reducing real estate costs.[6]

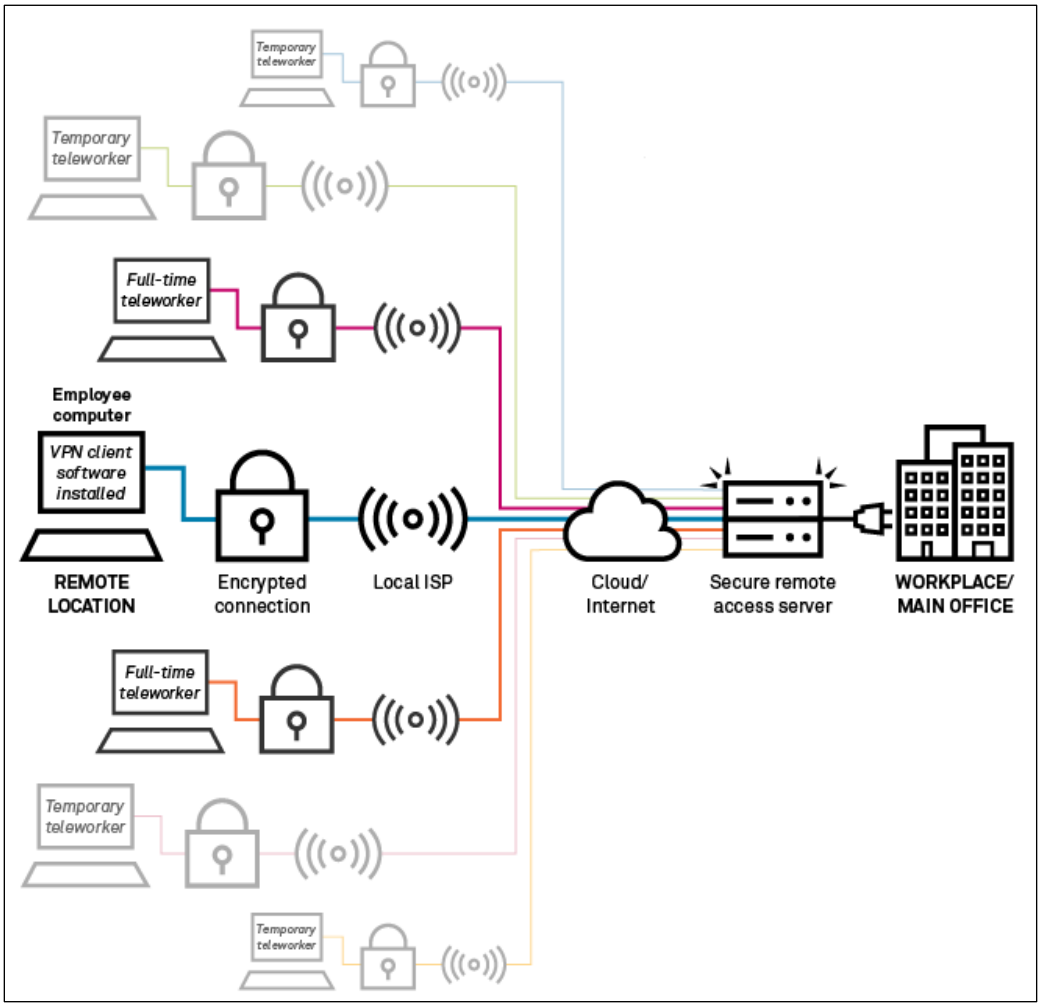
Employees may access an organization's information network on an organization-provided device (e.g., laptop or mobile phone) or their own device (i.e., under a bring-your-own-device, or BYOD, policy). Devices usually need some additional software to enable access, such as a virtual private network (VPN) client. A VPN creates an encrypted tunnel between the device and the network it is seeking to access. Data passes between the device and the organization using common internet infrastructure, but the encrypted tunnel is designed to prevent other users or devices from reading the data between the two.[7] The organization will usually have some appliance (i.e., a piece of hardware with dedicated software, like a secure remote access server) running at the point at which the organization connects to the internet. This appliance will serve to manage the VPN and allow access to the organization's network. In essence, a VPN is a software solution to allow devices to remotely connect to an organization's network as if they were physically attached to that network. **Figure 1** shows a graphical representation of how this could work.

