TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Cybersecurity and Telework During the COVID-19 Pandemic

December 17, 2021

Report Number: 2022-20-007

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta

HIGHLIGHTS: Cybersecurity and Telework During the COVID-19 Pandemic

Final Audit Report issued on December 17, 2021 **Report Number 2022-20-007**

Why TIGTA Did This Audit

The U.S. House of Representatives Committee on Oversight and Reform requested the Department of the Treasury Office of Inspector General identify any vulnerabilities created or exacerbated by the Department of the Treasury's use of remote access software to facilitate telework during the Coronavirus Disease 2019 (COVID-19) pandemic and whether any such vulnerabilities were effectively mitigated. TIGTA coordinated with the Office of Inspector General and completed this review to address the Committee's request relative to the IRS.

Our overall objective was to review cybersecurity related to IRS telework during the COVID-19 pandemic.

Impact on Taxpayers

The United States has recently been the target of several high-profile cyberattacks. As cybersecurity threats against the Federal Government and other entities continue to grow, protecting the confidentiality of taxpayer information continues to be a top concern for the IRS.

What TIGTA Found

The IRS stated it did not acquire new remote connections software to support telework during the COVID-19 pandemic but did purchase additional licenses. In March 2020, approximately 26,000 IRS employees were teleworking. As of September 2020, nearly 60,700 employees were teleworking. Remote access to IRS systems is allowed via a virtual private network, and IRS policy requires two-factor authentication. The IRS received and allocated $37 million for equipment and licenses for teleworking employees.

The IRS stated it uses or plans to start using several collaboration platforms, such as Zoom for Government and Cisco WebEx, to connect internal and external stakeholders virtually. Utilizing these applications minimized the impact of the COVID-19 pandemic but also increased the potential for data breaches and unauthorized disclosure.

The IRS stated that, for meetings supported by Zoom for Government and Cisco WebEx, participants could only attend by a direct invitation from the IRS host. In addition, file sharing was disabled for both platforms. The IRS is also working to complete its testing of Microsoft Teams and is beginning the implementation with a small group of pilot users in the production environment. The IRS had guidance in place to prevent the unauthorized dissemination of Controlled Unclassified Information, Personally Identifiable Information, and Sensitive But Unclassified information.

The IRS stated in September 2020, it implemented a scalable information technology asset management program, which improved the accuracy of compliance and other internal inventory reporting needs. This asset management program matured its capabilities to provide visibility into asset data by integrating additional configuration and asset inventory data of laptop computers, virtual workstations, and Personal Digital Assistants.

The IRS waived the requirement for employees to have an approved telework agreement and encouraged, but did not require, new teleworkers to complete the telework training program. While these telework policies will be waived through March 23, 2022, the IRS stated it will reassess periodically and may lift the waiver earlier.

The IRS has continuous monitoring and network scanning in place to identify vulnerabilities, and these processes were not impacted by the transition to telework. The IRS performs vulnerability scanning six days a week, and the scan results are ingested into an analytics and reporting tool, providing stakeholders continuous visibility into vulnerability data about their assets. The IRS has various network management programs, including configuration compliance scanning, audit log management, incident monitoring, and malicious code detection.

What TIGTA Recommended

TIGTA made no recommendations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

December 17, 2021

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

M. Weir for

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Cybersecurity and Telework During the COVID-19 Pandemic (Audit # 202220022)

This report presents the results of our review of cybersecurity related to Internal Revenue Service (IRS) telework during the Coronavirus Disease 2019 pandemic. This audit is in response to a request from the U.S. House of Representatives Committee on Oversight and Reform to the Department of the Treasury Office of Inspector General and does not include any recommendations. This review is part of our Fiscal Year 2022 Annual Audit Plan and addresses the major management challenge of *Enhancing Security of Taxpayer Data and Protection of IRS Resources*.

