Report No. DODIG-2021-064

~~CUI~~

INSPECTOR GENERAL

U.S. Department of Defense

MARCH 29, 2021

Audit of Maintaining Cybersecurity in the Coronavirus Disease–2019 Telework Environment

~~Controlled by: DoD OIG~~
~~Controlled by: Audit~~
~~CUI Category: DoD Critical Infrastructure Security Information~~
~~Distribution/Dissemination Control: FEDCON~~
~~POC:~~ [redacted]

INTEGRITY ★ INDEPENDENCE★ EXCELLENCE

~~CUI~~


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Results in Brief

Audit of Maintaining Cybersecurity in the Coronavirus Disease–2019 Telework Environment

March 29, 2021

Objective

The objective of this audit was to determine whether DoD Components maintained network protections during the coronavirus disease–2019 (COVID-19) pandemic while the DoD workforce maximized the use of telework capabilities to ensure the continuity of DoD operations.

Background

On March 11, 2020, the World Health Organization characterized the COVID-19 outbreak as a pandemic. In response to the COVID-19 pandemic, on March 27, 2020, the Secretary of Defense directed DoD Components to maximize telework to ensure the continuity of DoD operations. Most teleworkers remotely access agency networks using computing devices, such as laptops, tablets, and desktop computers from external locations other than the employee's official worksite. Telework and remote access solutions must provide confidentiality, integrity, and availability of DoD data on an organization's networks. DoD personnel can gain access to their organization's network using approved technologies, such as a virtual private network (VPN) or a virtual desktop infrastructure.

In March 2020, the DoD established the DoD Telework Readiness Task Force, led by the DoD Chief Information Officer (CIO), to ensure DoD networks remain telework-ready and secure to support DoD missions during the maximum telework period. The Task Force issued memorandums

Background (cont'd)

to DoD Components that provided best practices for ensuring cybersecurity when teleworking, such as guidance for maintaining the cybersecurity of DoD networks and using capabilities on DoD-issued laptops to maximize the telework environment.

Finding

The DoD Components we assessed did not consistently implement required cybersecurity controls to protect DoD networks during maximum telework. Specifically,

- ~~(FOUO)~~ network administrators for the Army, Navy, Air Force, and the DLA inconsistently [redacted] because language in the DISA VPN Security Requirement Guide does not clearly specify when DoD Components should [redacted];
- ~~(FOUO)~~ network administrators for the Army and Air Force did not [redacted] or develop plans of action and milestones for [redacted];
- ~~(FOUO)~~ account administrators for the Navy did not disable and remove inactive user accounts after [redacted] because the Commander, U.S. Fleet Cyber Command [redacted];
- ~~(FOUO)~~ the DoD Deputy Chief Information Officer for Information Enterprise, Cloud Computing Program Office, [redacted]

Results in Brief

Audit of Maintaining Cybersecurity in the Coronavirus Disease–2019 Telework Environment

Finding (cont'd)

~~(FOUO)~~ [redacted].

- Army, Navy, and Air Force personnel teleworked without approved telework agreements or required telework training because, according to Component officials, some supervisors were unaware of the supervisor responsibilities for telework or were overwhelmed with other duties during the COVID-19 pandemic.

Telework and remote access technologies require additional protection from malicious cyber actors because they receive higher exposure to external threats than technologies accessed by personnel physically located inside of the organization's facilities. Because the DoD Components that we assessed did not fully implement security controls to maintain cybersecurity in a maximum telework environment as outlined in National Institute of Standards and Technology, and DoD policies and guidance, DoD Components are at a higher risk of becoming victims to cyber attacks that could threaten the safety of the warfighter and the security of the United States.

Recommendations

Among other recommendations, we recommend that the DoD CIO:

- ~~(CUI)~~ direct the Defense Information Systems Agency to review the VPN Security Requirements Guide and add specific language that [redacted], and
- ~~(CUI)~~ direct the DoD Deputy CIO for Information Enterprise to implement security controls to [redacted].

In addition, we recommend that the CIOs for:

- ~~(FOUO)~~ the Air Force develop and implement a plan to [redacted]; and
- ~~(CUI)~~ the Navy direct the Commander, U.S. Fleet Cyber Command to identify mitigating efforts for preventing malicious cyber actors from exploiting inactive user accounts older than [redacted].

Management Comments and Our Response

The following include some of the management comments received.

~~(CUI)~~ The DoD CIO, disagreed with the recommendation to revise the VPN Security Requirements Guide, stating DISA concluded that adding language to [redacted] could have a negative impact on the organizations within the DoD. However, the DoD CIO did not provide additional information detailing [redacted]. Therefore, we cannot conclude on [redacted], in fact, have a negative impact on DoD Components. The DoD CIO should provide additional comments describing how DISA determined [redacted] could negatively impact organizations within the DoD.

Results in Brief

Audit of Maintaining Cybersecurity in the Coronavirus Disease–2019 Telework Environment

Comments (cont'd)

~~(FOUO)~~ In addition, the DoD CIO stated that he would direct the DoD Deputy CIO for Enterprise to implement [redacted]. Therefore, the recommendation is resolved but will remain open until the DoD CIO provides documentation showing the direction given to the DoD Deputy Chief Information Officer for Information Enterprise, such as a signed and dated memorandum, to [redacted].

~~(CUI)~~ The Commander, U.S. Fleet Cyber Command, reconsidered his decision to [redacted] and to [redacted] to Navy and Defense Information Systems Agency policies. Therefore, the recommendation is resolved but will remain open until the Commander provides documentation showing that network administrators configured group policies to disable or remove user accounts after [redacted] of inactivity.