[5] Murugiah Souppaya and Karen Scarfone, "User's Guide to Telework and Bring Your Own Device (BYOD) Security," NIST Special Publication 800-114 Revision 1, July 2016, at http://dx.doi.org/10.6028/NIST.SP.800-114r1.

[6] Office of Personnel Management, "Telework Legislation: Background and History," website, https://www.telework.gov/guidance-legislation/telework-legislation/background-history/.

[7] For more information on encryption, see CRS Report R44642, *Encryption: Frequently Asked Questions*, by Chris Jaikaran.

Figure 1. How VPN Is Used to Access a Business Network



Source: Cat Weeks, S&P Global Market Intelligence, March 18, 2020.

Notes: Local ISP = Local Internet Service Provider (e.g., Comcast or RCN). VPN = Virtual Private Network. Cloud/Internet = Internet backbone infrastructure (e.g., core providers and cloud services providers).

This model is not the only one for teleworking employees. For example, some organizations use cloud-based resources (e.g., Microsoft Office 365) in lieu of resources owned and maintained by the organization. In that case, the employee may access their organization's data without their internet traffic first routing through the organization. Some federal agencies do employ a cloud-based computing solution. For example, at the end of 2019, 76% of federal agencies had migrated their email services to a cloud-based service provider.[8] However, the full extent of federal agency cloud adoption is not publicly known.[9]

[8] Office of Management and Budget, *A Budget for America's Future: Analytic Perspectives*, Fiscal Year 2021, Washington, DC, February 2020, p. 220, https://www.whitehouse.gov/wp-content/uploads/2020/02/ap_15_it_fy21.pdf.

[9] For more information on federal cloud adoption, see GAO, "Cloud Computing Security: Agencies Increased the Federal Authorization Program, but Improved Oversight and Implementation Are Needed," GAO-20-126, December, 12, 2019, at https://www.gao.gov/products/GAO-20-126. For more information on federal cloud use, see CRS Report R46119, *Cloud Computing: Background, Status of Adoption by Federal Agencies, and Congressional Action*, by Patricia Moloney Figliola.

It is also important to note that employees may potentially access multiple networks in an organization. A teleworking employee may access an organization's data network to correspond using email or access a database. But an employee may also access an organization's voice network to access voicemail on a desk phone or forward business calls. Organizations may also have more than one voice, data, or video network on which their employees conduct their business.

Impact on Infrastructure

Since the outbreak of COVID-19, telework use has increased significantly. One estimate saw use of VPN in the United States increase 53% from early to mid-March, and predicts it will have increased by more than 150% from March 2019 to March 2020.[10] This trend has the potential to stress information communication infrastructure. As a whole, American internet service providers (ISPs) have been able to handle the shifts and spikes in internet usage; however, questions remain as to whether or not this infrastructure can continue to handle increased loads.[11]

Although ISPs have been able to manage demands for network access to date, other elements of internet infrastructure have been stressed. Content delivery networks (CDNs)[12] host multiple copies of information (e.g., webpages, videos, and files) that users seek to access on the internet in geographically disperse servers. This redundancy creates resiliency in users' ability to access content and allows content to be delivered faster. With the shift in when users are accessing internet services, some CDNs are prioritizing certain types of content (e.g., video teleconferencing service) and deprioritizing others (e.g., game downloads) in order to maintain speedy access to services.[13]

The Cybersecurity of Telework

This section discusses existing guidance agencies follow while managing cybersecurity risks related to telework and security risks they may experience.

Security Guidance

Generally, federal agencies follow the Federal Information Security Modernization Act (FISMA, P.L. 113-283) to guide their information technology risk management practices.[14] FISMA lays out responsibilities for:

[10] "VPN Use Spikes During Coronavirus, Boosting Business, Exposing Limitations," S&P Global, Market Intelligence, March 18, 2020, https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/vpn-use-spikes-during-coronavirus-boosting-business-exposing-limitations-57599742.