Copies of this report are also being sent to the IRS managers affected by the information in the report. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Background

The Federal Information Security Modernization Act of 2014 (FISMA)[1] requires inspectors general to conduct an annual evaluation of cybersecurity policies and practices of their respective departments and agencies. In June 2021, the U.S. House of Representatives Committee on Oversight and Reform[2] requested that an assessment of any vulnerabilities created or exacerbated by the Department of the Treasury's use of remote access software to facilitate telework during the Coronavirus Disease 2019 (COVID-19) pandemic, and whether any such vulnerabilities were effectively mitigated, be included with the annual FISMA reporting.[3] The request was addressed to the Department of the Treasury Office of Inspector General and recommended that the work be performed as a part of the annual FISMA assessment. We coordinated with the Office of Inspector General and completed this review to address the Committee's request relative to the Internal Revenue Service (IRS). Due to the scope of the work requested, we performed an audit separate from our FISMA audit[4] work to address the Committee's concerns.

The Federal Government adopted the widespread use of virtual private networks[5] (VPN) and other remote access technologies to facilitate continuity of operations and allow agencies to continue to serve the Nation throughout a deadly pandemic. However, this environment created additional cybersecurity vulnerabilities that could jeopardize the integrity of Federal information technology networks. The National Institute of Standards and Technology stated that major security concerns associated with telework include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, and the availability of internal resources to external hosts.[6]

The proliferation and growing sophistication of malicious state and nonstate cyber actors requires Federal agencies to be able to maintain and protect the integrity of their information technology systems—particularly if they adopt more flexible telework policies after the COVID-19 pandemic subsides.

[1] Pub. L. No. 113–283 (2014); 44 U.S.C. § 3555.

[2] See Appendix II for a copy of the Congressional Request letter.

[3] According to the Telework Enhancement Act of 2010 (Pub. L. No. 111–292 (2010)), the term 'telework' or 'teleworking' refers to a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work. On March 17, 2020, in response to the COVID-19 pandemic, the Office of Management and Budget directed U.S. departments and agencies to maximize telework. Office of Management and Budget, *Federal Agency Operational Alignment to Slow the Spread of Coronavirus COVID-19* (Mar. 17, 2020).

[4] Treasury Inspector General for Tax Administration, Report No. 2021-20-072, *Fiscal Year 2021 IRS Federal Information Security Modernization Act Evaluation* (Sept. 2021).

[5] See Appendix III for a glossary of terms.

[6] National Institute of Standards and Technology, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device Security* (July 2016).

Results of Review

Acquisition, Deployment, and Management of Remote Access Tools

Remote connections

The IRS stated that it did not acquire new remote connections software to support telework during the COVID-19 pandemic and instead only purchased additional licenses. The Enterprise Remote Access Project, operational since 2004, is the IRS's VPN solution for remote network access. It provides IRS employees the ability to securely connect to the IRS network while working remotely. The application uses security protocols to establish a secure remote connection to one of the three IRS Treasury Internet Connection sites. The user account is authenticated before access to the network is granted. The Enterprise Remote Access Project provides a VPN-based remote access solution that meets the remote access requirements of all IRS employees and approved contractors. The IRS reported[7] that it completed upgrades to double the bandwidth capacity to support 60,000 employees working remotely by the end of Fiscal Year 2020.

The Internal Revenue Manual (IRM) stated the policy regarding remote connections and VPNs prior to the pandemic, including authorization of remote access to information systems prior to allowing the connection, requiring the use of two-factor authentication, and providing remote access via the IRS-approved VPN.[8] The IRS has since made minor editorial updates to the IRM.

In September 2021, the Government Accountability Office issued a report[9] from which we concluded[10] that the IRS:

- Utilized a VPN and had established methods for employees to log in to agency systems and services remotely.
- Documented elements of a telework security policy, all relevant security controls and enhancements, and that it had assessed all of the relevant security controls and enhancements for protecting its systems that provide remote access.
- Demonstrated that it consistently monitored progress toward completing remedial actions for any identified weaknesses.

In March 2021, we issued an interim report[11] stating that, prior to the pandemic (between October 2019 and early March 2020), the IRS had an average of 26,000 employees teleworking approximately 22 hours per week. By September 2020, nearly 60,700 employees were

[7] IRS, Publication No. 5453, *Information Technology Annual Key Insights Report: Fiscal Year 2020 Successes and Accomplishments* (2021).