~~(CUI)~~ Although the Navy CIO, agreed to identify the mitigating efforts for preventing malicious cyber actors from exploiting inactive user accounts older than [redacted], he did not identify the actions that the Commander, U.S. Fleet Cyber Command, would take to prevent the exploitation of inactive user accounts older than [redacted]. Therefore, the recommendation is unresolved. The Navy CIO should provide additional comments describing how he will implement the recommendation.

~~(FOUO)~~ The Air Force CIO agreed to develop, implement, and enforce a plan to [redacted]. The recommendation is resolved but will remain open until the Air Force CIO provides documentation showing that Air Force policies include a requirement to [redacted].

Please see the Recommendations Table on the next page for the status of these recommendations among other recommendations.

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Chief Information Officer, Department of Defense	1.a	1.b	None
Chief Information Officer, Department of the Navy	5	None	None
Chief Information Officer, Department of the Air Force	None	6	None
Deputy Commander, U.S. Army Cyber Command	2.a, 2.b	None	None
Commander, U.S. Fleet Cyber Command, Department of the Navy	None	4	None
Deputy Chief of Staff for Manpower, Personnel, and Services, Department of the Air Force	7	None	None
Deputy Chief of Staff for Personnel, Department of the Army	3	None	None

Please provide Management Comments by April 29, 2021.

Note: The following categories are used to describe agency management's comments to individual recommendations.

- **Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **Closed** – OIG verified that the agreed upon corrective actions were implemented.

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

March 29, 2021

MEMORANDUM FOR CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE LOGISTICS AGENCY
AUDITOR GENERAL, DEPARTMENT OF THE NAVY
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

SUBJECT: Audit of Maintaining Cybersecurity in the Coronavirus Disease–2019 Telework Environment (Report No. DODIG-2021-064)

This final report provides the results of the DoD Office of the Inspector General's audit. We previously provided copies of the draft report and requested written comments on the recommendations. We considered management's comments on the draft when preparing the final report. Those comments are included in the report.

This report contains six recommendations that are considered unresolved because management officials did not provide written comments on the draft report or did not fully address the recommendations. Therefore, as discussed in the Recommendations, Management Comments, and Our Response sections of this report, the recommendations will remain unresolved until an agreement is reached on the actions to be taken to address the recommendations. Once an agreement is reached, the recommendations will be considered resolved but will remain open until adequate documentation has been submitted showing that the agreed-upon action has been completed. Once we verify that the action is complete, the recommendations will be closed.

The report contains three recommendations that are considered resolved. Therefore, as discussed in the Recommendations, Management Comments, and Our Response sections of this report, the recommendations will remain open until adequate documentation has been submitted showing that the agreed-upon action has been completed. Once we verify that the action is complete, the recommendations will be closed.

DoD Instruction 7650.03 requires that recommendations be resolved promptly. For the unresolved recommendations, please provide us within 30 days your response concerning specific actions in process or alternative corrective actions proposed on the recommendations. For the resolved recommendations, please provide us within 90 days documentation showing that the agreed-upon action has been completed. Your response should be sent as a PDF file to either audcso@dodig.mil if unclassified or [redacted] if classified SECRET. Responses must have the actual signature of the authorizing official for your organization.

We appreciate the cooperation and assistance received during the audit. Please direct questions to me at [redacted].

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

Contents


INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
INTEGRITY
EFFICIENCY

Introduction

Objective

The objective of this audit was to determine whether DoD Components maintained network protections during the coronavirus disease–2019 (COVID-19) pandemic while the DoD workforce maximized the use of telework capabilities to ensure the continuity of DoD operations. See Appendix A for a discussion on the scope and methodology and Appendix B for a discussion on the cybersecurity guidance for protecting DoD networks that support telework activities. See the Glossary for the definitions of technical terms.

Background

The COVID-19 is an infectious disease caused by a newly discovered coronavirus. On January 31, 2020, the Secretary of Health and Human Services declared a public health emergency due to confirmed cases of COVID-19 in the United States. On March 11, 2020, the World Health Organization declared the COVID-19 outbreak a pandemic, and on March 13, 2020, the President of the United States declared a national emergency as COVID-19 continued to spread across the country.[1] On March 15, 2020, to protect the health and safety of the workforce, the Acting Director of the Office of Management and Budget issued a memorandum asking all Federal Executive Branch departments and agencies to offer maximum telework flexibilities to all eligible personnel. Two days later, on March 17, 2020, the Office of Management and Budget issued a memorandum directing agencies to begin implementing policies and procedures to safeguard the health and safety of Federal workplaces, including maximizing telework across the Nation for the Federal workforce, while ensuring that Government operations continue.

In response to the requirement to maximize telework, on March 27, 2020, the Secretary of Defense directed DoD Components to allow personnel to telework and use virtual tools, such as video chat and file sharing, to continue DoD operations. The Secretary of Defense acknowledged that while some DoD personnel who perform mission-essential duties cannot telework and must continue to report to their official worksite, DoD Components should maximize telework for those personnel who can use the DoD Non-Classified Internet Protocol Routing Network to perform their primary duties.[2]

[1] The World Health Organization directs and coordinates international health within the United Nations system. A pandemic is a global outbreak of a disease that occurs when a new virus emerges to infect people and can spread between people sustainably.

[2] Mission-essential duties are those functions that must be performed under all circumstances to achieve missions or responsibilities. Government employees use the Non-Classified Internet Protocol Routing Network to perform non-classified work.

Using Remote Access to Telework

DoD personnel use enterprise telework technologies, such as remote access, to perform work from external locations other than their official worksite. Remote access is the ability for an authorized person to access a computer or a network from a geographical distance through an external network connection, such as the Internet. Teleworkers use various devices, such as desktop and laptop computers, smartphones, and tablets, to read and send e-mail, access websites, and review and edit documents, among other tasks.