[11] Marguerite Reardon, "Coronavirus Transforms Peak Internet Usage into the New Normal," *CNet*, March 23, 2020, at https://www.cnet.com/news/coronavirus-has-made-peak-internet-usage-into-the-new-normal/.

[12] CDNs are composed of a series of geographically dispersed servers which store internet content users seek to access. CDNs also enable services that users seek to engage, such as video teleconferencing. CDNs deliver content and services to users in a decentralized way, so that content can be delivered as quickly as possible and in a way that does not burden internet infrastructure. For more information on CDNs, see Cloudfare, "What Is a CDN," at https://www.cloudflare.com/learning/cdn/what-is-a-cdn/.

[13] Tom Leighton, "Working Together to Manage Global Internet Traffic Increases," *Akamai Blogs*, March 24, 2020, at https://blogs.akamai.com/2020/03/working-together-to-manage-global-internet-traffic-increases.html. Decisions on which traffic is prioritized is an ongoing discussion. CDNs engage with customers, ISPs, and regulators to determine which internet traffic to prioritize and how best to manage loads on their networks.

[14] 44 U.S.C. §§3551-3558.

- agency heads to be ultimately responsible for the security of their agency's information technology (but agency heads may delegate this responsibility to a senior agency official);
- the Director of the Office of Management and Budget (OMB) to provide strategic guidance on implementing FISMA;
- the Secretary of Homeland Security (through the Director of the Cybersecurity and Infrastructure Security Agency, CISA) to provide operational guidance and assistance to federal agencies in securing their networks;
- Inspectors General (IGs) to independently evaluate the information security programs of agencies; and
- the Director of the National Institute of Standards and Technology (NIST) to provide technical standards and guidance to agencies to follow in designing and implementing information technology security.

For COVID-19, OMB issued guidance directing federal agencies to maximize telework.[15] However, security guidance came from other agencies, namely NIST and CISA.

NIST Guidance

NIST has two primary documents that provide guidance to agencies on the security of telework: one addresses security of the enterprise[16] and the other addresses security of the user.[17] NIST has also published guidance for mobile device security.[18] In March 2020, NIST's National Cybersecurity Center of Excellence (NCCOE) provided additional guidance for telework security[19] and privacy during video teleconferences.[20] Among NIST's recommendations for enterprises are:

- Assume employees will be accessing the organization from untrusted devices and networks when developing telework policies;
- Develop telework, remote access, and bring-your-own-device (BYOD) policies together;
- Ensure that telework-enabled devices are updated regularly; and
- Separate network access and resources based on the type of device connecting to it.

[15] OMB, "Federal Agency Operational Alignment to Slow the Spread of Coronavirus COVID-19," M-20-16, March 17, 2020, at https://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf.

[16] Murugiah Souppaya and Karen Scarfone, "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security," NIST Special Publication 800-46 Rev. 2, July 2016, at https://doi.org/10.6028/NIST.SP.800-46r2.

[17] Murugiah Souppaya and Karen Scarfone, "User's Guide to Telework and Bring Your Own Device (BYOD) Security," NIST Special Publication 800-114 Revision 1, July 2016, at http://dx.doi.org/10.6028/NIST.SP.800-114r1.

[18] Murugiah Souppaya and Karen Scarfone, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," NIST SP 800-124 Rev. 1, June 2013, at https://doi.org/10.6028/NIST.SP.800-124r1.

[19] Jeff Greene, "Telework Security Basics," *Cybersecurity Insights: A NIST blog*, March 19, 2020, at https://www.nist.gov/blogs/cybersecurity-insights/telework-security-basics.

[20] Jeff Greene, "Preventing Eavesdropping and Protecting Privacy on Virtual Meetings," *Cybersecurity Insights: A NIST blog*, March 17, 2020, at https://www.nist.gov/blogs/cybersecurity-insights/preventing-eavesdropping-and-protecting-privacy-virtual-meetings.

Among NIST's recommendations for users are:

- Ensure data is backed up so that users can still access information even in a loss of network functionality;
- Receive training on and understand their organization's teleworking policies;
- Ensure their devices (to include home networking equipment) are updated and secure; and
- Avoid accessing organization computer resources on unapproved devices.