[8] IRM 10.8.1.4.1.16 (May 9, 2019).

[9] Government Accountability Office, GAO 21-583, *Selected Agencies Overcame Technology Challenges to Support Telework but Need to Fully Assess Security Controls* (Sept. 2021).

[10] The Government Accountability Office identified the audited agencies that were not meeting the listed standards, indicating that the agencies not specifically identified had met the standard.

[11] Treasury Inspector General for Tax Administration, Report No. 2021-IE-R002, *Interim Report – The IRS Leveraged Its Telework Program to Continue Operations During the COVID-19 Pandemic* (Mar. 2021).

teleworking an average of 36 hours per week. The number of teleworkers and average hours worked per week have remained relatively consistent from September 2020 through June 2021.

Collaboration platforms

The IRS stated that it utilizes or has plans to start utilizing several collaboration platforms to connect internal and external stakeholders virtually, including Skype for Business, Cisco WebEx, Saba Meeting, Zoom for Government (ZoomGov), and Microsoft Teams. The use of such applications allowed the IRS to minimize the impact of the COVID-19 pandemic; however, it also increased the potential for data breaches and unauthorized disclosure.

The IRS stated in the Fiscal Year 2020 Information Technology Annual Key Insights Report that it deployed Cisco WebEx to resume national settlement days virtually. The IRS stated that the Cisco WebEx platform can support 800 users per server license and that it has 1,495 Martinsburg server licenses and 640 Memphis server licenses.

In September 2020, the IRS stated that it purchased 1,100 Zoom Professional licenses, and it deployed ZoomGov to all IRS workstations. The User and Network Services function's ZoomGov team manages the administration of the application, including user roles. The application is implemented using Single Sign On, which is by default a multifactor authentication mechanism. In the Fiscal Year 2020 Information Technology Annual Key Insights Report, the IRS also reported that it delivered ZoomGov to enable IRS Chief Counsel to participate in virtual court sessions. The IRS stated that for the ZoomGov platform it has:

- 1,050 Professional Licenses which can each host 500 users.
- 50 Professional License Large Meeting licenses which can each host 1,000 users.

The IRS is working to complete its testing of Microsoft Teams. It is beginning the implementation of Teams with a small group of pilot users in the production environment. The Cybersecurity function and the Privacy, Governmental Liaison, and Disclosure Office are partners in the implementation of Teams. Together, they are working to create a secure, protected environment. The Teams product was included in the Office 365 subscriptions and purchased in 2019. The Strategy and Planning function holds the Microsoft Enterprise Licensing Agreement. The IRS stated that its Applications Development function reviewed the Slack product, but that the IRS did not acquire it.

Security of collaboration platforms

The IRS stated that, for meetings supported by both ZoomGov and Cisco WebEx, participants can only attend by a direct invitation from the IRS host. In addition, file sharing is disabled for both platforms. The IRS had existing guidance in the IRM to prevent the unauthorized dissemination of Controlled Unclassified Information, Personally Identifiable Information (PII), and Sensitive but Unclassified (SBU) information. The policies state that:

- All collaborative technology must be approved by the appropriate authorizing official following an assessment of risk with mitigation.
- E-mail messages, appointments, and other collaborative mechanisms containing confidential data must be encrypted when transmitted and stored.

Access management

The IRS stated that it used two-factor authentication since 2005. It initially started using grid cards for two-factor authentication but is now using smart cards with a Personal Identification Number for access. Prior to the COVID-19 pandemic, the IRM required two-factor authentication for all remote access to an IRS system and that systems must monitor and control remote access methods. Personal Identity Verification cards are used to authenticate users on a VPN. The IRS stated that, in the event of a Personal Identity Verification card failure, the user is granted temporary access to a secure site to obtain a grid card. To accommodate potential Personal Identity Verification card failures, the IRS purchased 40,000 additional grid card licenses. Procedures are in place to remove inactive accounts and for emergency removal of accounts when a user is no longer authorized to have one. From March 15, 2020, through October 27, 2021, 350 unauthorized user accounts and more than 16,000 inactive user accounts were removed from IRS system access.