According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-46, "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device Security," telework and remote access solutions require confidentiality, integrity, and availability of DoD data on an organization networks.[3] Confidentiality ensures that unauthorized parties cannot read remote access communications and stored user data. Integrity ensures the detection of any intentional or unintentional changes to remote access communications that occur in transit. Availability ensures that users can access resources through remote access whenever needed. An organization's telework and remote access solutions, including devices, remote access servers, and internal servers, should be secured against a variety of threats, such as lack of physical security controls, the use of unsecured networks, and infected devices on internal networks, at the same security level provided when personnel are physically located inside of the organization's facilities. Telework and remote access technologies often need additional protection because they generally receive higher exposure to external threats than technologies accessed only from inside the organization. The remote access methods that teleworkers most commonly use include tunneling, portals, remote desktop access, and direct application access.[4]

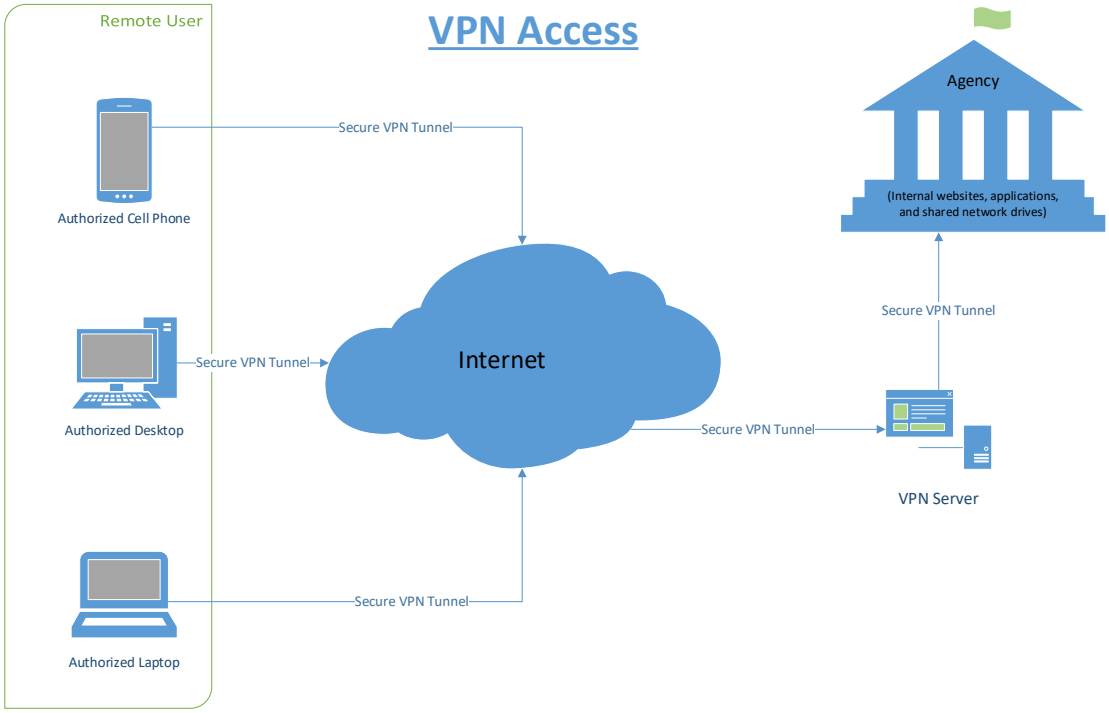
DoD personnel can gain access to their organization's networks using approved technologies, such as a virtual private network (VPN), which remotely connects an employee's government-furnished device to the organization's network. A VPN routes the device to the VPN server using an employee's Internet Service provider to gain access to the DoD Network. Once the connection is established, an employee can access many of the organization's computing resources through the connection. The types of VPN most commonly used for teleworkers are Internet

[3] NIST SP 800-46, Revision 2, "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device Security," July 2016.

[4] A tunnel offers a secure connection to transmit information between networks. Tunnels are typically established through a virtual private network. A portal is a server that offers access to one or more applications through a single centralized interface. A remote desktop solution gives a teleworker the ability to remotely control a particular computer at an organization, most often the user's own computer. Direct application access allows a user to access an application directly, without using remote access software. A common example of direct application access is webmail.

Protocol Security and Secure Sockets Layer connections.[5] The figure below shows an example of the VPN process.

Figure. Process for Accessing the Virtual Private Network



Note: A tunnel is technology that enables one network to send its data through another network's connections.

Source: The DoD OIG.

As an alternative to VPN, some DoD Components, such as the Defense Logistics Agency (DLA), use a virtual desktop infrastructure (VDI) that can remotely access a desktop through a centralized server and display it on a teleworker's non-government-furnished equipment, such as a **personal** [emphasis added] computer or tablet. Once teleworkers accesses the virtual desktop, they can select applications to perform their work as usual. In most instances, when the teleworker is finished with a remote access session, the virtual image is discarded so that the next user will have a clean virtual desktop. VDI is particularly helpful for safeguarding information on non-government-furnished equipment, which are more likely than government-furnished equipment to not meet DoD's security requirements.

[5] An Internet Protocol Security is a protocol that adds security features, and provide confidentiality and integrity services to the standard internet protocol. A Secure Sockets Layer is a protocol used to protect private information during the transmission of data over the internet.

On April 13, 2020, the DoD Chief Information Officer (CIO) issued a memorandum to approve the temporary use of a Commercial Virtual Remote (CVR) environment, one of DoD's authorized commercial cloud services, to support the DoD's telework posture in response to the COVID-19 pandemic.[6] The CVR environment is a virtual collaboration tool that includes capabilities such as virtual meeting, screen share, and video chats. When the DoD returns to a normal operational status, the CVR will be decommissioned and its data erased at the direction of the DoD CIO and the Commander of U.S. Cyber Command. The CVR environment resides on the DoD Enterprise Cloud, which consists of multiple clouds that are globally available for DoD users to access. The CVR is accessible through the Internet using government-furnished and non-government-furnished equipment.