CISA Guidance

To complement NIST's guidance, the DHS Cybersecurity and Infrastructure Security Agency (CISA) issued additional guidance to organizations using telework in response to COVID-19.[21] CISA also issued an alert advising that malicious actors have a history of using world events to improve the likelihood that users fall prey to their scams, phishing attempts, and malware.[22] Phishing is a technique for "[t]ricking individuals into disclosing sensitive personal information through deceptive computer-based means." Malware is "[h]ardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose."[23] Among CISA's recommendations are:

- Avoid clicking on unsolicited web links and email attachments, which may carry malware;
- Use trusted sources for information, such as government websites with valid website certificates;
- Double check a source's authenticity prior to sending money, and check with the Federal Trade Commission (FTC) to see if it is a scam;[24]
- Update network devices and VPN appliances with the latest available patches to minimize the risk from known vulnerabilities;
- Enable network logging so that security personnel can audit, detect, and respond to incidents with current information; and
- Enable multi-factor authentication[25] for credentials accessing organization networks.

[21] CISA, "Enterprise VPN Security," *Alert AA20-073A*, March 13, 2020, at https://www.us-cert.gov/ncas/alerts/aa20-073a.

[22] CISA, "Defending against COVID-19 Cyber Scams," website, March 6, 2020, at https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams.

[23] Definitions are taken from the NIST Computer Security Resource Center Glossary, at https://csrc.nist.gov/glossary/.

[24] FTC, "Before Giving to a Charity," website, at https://www.consumer.ftc.gov/articles/0074-giving-charity.

[25] The term "multifactor authentication" refers to "[a]uthentication using two or more factors to achieve authentication. Factors are (i) something you know (e.g., password/personal identification number); (ii) something you have (e.g., cryptographic identification device, token); (iii) something you are (e.g., biometric)." William Newhouse, Michael Bartock, Jeffrey Cichonski, et al., "Derived Personal Identity Verification (PIV) Credentials," NIST Special Publication 1800-2, August 2019, at https://doi.org/10.6028/NIST.SP.1800-12.

Cybersecurity Risks

In addition to the persistent risks that organizations, administrators, and users face in cyberspace, the COVID-19 outbreak and response created two unique risks: a high-profile event and a rapid change in computing habits (i.e., telework).

A High Profile Event

Adversaries have a history of using high-profile events to entice and trick users. Government agencies[26] and private sector researchers[27] have issued warnings surrounding major events like the Olympics in the past. The coronavirus outbreak is no different.[28] Adversaries are counting on users' demand for the latest information, a desire to be charitable during a time of crisis, and the heightened public interest to improve the likelihood that a user engages with malicious websites, attachments, and emails.

The news media is reporting increased phishing attempts related to coronavirus.[29] Cybersecurity firms have also reported an increase in coronavirus-related phishing attempts.[30] The goal of these attempts is to get a user to click a link in an email, visit a malicious website, or download a compromised file in order to distribute malware to the user's device or to trick the user into sending money to an illegitimate recipient.[31] This activity is not limited to cyber criminals, but is also employed by nation-state actors, as well.[32] Hackers are not limited to compromising an end-user device. Some infiltrate home routers and other network infrastructure to reroute user web traffic from legitimate websites to illegitimate ones that distribute malware.[33]

Increased Telework

The second risk comes from the rapid pace at which organizations and employees are shifting their computing habits to telework. The rate at which agencies adopted a strategy of maximum telework in response to COVID-19 left little time for administrators to check their networks, improve policies, and apply updates. Employees are no longer accessing agency computing resources from inside agency facilities, with the physical security that comes with those

[26] CISA,"Pyeongchang 2018: Staying Cyber Safe During the Olympics," website, February 1, 2018, at https://www.us-cert.gov/ncas/current-activity/2018/02/01/Pyeongchang-2018-Staying-Cyber-Safe-during-Olympics.

[27] Tom Burt, "New Cyberattacks Targeting Sporting and Anti-Doping Organizations," *Microsoft on the Issues blog*, October 28, 2019, at https://blogs.microsoft.com/on-the-issues/2019/10/28/cyberattacks-sporting-anti-doping/.

[28] FBI, "FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic," Alert Number I-032020-PSA, March 20, 2020, at https://www.ic3.gov/media/2020/200320.aspx.