In August 2020, we reported[12] that the IRS had effective strategies and protocols to authenticate network user identities, but additional work was needed to authenticate devices. In the report, we found that not all of the devices accessing the IRS network through a VPN were authenticated. We asked the IRS about the current status of the device authentication solution. The IRS responded that the device solution has been delayed due to challenges with the vendor.

Distribution and Management of Virtual and Physical Assets

The IRS stated that, in September 2020, the Information Technology Asset Management Program implemented a scalable data integration and analytics platform, which improved the accuracy of compliance and other internal inventory reporting needs. In addition, the Information Technology Asset Management Program operationalized a data remediation process and tool to improve overall asset data quality. In Calendar Year 2021, the Information Technology Asset Management Program matured these capabilities by integrating additional configuration and asset inventory data of assets such as laptop computers, virtual workstations, and Apple micro–Personal Digital Assistants.

According to the IRS, the Hardware Asset Management team manages the physical hardware assets, including laptop computers and smartphones, throughout their life cycles in the Knowledge, Incident/Problem Service Asset Management Asset Manager Database. Inventory transactional updates are reported to the Hardware Asset Management team as asset movement occurs. The Knowledge, Incident/Problem Service Asset Management Asset Manager does not track employees who are teleworking. Assets assigned to teleworking employees are designated with the employee's Place of Duty on record.

The IRS also stated that the Logistics Management team manages the distribution of assets and virtual workstations, including the distribution and provisioning of physical and virtual devices through the Knowledge, Incident/Problem Service Asset Management Database's authoritative source inventory transactions. The IRS reported in the Fiscal Year 2020 Information Technology Annual Key Insights Report that, through the ***Depot to Home*** initiative, laptop computers were

[12] Treasury Inspector General for Tax Administration, Report No. 2020-20-036, *Strategies and Protocols to Authenticate Network User Identities Are Effective; However, More Action Is Needed to Verify the Identity of Devices* (Aug. 2020).

shipped directly to more than 2,000 employees. The IRS stated that it accounted for all laptop computer shipments and no shipments resulted in permanent loss.

In our March 2021 interim report, we stated that, by May 2020, the IRS distributed more than 12,600 laptop computers and nearly an additional 6,000 by October 2020. No details were provided on smartphones or other information technology–related equipment. Our report also indicated that growth of telework during this period was limited by the IRS's ability to identify, prioritize, and issue laptop computers and other information technology equipment to employees who previously had not participated in the telework program.

The IRS stated that, in July 2020, it received approximately $1.6 million to procure desktop and portable printers and monitors. In September and October 2020, the IRS issued product awards for nearly 5,000 printers and more than 1,700 monitors. The equipment began arriving in February 2021. By August 31, 2021, all of the printers were delivered, while all but three monitors were delivered by October 31, 2021.

The IRS also reported that, in December 2020, it received nearly $2 million of additional funding for desktop and portable printers. In April 2021, the IRS issued the second product award, and items began arriving at the end of that month. During this time, employees requested more than 9,800 printers. As of October 15, 2021, 5,543 (57 percent) of the 9,780 printers ordered from the vendor were received. An additional 4,237 printers are awaiting delivery from the vendor.

In May 2021, we issued another interim report[13] that identified a spend plan in May 2020 allocating $35 million to Continuity of Operations for costs associated with purchasing laptop computers, wireless devices, and software licenses in support of employees teleworking. A September 2020 amendment to the spend plan separated Continuity of Operations into $22 million funded by the Coronavirus Aid, Relief, and Economic Security Act[14] and $15 million funded by the Families First Coronavirus Response Act.[15] The September 2020 quarterly report on actual expenditures reported that more than half of the total funds had been spent but did not provide details on expenditures in each area.