DoD Telework Readiness Task Force

On March 10, 2020, the DoD established the DoD Telework Readiness Task Force to ensure DoD networks remain telework-ready and secure as personnel work from home during the COVID-19 pandemic. The DoD CIO leads the Task Force that includes CIOs and information technology officials from across the Military Services and other DoD Components. As a part of its efforts to oversee and manage network challenges, the DoD Telework Readiness Task Force issued the following memorandums to DoD Components to provide guidance for ensuring cybersecurity when teleworking.

"COVID-19 Response: Remote Work Capability," March 19, 2020

> Provides guidance for maintaining the cybersecurity of DoD networks and describes enterprise services that are available to personnel such as the Defense Collaboration Services, which includes web conferencing and chat capabilities, that allow DoD personnel to share and collaborate on tasks while teleworking.

"Revised Guidance for Use of Embedded Computer Capabilities and External Computer Peripherals in Telework Environments," June 5, 2020

> Provides guidance for enabling and using capabilities on DoD-issued laptops to maximize telework, such as cameras; microphones; Wi-Fi; and external keyboards and monitors.

[6] DoD CIO memorandum, "Authorized Telework Capabilities and Guidance," April 13, 2020.

Cybersecurity Controls Assessed

To determine whether DoD Components maintained network protections as the DoD workforce maximized the use of telework capabilities, we assessed selected cybersecurity controls that we consider critical to the protection of DoD networks and data in a maximum telework environment. We assessed the cybersecurity controls at the following Components and sub-Components during our audit:

- Army – Office of the Judge Advocate General,
- Navy – Naval Information Warfare Systems Command,
- Air Force – Cyberspace Capabilities Center, and
- DLA.

Cybersecurity controls are safeguards and countermeasures that are designed to protect the confidentiality, integrity, and availability of information that is processed by, stored on, and transmitted through the DoD networks. Table 1 identifies the cybersecurity controls assessed and their importance in a telework environment.

Table 1. Cybersecurity Controls Assessed and Their Importance in the Telework Environment

Cybersecurity Control	Importance of Cybersecurity Control in a Telework Environment
VPN Session Inactivity Thresholds	VPN session inactivity thresholds establish a timeframe for [redacted] on endpoint devices.[1] [redacted] frees up network bandwidth and memory; and allows new sessions to connect to the network so that personnel can sustain DoD Component missions.
Vulnerability Identification and Mitigation	Identifying and mitigating vulnerabilities includes scanning networks and systems to identify potential weaknesses, such as VPN vulnerabilities, that can be exploited on a computer or network. Malicious cyber actors can exploit vulnerabilities on DoD networks and systems, and steal information related to some of the Nation's most valuable advanced defense technologies.[2] Identifying and mitigating network and system vulnerabilities reduces a malicious cyber actor's ability to gain unauthorized access to DoD networks and systems; introduce malware, and steal critical national security information. Identifying and mitigating vulnerabilities during the pandemic is critical because telework and remote access technologies generally receive higher exposure to external threats than technologies accessed by personnel located physically inside the organization's facilities.
Inactive User Account Thresholds	Inactive user account thresholds are established timeframes for disabling and deleting user accounts that remain inactive for an extended period of time. Automatically disabling and deleting inactive user accounts within required timeframes reduces a malicious cyber actor's ability to gain unauthorized and undetected access to DoD networks. Automatically disabling and removing inactive user accounts limits unauthorized access and malicious actions that could jeopardize mission operation during maximized telework periods.

Table 1. Cybersecurity Controls Assessed and Their Importance in the Telework Environment (cont'd)

Cybersecurity Control	Importance of Cybersecurity Control in a Telework Environment
Protection of Controlled Unclassified Information	Protecting controlled unclassified information (CUI) by implementing access, system, and communications security controls allows DoD Components to safeguard information that, if disclosed, would reveal vulnerabilities in the DoD critical infrastructure and, if exploited, would likely result in the significant disruption, destruction, or damage of or to DoD operations, property, or facilities. The lack of controls around capabilities used by teleworkers, such as the CVR environment, puts the DoD at greater risk of cyberattacks from malicious cyber actors who can compromise CUI stored on non-government-furnished equipment.
Telework Training and Authorization	Telework training provides personnel with a brief and practical introduction to telework and offers tools for deciding whether telework is appropriate for the employee's specific job. Supervisors are responsible for determining and documenting personnel eligibility to telework.

[1] For the purpose of this report, endpoint devices include desktop or laptop computers, as well as portable devices such as tablets and smartphones.

[2] A malicious cyber actor is an individual that uses technology with the intent to cause harm.

Source: The DoD OIG.

Review of Internal Controls

DoD Instruction 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls.[7] We identified internal control weaknesses related to maintaining network protections on DoD networks in a maximum telework environment. We will provide a copy of the final report to the senior official responsible for internal controls in the Departments of the Army, Navy, Air Force, the Office of the DoD CIO, and the DLA.

[7] DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

Finding

Cybersecurity Controls Were Not Consistently Implemented to Protect DoD Networks During Maximum Telework

The DoD Components did not consistently maintain network protections as the DoD workforce maximized the use of telework capabilities during the coronavirus disease–2019 (COVID-19) pandemic. Specifically;

- ~~(FOUO)~~ Network administrators for the Army, Navy, Air Force, and the DLA did not implement a consistent timeframe for [redacted]. While network administrators for the Navy and the DLA [redacted] after [redacted] respectively, the Air Force network [redacted], and the Army network [redacted]. This occurred because the language in the DISA VPN Security Requirement Guide did not explicitly define the amount of time that DoD Components should allow [redacted], stating only that [redacted] or less was a "common best practice."[8]
- ~~(FOUO)~~ Network administrators for the Army and Air Force did not [redacted] or develop plans of action and milestones for [redacted]. [redacted] could result in malicious cyber actors exploiting the [redacted] to gain unauthorized access to networks, introduce malware, or steal CUI.
- ~~(FOUO)~~ Account administrators for the Navy did not disable inactive user accounts in accordance with DISA Application Security and Development Security Technical Implementation Guide (STIG) requirements. The Commander, U.S. Fleet Cyber Command [redacted].[9] However, although the Commander, U.S. Fleet Cyber Command is authorized to accept the risk, [redacted].