[29] Lily Hay Newman, "Watch Out for Coronavirus Phishing Scams," *Wired*, January 31, 2020, at https://www.wired.com/story/coronavirus-phishing-scams/.

[30] Fleming Shi, "Threat Spotlight: Coronavirus-Related Phishing," *Barracuda Network Blog*, March 26, 2020, at https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/.

[31] Catalin Cimpanu, "State-Sponsored Hackers Are Now Using Coronavirus Lures to Infect Their Targets," *ZDNet*, March 13, 2020, at https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/. BAE Systems, "COVID-19 Campaigns," infographic, March 2020, at https://info.ai.baesystems.com/rs/308-OXI-896/images/COVID-19-Infographic-Mar2020.pdf.

[32] Shannon Vavra, "Cybercriminals, Nation-States Increasingly Tailoring Coronavirus Spearphishing Campaigns," *CyberScoop*, March 12, 2020, at https://www.cyberscoop.com/coronavirus-phishing-scams-iran-china/.

[33] Dan Goodin, "New Attack on Home Routers Sends Users to Spoofed Sites That Push Malware," *Ars Technica*, March 25, 2020, at https://arstechnica.com/information-technology/2020/03/new-attack-on-home-routers-sends-users-to-spoofed-sites-that-push-malware/.

facilities.[34] They may be using unsecured home networks or devices (e.g., unpatched equipment) to access agency information. Agencies may have had to increase network access rapidly to allow for maximum telework, without establishing, testing, and refining security measures to protect data. Even with security measures in place within an agency's network, the proverbial 'perimeter' of the agency's network is extended well beyond its baseline posture with many more employees teleworking. NIST and CISA alerted agencies to these risks and encouraged them to put into place measure to minimize these risks.[35]

Federal agencies have been moving to a shared-services model under the Trump Administration.[36] CISA provides many of the cybersecurity services agencies rely on, including Continuous Diagnostics and Mitigation (CDM, a program to scan agency networks for vulnerabilities); EINSTEIN (a program to detect intrusions to agency networks coming from the internet); and Trusted Internet Connections (TIC, a program to consolidate internet access points for the federal government).[37] However, information on the ability for these programs to adequately operate in an environment where agency information is being accessed through heavy use of virtual private networks (VPNs), information being accessed directly through cloud service providers, or through other arrangements, is not publicly available. On April 8, 2020, CISA published interim guidance to federal agencies on using the TIC program during a surge in telework because of COVID-19. One of the goals of this document is to insure that network-level security protocols continue to protect agency information during the surge in telework arrangements.[38]

Adversaries may seek to compromise the VPNs themselves to gain access to agency networks or user devices. Vulnerabilities in VPN appliances were discovered in the past, leading government agencies to issue warnings and mandates to patch network infrastructure.[39] Adversaries may seek to compromise federal agency networks during this time of alternative data access. However, they may not need to attack the network itself. With so many users teleworking, an adversary may only need to compromise one or a few user devices, and then use their VPN connection to access agency information, appearing as legitimate traffic and network use to an agency's internal defenses and logs.[40]

---

[34] Many organizations have quickly adopted technologies to enable telework without testing them in their environment, such as video-teleconferencing applications. This practice may be prevalent in the private sector and would present certain security risks. However, CRS research did not identify instances of federal agencies using untested technologies to support maximum telework orders. As such, that risk is not addressed in this report.

[35] Karen Scarfone, Jeffrey Greene, and Murugiah Souppaya, "Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions," *ITL Bulletin*, March 2020, at https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf. CISA, "Enterprise VPN Security," *Alert AA20-073A*, March 13, 2020, at https://www.us-cert.gov/ncas/alerts/aa20-073a.

[36] Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," 82 *Federal Register* 22391-22397, May 11, 2017.

[37] CISA, "Securing Federal Network," website, February 25, 2020, at https://www.cisa.gov/securing-federal-networks.

[38] CISA, "Trusted Internet Connections 3.0: Interim Telework Guidance," guidance document, April 8, 2020, at https://www.cisa.gov/sites/default/files/publications/CISA-TIC-TIC%203.0%20Interim%20Telework%20Guidance-2020.04.08.pdf.