Remote Access Telework Security Policies and Operations

Security policy changes for telework

The IRS stated that information technology security policy is set at an organizational and system level and that there were no updates to the security policies specific to the COVID-19 pandemic. However, a June 2021 memorandum provided guidance on several items, including the connection of personally owned and non-Government–furnished equipment to IRS systems and network. The IRS also issued several operational updates regarding telework, which included:

- Teleworking from a vehicle with a wireless Internet connection – The IRS stated that vehicles generally do not provide reasonable security and protection of Government

[13] Treasury Inspector General for Tax Administration, Report No. 2021-16-026, *Interim Report – Status of Coronavirus Response Funding* (May 2021).

[14] Pub. L. No. 116-136 (Mar. 27, 2020).

[15] Pub. L. No. 116-127 (Mar. 18, 2020).

equipment and data. If an employee is working with taxpayer data in their vehicle, there is a risk that bystanders could see through the vehicle's windows, which could allow for inadvertent disclosure of PII.

- Disposal and destruction of waste material containing PII or SBU data – The operational requirements stated that under no circumstance can employees burn paper with PII or SBU data and information at their telework locations. In addition, employees under no circumstance are permitted to use non-Government equipment (such as shredders) to process IRS data. Further, the IRS requires employees while teleworking to bring paper with SBU data into the office for proper disposal. Employees are also required to keep paper with PII and SBU data secure in a locked receptacle. Finally, employees must protect PII and SBU data in transit during transport to the office for proper disposal.

The Privacy, Governmental Liaison, and Disclosure Office published a Privacy and Records Telework Policy checklist. This included the requirements to follow a Clean Desk Policy while on telework, use IRS e-mail accounts to conduct official IRS business, and immediately report any breach of sensitive information or record loss.

Our March 2021 interim report stated that the IRS waived the requirement for employees to have an approved telework agreement and encouraged, but did not require, new teleworkers to complete the telework training program. The Human Capital Office stated that the IRS waived several other telework policies. On September 30, 2021, the IRS extended the waiver of telework policies through March 23, 2022. The IRS stated that it plans to reassess the situation periodically and may lift the waiver earlier. It would provide employees with at least 30 days advance notice before requiring them to return to the office.

Continuous monitoring

The IRS stated that it has continuous monitoring and network scanning in place to identify vulnerabilities and that these processes were not impacted by the IRS's transition to telework. The IRS performs vulnerability scanning six days a week, and the scan results are ingested into an analytics and reporting tool, providing stakeholders continuous visibility into vulnerability data about their assets. The IRS has various network management programs, including configuration compliance scanning, audit log management, incident monitoring, and malicious code detection.

In its September 2021 report, the Government Accountability Office concluded that the IRS has:

- Assessed all of the relevant security controls and enhancements for protecting its systems that provide remote access.
- Demonstrated that it consistently monitored progress toward completing remedial actions for any identified weaknesses.

In September 2021, we reported[16] that the IRS purchased and deployed an Endpoint Detection and Response solution, which analyzes various items such as processes running on workstations, memory artifacts, and other data points. As of September 21, 2021, 86,593 (98 percent) of the eligible 88,595 workstations had a successful deployment of the Endpoint Detection and

[16] Treasury Inspector General for Tax Administration, Report No. 2021-20-065, *The Endpoint Detection and Response Solution Has Been Deployed to Most Workstations and Is Operating As Intended, but Improvements Are Needed* (Sept. 2021).

Response solution. The collected data are correlated and compared to rules that have been established or associated with known indicators of compromise. If anything is detected, an alert is generated. We found that the alerts generated were properly tracked and worked. No alerts in the sample period were elevated to an incident.