[8] Virtual Private Network System Requirement Guide Overview, Version 1 Release 1, July 19, 2019.

[9] An active directory manages users and groups of computers within a network.

- ~~(FOUO)~~ Officials at the Cloud Computing Program Office, under the direction of the DoD Deputy CIO for Information Enterprise, did not implement safeguards for Microsoft Teams (software) to prevent teleworkers from storing and transferring CUI on non-government-furnished equipment while using collaborative capabilities in a CVR environment.[10] The Cloud Computing Program Office Technical Director stated that the network administrators could not implement a safeguard on the CVR to prevent the storage of CUI for personal computer users because applying such a safeguard would also prevent users on government-furnished equipment from storing CUI when using [redacted]. However, if network administrators implemented a safeguard to prevent teleworkers from storing and transferring CUI on non-government-furnished equipment, there are other DoD-approved data collaboration tools available to government-furnished equipment users who want to exchange CUI, such as Defense Collaboration Services.[11] With 1 million CVR users who exchange and possibly store an average of over 1.65 million messages per day that could include CUI, there is an increased risk that DoD CUI could be intentionally or unintentionally disclosed if the non-government-furnished equipment is compromised. In addition, transferring CUI on non-government-furnished equipment puts the DoD at greater risk of cyberattacks from malicious cyber actors who can intercept the transmission and deploy malicious code into word processing software, spreadsheets, or image files on a victim's system.
- Army, Navy, and Air Force supervisors approved personnel for telework without ensuring the required telework agreements and telework training were completed. According to Component officials, some Army, Navy, and Air Force supervisors stated that they were unaware of the supervisor responsibilities for telework or overwhelmed with other duties during the COVID-19 pandemic.

Maintaining a high level of cybersecurity while teleworking is critical because the inherent security measures present when at a DoD worksite may not be fully practiced while working remotely. As the DoD workforce continues to maximize the use of telework capabilities, personnel should be especially alert and attentive to cyber attacks, malware, phishing attempts, and network security protocols that may threaten Government information stored on telework devices and transmitted across external networks. Telework and remote access solutions are critical to the success of DoD's efforts to continue operations during the COVID-19 pandemic. As such, telework and remote access technologies often need additional protection

[10] ~~(FOUO)~~ [redacted] is a collaboration tool that allows video, voice, and text communication, and document sharing.

[11] Defense Collaboration Services provides web conferencing and chat capabilities to allow DoD personnel to share and collaborate on tasks while teleworking.

from malicious cyber actors because they generally receive higher exposure to external threats than technologies accessed by personnel physically located inside the organization's facilities.

DoD Components Did Not Always Maintain Cybersecurity to Protect DoD Networks in a Maximum Telework Environment

DoD Components did not consistently implement controls and processes to protect DoD networks in the maximum telework environment. The March and June 2020 DoD CIO memorandums require DoD Components to maintain the cybersecurity of DoD networks, collaboration tools, laptops, and external keyboards and monitors during telework.[12] To determine whether DoD Components maintained cybersecurity as the DoD workforce maximized the use of telework capabilities, we assessed cybersecurity controls used to secure VPNs, identify and mitigate vulnerabilities; monitor user activities; manage user access, protect CUI, and manage risk.

[redacted] *Virtual Private Network* [redacted] *Were Not Consistently*

~~(FOUO)~~ Network administrators for the Army, Navy, Air Force and the DLA did not implement a consistent timeframe for [redacted]. Specifically, the Navy and the DLA network administrators [redacted] the Air Force network administrators [redacted], and the Army network administers [redacted]. NIST SP 800-77 states that it is "reasonable" to [redacted] but also does not mandate a specific threshold.[13] DISA VPN Security Requirements Guide states that a "common best practice" for [redacted] is [redacted] minutes or less but does not mandate that time threshold.[14] To determine the DoD Components threshold of [redacted], we observed screenshots of the group policy for timeout settings to verify the timeframe that [redacted] on each workstation.

[12] DoD CIO memorandum, "COVID-19 Response: Remote Work Capability," March 19, 2020. DoD CIO memorandum, "Revised Guidance for Use of Embedded Computer Capabilities and External Computer Peripherals in Telework Environments," June 5, 2020.

[13] NIST SP 800-77, Revision 1, "Guide to Internet Protocol Security VPNs," June 2020.

[14] VPN Security Requirements Guide, Version 1, Release 1, July 19, 2019.

(FOUO) The [redacted]. However, during the audit, [redacted]. The Army Network Enterprise Technology Command's Director for Operations stated that the Army Network Enterprise Technology Command [redacted] because it needed the [redacted] so that the endpoint devices could be scanned and patched. However, VPN sessions [redacted] If [redacted] before the Army begins its patching process, endpoint devices will still receive a portion of the patches once the device reconnects to the Army's network.

(FOUO) DoD Components could reduce available points of access for malicious cyber actors to exploit by [redacted]. In addition, [redacted] strain resources (such as bandwidth and memory), prevent [redacted] from connecting [redacted], and limit the ability of DoD personnel to sustain the mission of their respective Component. Including explicit language in the DISA VPN Security Requirements Guide on the time limit (threshold) to [redacted] would provide clear direction to all DoD Components.