[39] CISA, "Threat to Network Infrastructure Devices," *Binding Operational Directive 16-02*, September 27, 2016, at https://cyber.dhs.gov/bod/16-02/. National Cyber Security Centre, "Vulnerabilities Exploited in VPN Products Used Worldwide," website, October 8, 2019, at https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities.

[40] Matthew Collins, *Common Sense Guide to Mitigating Insider Threats*, Software Engineering Institute: Carnegie Mellon University, Technical Note CMU/SEI-2015-TR-010, Hanscom AFB, MA, November 2016, p. 40, https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf.

Other risks may arise if employees are processing federal information outside of a secured device-to-agency connection. If employees are using publicly available, internet-based applications and platforms to conduct their business, they may not be using the cybersecurity tools offered by the agency—potentially exposing government information to malicious actors.[41]

How the shift to telework is affecting federal agencies is currently unknown. Federal agencies have not reported how prevalent telework is during the COVID-19 response. Before the COVID-19 outbreak, the Government Accountability Office (GAO) examined telework practices at agencies. GAO's investigations focused on the use of telework as a human capital and real property management tool, and agencies considered telework in terms of costs and benefits under that rubric. Despite existing guidance, GAO found data from agencies on the use of telework to be unreliable.[42]

Considerations for Congress

The U.S. Congress has held hearings to examine telework policy in federal agencies and considered legislation on the subject. Recent committee hearings have focused on employee abuse of telework.[43] At the start of the millennium, Congress looked at ways to promote telework as an employee benefit and to reduce real property costs.[44] However, after the attacks of September 11, 2001, Congress examined telework as a tool to ensure continuity of operations in the event of terrorist attacks or pandemics.[45] Congress has also considered legislation concerning telework and passed the Telework Enhancement Act of 2010 (P.L. 111-292). Concerning the COVID-19 outbreak, a bill introduced in the116th Congress would require federal agencies to permit employees to telework (S. 3561). These efforts do not significantly address cybersecurity matters of telework.

As the coronavirus outbreak continues and as government examines its response, policymakers may choose to examine the use of telework further. Three areas Congress may choose to explore are agency oversight, interagency collaboration, and cybersecurity investments.[46]

---

[41] FBI, "Cyber Actors Take Advantage of COVD-19 Pandemic to Exploit Increased Use of Virtual Environments," Alert Number I-040120-PSA, April 1, 2020, at https://www.ic3.gov/media/2020/200401.aspx. CISA, "COVID-19 Exploited by Malicious Cyber Actors," Alert (AA20-009A), April 8, 2020, at https://www.us-cert.gov/ncas/alerts/aa20-099a.

[42] GAO, "Federal Telework," key issue webpage, at https://www.gao.gov/key_issues/federal_telework/issue_summary.

[43] U.S. Congress, House Committee on the Judiciary and House Committee on Oversight and Government Reform, *Abuse of USPTO's Telework Program: Ensuring Oversight, Accountability and Quality*, 113th Cong., 2nd sess., November 18, 2014.

[44] U.S. Congress, House Committee on Government Reform Subcommittee on Technology and Procurement Policy, *Telework Policy*, 107th Cong., 1st sess., March 22, 2001, Serial No. 107-1 (Washington: GPO, 2001). U.S. Congress, House Committee on Government Reform, Subcommittee on Technology and Procurement Policy, *Toward a Telework-Friendly Government Workplace: An Update on Public and Private Approaches to Telecommuting*, 107th Cong., 1st sess., September 6, 2001, Serial No. 107-125 (Washington: GPO, 2002).

[45] U.S. Congress, House Committee on Government Reform, Subcommittee on Federal Workforce and Agency Organization, *Telecommuting: A 21st Century Solution to Traffic Jams and Terrorism*, 109th Cong., 2nd sess., July 18, 2006, Serial No. 109-230 (Washington: GPO, 2007). U.S. Congress, House Committee on Government Reform, *Beneficial or Critical? The Heightened Need for Telework Opportunities in the Post-9/11 World*, 108th Cong., 2nd sess., July 8, 2004, Serial No. 108-210 (Washington: GPO, 2004). U.S. Congress, House Committee on Government Reform, *Working Through an Outbreak: Pandemic Flu Planning and Continuity of Operations*, 109th Cong., 2nd sess., May 11, 2006, Serial No. 109-155 (Washington: GPO, 2006).