Network protection

The IRS fully implemented the Common Communication Gateway, which was approved by the Department of Homeland Security to be a Trusted Internet Connection up to version 2.0. According to the IRS, there are no identified and approved use cases for Trusted Internet Connection version 3.0. Until the version 3.0 standard is finalized and the IRS receives direction from the Department of the Treasury, the IRS will continue with the traditional use case and the version 2.0 implementation.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to review cybersecurity related to IRS telework during the COVID-19 pandemic, as requested by the U.S. House of Representatives Committee on Oversight and Reform. To accomplish this objective, we:

- Reviewed our related audit reports and those issued by the Government Accountability Office as well as relevant IRS policy and documentation, *e.g.,* the IRM and the Information Technology Annual Key Insights Report.
- Requested and reviewed information from IRS personnel within the Cybersecurity and the User and Network Services functions to determine whether the IRS implemented and monitored security controls over networks, hardware, and software used to facilitate telework.

Performance of This Review

This review was performed with information obtained from the IRS Information Technology organization's Cybersecurity and User and Network Services functions' management offices, located in the New Carrollton Federal Building in Lanham, Maryland, and the IRS Headquarters in Washington, D.C., during the period of September through November 2021. We conducted this performance audit 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Jena Whitley, Director; Myron Gulley, Audit Manager; Mark Carder, Lead Auditor; Daniel Preko, Senior Auditor; and Danielle Synnestvedt, Auditor.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: the IRM Cybersecurity policies and procedures, including telework policies set in place prior to the pandemic and any interim communication, and the IRM privacy policies and procedures, including data protection and its importance as a primary telework consideration. We evaluated these controls by interviewing Cybersecurity function personnel; Privacy, Governmental Liaison, and Disclosure Office personnel; and the Treasury Inspector General for Tax Administration's Office of Inspections and Evaluations personnel about their work in the area of the IRS's pandemic preparedness as it relates to telework. We also reviewed relevant documentation.

Appendix II

Congressional Request Letter

CAROLYN B. MALONEY, NEW YORK
CHAIRWOMAN

ONE HUNDRED SEVENTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5051
MINORITY (202) 225–5074

https://oversight.house.gov

JAMES COMER, KENTUCKY
RANKING MINORITY MEMBER

June 2, 2021

Mr. Richard K. Delmar
Acting Inspector General
Department of the Treasury
1500 Pennsylvania Avenue, N.W.
Washington, D.C. 20220

Dear Acting Inspector General Delmar:

The Federal Information Security Modernization Act of 2014 (FISMA) requires inspectors general appointed under the Inspector General Act of 1978 to conduct an annual evaluation of the cybersecurity policies and practices of their respective departments and agencies.[1] We write today to encourage you, in your office's forthcoming annual evaluation of the information security program at the Department of the Treasury, to include an assessment of any vulnerabilities created or exacerbated by the Department's use of remote-access software to facilitate telework during the coronavirus pandemic, and whether any such vulnerabilities were effectively mitigated.[2]

The United States has recently been the target of several high-profile cyber attacks, including through the compromise of the SolarWinds Orion platform and on-premises Microsoft Exchange servers.[3] On April 20, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) confirmed an announced that Pulse Connect, a remote-access software used widely by government agencies, had been breached.[4] *The Washington Post* reported that "Chinese

[1] Pub. L. No. 113–283 (2014); 44 U.S.C. §3555.

[2] According to the Telework Enhancement Act of 2010, "[t]he term 'telework' or 'teleworking' refers to a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work." Pub. L. No.111–292 (2010). On March 17, 2020, in response to the coronavirus pandemic, the Office of Management and Budget directed U.S. departments and agencies to maximize telework. Office of Management and Budget, *Federal Agency Operational Alignment to Slowthe Spread of Coronavirus COVID-19* (Mar. 17, 2020) (online at www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf).

[3] Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (online at https://us-cert.cisa.gov/ncas/alerts/aa20-352a); Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromiseof Microsoft Exchange Server* (Mar. 10, 2021) (online at https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server).

[4] Cybersecurity and Infrastructure Security Agency, *Exploitation of Pulse Connect Secure Vulnerabilities* (Apr. 20, 2021) (AA21-110A) (online at https://us-cert.cisa.gov/ncas/alerts/aa21-110a) (confirming an "a ctive exploitation of vulnerabilities in Pulse Connect Secure products, a widely used remote access solution.").

government hackers are believed to have compromised dozens of U.S. government agencies" through the Pulse Connect breach.[5]

The widespread use of virtual private networks (VPNs) and other remote-access technologies to facilitate continuity of operations across the federal government allowed federal agencies to continue to serve the nation throughout a deadly pandemic but also created additional cybersecurity vulnerabilities that could jeopardize the integrity of federal information technology networks.