Virtual Private Network Vulnerabilities Were Not Mitigated in a Timely Manner

(FOUO) Network administrators for the Army and Air Force did not mitigate known [redacted] and [redacted] VPN vulnerabilities in accordance with DoD requirements.[15] In addition, the Army CIO did not develop a plan of action and milestones for vulnerabilities that the Army was not able to mitigate. Army Regulation 25-2 requires Army Commands to mitigate vulnerabilities in a timely manner.[16] To determine whether the four DoD Components we assessed mitigated VPN vulnerabilities in a timely manner, we compared VPN network scan results, selected a sample of vulnerabilities, and calculated the number of days it took to mitigate the identified vulnerabilities. For the Army Network Enterprise Technology Command, we selected a sample of [redacted] of [redacted] vulnerabilities from an October 2020 scan and calculated the number of days the Army Network Enterprise Technology Command took to mitigate identified vulnerabilities.

[15] Critical vulnerabilities, if exploited by unauthorized users, would have a disastrous effect on DoD operations and assets. High vulnerabilities, if exploited by unauthorized users, could have a catastrophic effect on DoD operations and assets.

[16] Army Regulation 25-2, "Army Cybersecurity," April 4, 2019.

~~(FOUO)~~ At the Army Network Enterprise Technology Command, an October 2020 scan revealed that [redacted] of the [redacted] vulnerabilities sampled remained unmitigated. The [redacted] vulnerabilities consisted of [redacted] and [redacted] vulnerabilities. For example, one of the Army's unmitigated [redacted] vulnerabilities [redacted] In addition, another of the Army's unmitigated high vulnerabilities related to [redacted]

~~(FOUO)~~ The Army Network Enterprise Technology Command did not include any of the [redacted] unmitigated [redacted] and [redacted] vulnerabilities identified in our analysis in a plan of action and milestones. According to the [redacted], network administrators wanted to focus on mitigating vulnerabilities instead of completing paperwork to create plan of action and milestones.

~~(FOUO)~~ At the Air Force 83rd Network Operations Squadron, an August 2020 Command Cyber Readiness Inspection identified [redacted] vulnerabilities related to [redacted].[17] For example, one unmitigated Air Force critical vulnerability from [redacted] however, as of December 2020, the Air Force did not provide supporting documentation, such as comparative vulnerability scans or plan of action and milestones, to show that vulnerabilities were mitigated within the timelines outlined in the Air Force mitigation schedule.[18] DoD Instruction 8510.01 requires DoD organizations to develop a plan of action and milestones for vulnerabilities that cannot be immediately mitigated by documenting the tasks that need to be accomplished to remediate or mitigate the vulnerabilities.[19] In addition, the March 19, 2020, DoD CIO memorandum states that during the maximized telework period, the DoD must ensure that it maintains the cybersecurity of its networks, which includes mitigating vulnerabilities in a timely manner.

Regularly mitigating known vulnerabilities is part of basic cyber hygiene. According to the Cybersecurity and Infrastructure Security Agency, as organizations use VPNs for telework, malicious cyber actors are identifying

[17] Command Cyber Readiness Inspections ensure that DoD Components and individual units comply with system requirements, validate the use and configuration of mandated DoD enterprise cybersecurity tools, and determine the components' readiness to handle incidents in compliance with DoD cybersecurity policies.

[18] ~~(FOUO)~~ [redacted]

[19] DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology," July 28, 2017.

and targeting VPN vulnerabilities to potentially obstruct VPN sessions and download files from servers using malicious codes.[20] Failure to identify and mitigate vulnerabilities timely could result in malicious cyber actors exploiting the vulnerabilities to gain unauthorized access to networks, introduce malware, or steal CUI. If a malicious cyber actor gains unauthorized access to enterprise resources and telework devices, compromised resources could be used to eavesdrop on and manipulate communications, as well as provide a mechanism to attack other networks within the organization.

The Navy Did Not Disable or Remove Inactive User Accounts Timely

~~(FOUO)~~ The Navy account administrators did not disable or remove [redacted] [21] The DISA Windows 10 STIG requires that user accounts be disabled or removed after 35 days of inactivity.[22] In addition, NIST SP 800-53 states that information systems should automatically disable inactive accounts after an organization-defined time period.[23] To determine whether the DoD Components disabled or removed inactive user accounts after 35 days, we observed network settings to verify that network administrators configured group policies in accordance with the DISA STIG.

~~(FOUO)~~ Before the COVID-19 pandemic, the Navy required agencies to disable user accounts after 30 days of inactivity.[24] However, from March 2020 to September 2020, the U.S Fleet Cyber Commander [redacted] and accepted and documented the risk of not [redacted].[25] In September 2020, the Commander, U.S Fleet Cyber Command [redacted] and the DISA STIG. The Commander accepted the risk because [redacted].[26]

[20] The Cybersecurity and Infrastructure Security Agency is the Nation's risk advisor and leads the efforts to increase the security of the Federal Government critical networks.

[21] Inactive user accounts are based on the last time users logged into the network.

[22] DISA Windows 10 Security Technical Implementation Guides, Version 1, Release 23, June 17, 2020.

[23] NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, Updated as of January 22, 2015.

[24] The Navy Telecommunications Directive (NTD) 01-19, "Management of Dormant Accounts," November 2019, states that accounts that have been inactive (dormant) for 30 days (60 days for Reserve Forces) should be disabled and accounts that have been inactive for 45 (90 days for Reserve Forces) should be deleted.

[25] In response to questions related to cybersecurity requirements, on April 3, 2020, the DoD Senior Information Security Officer issued a memorandum, "Authorizations to Operate Extensions and Cybersecurity Function Prioritization Guidance," allowing Authorizing Officials to make risk decisions to extend the inactivity time before disabling user accounts.