[46] Congress may also choose to consider policy options concerning the use of telework, its expansion or contraction, or its role in agency operations. Additionally, Congress may also be interested in the effects wide telework adoption has

- **Agency Oversight.** Some agencies reported disruptions as employees started to telework en masse.[47] Other agencies braced for stress to their network infrastructure.[48] Regardless of the prevalence of employee teleworking, agencies still face the need to manage ordinary risks to their cyber infrastructure (e.g., performing updates, inventorying assets on their network, and ensuring proper network use). Congress may exercise oversight to ensure that agencies are able to fulfill their required operations securely, while employing increased telework capabilities.
- **Interagency Collaboration.** Federal agencies have forums[49] and requirements[50] to share cybersecurity information. Congress has taken action to require changes in the ways federal agencies engage with each other on cybersecurity threats.[51] Despite these preventive efforts, risks to federal IT are increasing.[52] Recent adoption of telework has shifted the risk landscape. Some agencies may be adapting to those changes while others are struggling with or unaware of their security posture. Congress may see additional need to review and change agency requirements to share information on cybersecurity risks and strategies to mitigate those risks. Additionally, Congress could choose to require agencies to adopt certain risk management strategies that have been successfully deployed at other agencies.
- **Cybersecurity Investments.** There has been a market trend away from organization-owned and -controlled computing resources towards mobile, cloud, and leased computing resources—a trend that the federal government is embracing. The Federal Chief Information Officer published a strategy to drive cloud adoption at federal agencies,[53] and Congress passed a law encouraging agencies to seek cloud services as they modernized legacy agency systems.[54] Cloud computing's offsite facilities may present new or altered security risks for organizations that adopt them. As agencies are implementing increased telework, they are also experiencing different stresses and demands on their IT security

had on internet infrastructure. While these may be pertinent questions for policymakers, they are unrelated to the cybersecurity of federal agency networks, and thus not discussed here.

[47] Lauren C. Williams, "DOD Faces Network Attacks amid Telework Uptick," *FCW*, March 16, 2020, at https://fcw.com/articles/2020/03/16/dod-telework-cyber-attacks.aspx.

[48] Mark Rockwell, "Telework Tests Await Networks, Federal Agencies," *FCW*, March 13, 2020, at https://fcw.com/articles/2020/03/13/telework-uptick-risks-rockwell.aspx.

[49] Two examples are incident reporting through the United States Computer Emergency Readiness Team (https://www.us-cert.gov/report) and the Federal Chief Information Officer Council (https://www.cio.gov/).

[50] Office of Management and Budget, "Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements," *M-20-04*, November 19, 2019, at https://www.whitehouse.gov/wp-content/uploads/2019/11/M-20-04.pdf.

[51] P.L. 114-113, Division N—The Cybersecurity Act of 2015. Section 103 requires the timely sharing of classified and unclassified cyber threat information among federal entities, and among nonfederal entities when appropriate. The government implemented this requirement through a computer-based, automated information sharing system. Congress tasked the Director of National Intelligence, Secretary of Homeland Security, the Secretary of Defense, and the Attorney General with developing procedures for that information sharing. These procedures may be found online at https://www.us-cert.gov/ais.

[52] U.S. Government Accountability Office, "High Risk Series: Urgent Actions are Needed to Address Cybersecurity Challenges Facing the Nation," GAO-18-645T, July 25, 2018, at https://www.gao.gov/products/GAO-18-645T.

[53] Suzette Kent, "Federal Cloud Computing Strategy," strategy, June 24, 2019, at https://www.whitehouse.gov/wp-content/uploads/2019/06/Cloud-Strategy.pdf.

[54] The Modernizing Government Technology Act, Subtitle G of P.L. 115-91.

- infrastructure. Congress may choose to use this information to guide future agency appropriations or cybersecurity authorizations.

Author Information

Chris Jaikaran
Analyst in Cybersecurity Policy

Disclaimer