Even before the pandemic began, the National Institute of Standards and Technology warned that "major security concerns" associated with telework "include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, and the availability of internal resources to external hosts."[6]

The proliferation and growing sophistication of malicious state and non-state cyber actors requires federal departments and agencies to be able to maintain and protect the integrity of their information technology systems—particularly if they adopt more flexible telework policies after the coronavirus pandemic subsides.[7]

To that end, as part of your annual Department of the Treasury FISMA cybersecurity evaluation for fiscal year 2021, we recommend that your office examine:

- The acquisition, deployment, management, and security of remote connections to Department networks, including those facilitated by VPNs and/or virtual network controllers ;
- The acquisition, deployment, management, and security of collaboration platforms such as Microsoft Teams, Zoom, Slack, and Cisco Webex;
- Whether the Department, and all components, has implemented security controls to prevent the unauthorized dissemination of controlled unclassified information, personally identifiable information, or sensitive but unclassified information via third-party collaboration platforms;

[5] *Chinese Hackers Compromise Dozens of Government Agencies, Defense Contractors*, Washington Post (Apr. 21, 2021) (online at www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac_story.html).

[6] National Institute of Standards and Technology, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* (July 2016) (online at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf).

[7] Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (AA20-352A) (online at https://us-cert.cisa.gov/ncas/alerts/aa20-352a); Federal Bureau of Investiga tion and Cybersecurity and Infrastructure Security Agency, *FBI-CISA Joint Advisory on Compromiseof Microsoft Exchange Server* (Mar. 10, 2021) (online at https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server).

- The identity, credential, and access management of users that permit remote access to Department networks, including the extent to which the Department has enabled multi-factor authentication and implemented procedures to disable inactive and potentially unauthorized user accounts;

- The distribution and management of virtual and physical assets that facilitate telework, including laptop computers, smartphones, and RSA tokens;

- The Department's adherence to Trusted Internet Connection 3.0 guidance;[8]

- Whether the Department's chief information officer and all component chief information officers implemented additional security policies in response to coronavirus-related telework and how they are enforcing those policies; and

- Whether the Department has implemented continuous monitoring and scanning of networks to identify vulnerabilities.

The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X.

If you have any questions regarding this request, please contact Committee staff at (202) 225-5051. Thank you for your prompt attention to this important matter.

Sincerely,

Carolyn B. Maloney
Chairwoman
Committee on Oversight and Reform

Stephen F. Lynch
Chairman
Subcommittee on National Security

Gerald E. Connolly
Chairman
Subcommittee on Government Operations

Raja Krishnamoorthi
Chairman
Subcommittee on Economic and Consumer Policy

[8] Cybersecurity and Infrastructure Security Agency, *TIC 3.0 Core Guidance Documents* (accessed on Apr. 22, 2021) (online at www.cisa.gov/publication/tic-30-core-guidance-documents).

Jamie Raskin
Chairman
Subcommittee on Civil Rights and
Civil Liberties

Ro Khanna
Chairman
Subcommittee on Environment

cc: The Honorable James Comer, Ranking Member
Committee on Oversight and Reform

The Honorable Glenn Grothman, Ranking Member
Subcommittee on National Security

The Honorable Jody Hice, Ranking Member
Subcommittee on Government Operations

The Honorable Michael Cloud, Ranking Member
Subcommittee on Economic and Consumer Policy

The Honorable Pete Sessions, Ranking Member
Subcommittee on Civil Rights and Civil Liberties

The Honorable Ralph Norman, Ranking Member
Subcommittee on Environment

Ms. Allison C. Lerner, Chair
Council of the Inspectors General on Integrity and Efficiency