[26] DoD Components use Active Directory for managing permissions and user access to network resources.

~~(FOUO)~~ According to the Naval Network Warfare Command Cybersecurity Division Officer, individual commands that the Naval Network Warfare Command supports, including the Reserve Forces Command, [redacted]. However, although the Commander, U.S. Fleet Cyber Command is authorized to accept the risk, [redacted]. At the start of the COVID-19 pandemic, this action was understandable given all of the unknowns regarding employee access to systems and working environments. However, as the working environment has solidified, [redacted] may not be appropriate at this point. The Naval Network Warfare Command should identify and implement an additional layer of defense against cyberattacks that target [redacted].

The DoD Deputy CIO Did Not Implement Controls to Prevent the Storage and Transmission of CUI to Non-Government Furnished Equipment

~~(FOUO)~~ Officials at the Cloud Computing Program Office, under the direction of the DoD Deputy CIO for Information Enterprise, [redacted]. The Cloud Computing Program Office provides administrative support, such as secure enterprise services, to the CVR environment, which includes managing [redacted]. DoD Instruction 5200.48 requires DoD Components to implement physical and logical procedures to protect CUI that has the potential to impact national security.[27] In addition, NIST SP 800-114 recommends restricting file transfers on non-government-furnished equipment for teleworkers using instant messaging clients. Furthermore, in March 2020, a memorandum signed by the DoD CIO Senior Information Security Officer established the CVR environment to support effective collaboration. The DoD CIO Senior Information Security Officer stated that the following types of CUI are prohibited in the CVR environment.

[27] DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020.

- CUI under the control and direction of the Department of Defense (Controlled Technical Information, Critical Infrastructure Security Information, Naval Nuclear Propulsion Information and Unclassified Controlled Nuclear Information – Defense).
- All data types under the Law Enforcement CUI grouping.
- All data types under Privacy data.

~~(FOUO)~~ On April 13, 2020, the DoD CIO issued a memorandum that allowed DoD personnel in the CVR environment to use the [redacted] during maximum telework. [redacted] is a collaboration tool that allows video, voice, and text communication, and document sharing.[28] While network administrators for the Army, Navy, Air Force, and the DLA implemented group policy settings and host-based security system applications to detect whether personnel attempted to store and transfer CUI to unauthorized storage devices, these DoD Components did not have the capability to prevent users from doing so.[29] To determine whether security controls were implemented to prevent CVR users from storing and transferring CUI to non-government furnished equipment, we conducted interviews with officials in the Cloud Computing Program Office and obtained screenshots of the controls implement for [redacted].

~~(FOUO)~~ While the DoD CIO and Senior Information Security Officer supported capabilities to promote collaboration during the maximized telework period, the DoD Deputy CIO for Information Enterprise did not implement controls [redacted]. The Cloud Computing Program Office Technical Director stated that the network administrators could not implement a safeguard on the CVR to prevent the storage of CUI for personal computer users only because applying such a safeguard would also prevent users on government-furnished equipment from storing CUI when using [redacted].

~~(FOUO)~~ According to the Technical Director, the Cloud Computing Program Office monitors the CVR for unusual activity, including file transfers larger than 700 individual files. However, monitoring the CVR for unusual activity is not a substitute for having technical controls built-in to the system to prevent the storage and transmission of CUI. [redacted]. The CVR's 1 million users who exchange an average of over 1.65 million messages (possibly containing CUI) per day increases the risk that DoD CUI could be intentionally or unintentionally disclosed

[28] An example of data collaboration is file sharing, which allows users to read, edit, or present a document with multiple users in real time.

[29] Host-based security is a set of capabilities that provide a framework to implement the wide-range of security solutions on hosts. This framework includes a trusted agent and a centralized management function that together provide automated protection to detect, respond, and report host-based vulnerabilities and incidents.

~~(FOUO)~~ if non-government-furnished equipment is compromised. Transferring [redacted].

Personnel Allowed to Telework Without Approved Telework Agreements or Required Telework Training

Army, Navy, and Air Force supervisors allowed personnel to telework without approved telework agreements or required telework training.[30] DoD Instruction 1035.01 requires all personnel authorized to telework to complete telework agreement and telework training before entering into a written telework agreement.[31] Supervisors are responsible for ensuring that all telework-eligible personnel:

- complete training on information security management and accessing DoD technology remotely, and
- understand their responsibilities in safeguarding work-related information.

To determine whether users completed telework training and had approved telework agreements in accordance with DoD requirements, we selected a statistical sample of 153 of 27,791 teleworkers from the Army OTJAG, Naval Information Warfare Systems Command, Air Force Cyberspace Capabilities Center, and the DLA. Table 2 lists, by subcomponent, the number of users who teleworked without completing a telework agreement and the required telework training.

Table 2. Unauthorized Telework at DoD Components

Component	Population of Teleworkers*	Users Sampled	Users Without Approved Telework Agreements	Users Who Did Not Complete Telework Training
Army Office of the Judge Advocate General	68	30	1	11
Naval Information Warfare Systems Command	10,627	45	8	2
Air Force Cyberspace Capabilities Center	146	33	0	2
DLA	16,950	45	0	0
Total	**27,791**	**153**	**9**	**15**

* The population of teleworkers represent the number of DoD personnel that officials from the DoD Components that we assessed stated were eligible to telework.

Source: The DoD OIG.

[30] Personnel refers to DoD civilians and not service members.

[31] DoD Instruction 1035.01, "Telework Policy," April 4, 2012, Incorporating Change 1, April 7, 2020. DD Form 2946, "Department of Defense Telework Agreement," December 2011.