The Honorable Mark Lee Greenblatt, Vice Chair
Council of the Inspectors General on Integrity and Efficiency

The Honorable Hannibal "Mike" Ware, Chair
Audit Committee, Council of the Inspectors General on Integrity and Efficiency

The Honorable Cathy L. Helm, Vice Chair
Audit Committee, Council of the Inspectors General on Integrity and Efficiency

Appendix III

Glossary of Terms

Term	Definition
Audit Log	A chronological record of information system activities, including records of system accesses and operations performed in a given period.
Common Communication Gateway	The demilitarized zone, which provides Internet connectivity and external data connectivity to Federal, State, and local government agencies and tax partners.
Continuous Monitoring	The process implemented to maintain a current security status for one or more information systems on which the operational mission of the enterprise depends. The process includes: 1) the development of a strategy to regularly evaluate selected information assurance controls and metrics; 2) recording and evaluating relevant events and the effectiveness of the enterprise in dealing with those events; 3) recording changes to controls or changes that affect risks; and 4) publishing the current security status to enable information-sharing decisions involving the enterprise.
Controlled Unclassified Information	A designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, *Classified National Security Information* (April 17, 1995), as amended March 25, 2003, but 1) is pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government and 2) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation Controlled Unclassified Information replaces "Sensitive But Unclassified."
Demilitarized Zone	A network segment inserted as a "neutral zone" between an organization's private network and the Internet.
Encrypted	The process of converting plain text to cipher text by means of a cryptographic system.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.
Grid Card	A method of identifying users in which the user is asked to input a series of characters based on a preregistered pattern on a grid (that the user knows) and a grid of pseudo-random characters generated by the authenticator. This method results in a different series of characters each time the user authenticates.
Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Term	Definition
Multifactor Authentication	Verifying the identity of a user, process, or device using two or more factors to achieve authentication, often as a prerequisite to allowing access to resources in an information system. Factors include: 1) something you know, *e.g.,* password/Personal Identification Number; 2) something you have, *e.g.,* cryptographic identification device, token; or 3) something you are, *e.g.,* biometric.
National Settlement Days	A program in which the IRS spends certain days 1) coordinating efforts that aim to resolve/settle cases in U.S. Tax Court and 2) coming to a settlement agreement with taxpayers who owe back taxes.
Personal Identification Number	A short numeric password (six to eight digits) used as an authenticator by the Personal Identity Verification card to authenticate the cardholder.
Personal Identity Verification Card	A Government-issued identity credential that contains a contact and a contactless chip. The cardholder's facial image is printed on the card along with other identifying information and security features that can be used to authenticate the user for physical access to Federally controlled facilities and logical access to Federally controlled information systems.
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, and biometric records, alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth and mother's maiden name.
Sensitive But Unclassified	Any information that requires protection due to the risk and magnitude of loss or harm to the IRS or the privacy to which individuals are entitled under 5 U.S.C. § 552a (the Privacy Act of 1974), which could result from inadvertent or deliberate disclosure, alteration, or destruction.
Slack Product	A messaging application for business that connects people to the information they need by way of dedicated spaces called channels (*i.e.,* regardless of your location, time zone, or function).
Smart Card	A plastic card about the size of a credit card, with an embedded microchip that can be loaded with data.
Trusted Internet Connection	A Federal initiative for which the primary goals are to consolidate and secure Federal agency external connections using a common set of security controls and to improve the Federal Government's incident response capability.
Virtual Private Network	A secure way of connecting to a private Local Area Network at a remote location, using the Internet or any insecure public network to transport the network data packets privately, using encryption.

Appendix IV

Abbreviations

COVID-19	Coronavirus Disease 2019
FISMA	Federal Information Security Modernization Act of 2014
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
PII	Personally Identifiable Information
SBU	Sensitive But Unclassified
VPN	Virtual Private Network

To report fraud, waste, or abuse,
call our toll-free hotline at:

(800) 366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration

P.O. Box 589

Ben Franklin Station

Washington, D.C. 20044-0589

Information you provide is confidential, and you may remain anonymous.