The Administrative Officer for the Army Office of the Judge Advocate General (OTJAG) stated that during the maximized telework period, the OTJAG Administrative Division became overwhelmed with other duties that required immediate attention, and therefore did not verify that personnel completed telework training and had approved telework agreements before teleworking. The Air Force Chief Information Security Officer stated that some personnel did not successfully save their completed training certificates. However, it is the responsibility of supervisors to verify that personnel complete all telework requirements before authorizing telework. Supervisors should ensure telework training is completed and certificates are maintained before approving personnel to telework. The Naval Information Warfare Systems Command Telework Program Manager stated that some supervisors did not remember to sign telework agreements or inform employees of telework requirements.

According to DoD Instruction 1035.01, telework agreements outline security requirements and telework responsibilities for DoD information. In addition, NIST SP 800-46 states that one of the most important security considerations for telework is training users on how to detect and respond to cyber threats, such as phishing attacks. As DoD personnel continue to telework during the COVID-19 pandemic, it is critical that telework agreements and trainings are completed to ensure that personnel follow good cybersecurity practices, such as protecting CUI. Users with completed telework agreements and training are more likely to maintain the same discipline, awareness, and security standards that are required for on-site work environments. DoD Components that do not verify that users completed telework agreements increase the risk that personnel will not safeguard DoD information and protect government-furnished equipment. In addition, users who do not complete telework trainings may be unaware of how to respond to social engineering attacks (such as phishing) on telework devices and remote access connections.[32]

DoD Data and Networks Could Be Compromised by Cyber Attacks

~~(FOUO)~~ According to the Cybersecurity and Infrastructure Security Agency, as the COVID-19 pandemic has brought a significant increase in teleworking, attacks from malicious cyber actors have also increased. In addition, the use of potentially vulnerable services, such as [redacted] amplifies the threat to individuals and organizations in a maximized telework environment. DoD Components that do not fully implement NIST and DoD security controls to maintain cybersecurity in a maximum telework environment, make themselves more vulnerable to targeted

[32] A social engineering attack uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. Phishing is a form of social engineering that uses e-mail or malicious websites to solicit personal information by posing as a trustworthy organization.

~~(FOUO)~~ [redacted] attacks from malicious cyber actors. Specifically, malicious cyber actors could exploit [redacted] vulnerabilities, disrupt DoD operations through denial of service attacks, and steal information related to some of the Nation's most valuable missions and technologies. Identifying and mitigating vulnerabilities in a timely manner decreases the risk that cyber attacks could exploit [redacted] that malicious cyber actors could use to gain unauthorized access to telework devices or resources that could be used to eavesdrop on and manipulate communications. The unauthorized disclosure of DoD information could threaten the safety of the warfighter, cause the United States to be at a disadvantage against its adversaries, and jeopardize mission operations.

~~(FOUO)~~ DoD Components that do not consistently [redacted] for teleworkers to sustain the mission of their DoD Component. In addition, [redacted] limits unauthorized access and malicious actions that could jeopardize mission operations during maximized telework periods. Furthermore, DoD Components that allow personnel to telework without approved telework agreements and required training increase the risk of insider threat and may allow for the unauthorized disclosure of CUI and other sensitive and critical DoD information, which could threaten the safety of the warfighter and cause the United States to be at a disadvantage against its adversaries. When DoD Components do not fully implement required cybersecurity controls over [redacted], malicious actors could exploit vulnerabilities and steal CUI and other sensitive technical information stored on DoD networks. For example, in September 2020, the Cybersecurity and Infrastructure Security Agency issued two reports identifying cyberattacks on Federal agencies by malicious cyber actors who exploited known VPN vulnerabilities to gain unauthorized and undetected access to Federal networks.[33]

Recommendations, Management Comments, and Our Response

Redirected and Renumbered Recommendations

As a result of management comments, we:

- Redirected Recommendations 2.a and 2.b from the Army CIO to the Deputy Commander, U.S. Army Cyber Command, who has the responsibility to plan and direct cybersecurity protective measures on the Army's portion of the DoD Information Network at the strategic and operational levels.

[33] Alert AA20-259A, "Iran-Based Threat Actor Exploits VPN Vulnerabilities", September 15, 2020; and Analysis Report AR20-268A, "Federal Agency Compromised by Malicious Cyber Actor," September 24, 2020.

- Redirected Recommendation 2.c from the Army CIO to the Army Deputy Chief of Staff for Personnel, who has the authority to require supervisors to ensure their employees complete telework agreements and telework training as a condition for telework participation; and renumbered it as Recommendation 3.
- Renumbered Recommendation 3 as Recommendation 4.
- Renumbered Recommendation 4 as Recommendation 5.
- Renumbered Recommendation 5 as Recommendation 6.
- Renumbered Recommendation 6 as Recommendation 7.

Recommendation 1

~~(CUI)~~ We recommend that the DoD Chief Information Officer:

a. **~~(CUI)~~ Direct the Defense Information Systems Agency to review the language in the Virtual Private Network Security Requirements Guide and revise the guide to include specific language that [redacted].**

Department of Defense Chief Information Officer Comments

~~(CUI)~~ The DoD CIO disagreed, stating that DISA concluded that [redacted] at an enterprise level could have a negative impact on the organizations within the Department.

Our Response

~~(CUI)~~ Comments from the DoD CIO did not address the specifics of the recommendation; therefore, the recommendation is unresolved. Although the DoD CIO agreed with DISA's conclusion that defining a value to [redacted] could have a negative impact on the organizations within the Department, the DISA Risk Management Executive agrees that [redacted] may free up VPN resources. However, the DoD CIO did not provide additional information detailing the increased risk of [redacted]. Therefore, we cannot conclude on whether [redacted] would, in fact, have a negative impact on DoD Components. The DoD CIO should provide additional comments describing how DISA determined that [redacted] could negatively impact organizations within the DoD.

Risk Management Executive for the Defense Information Systems Agency Comments

~~(CUI)~~ Although not required to comment, the Risk Management Executive, Defense Information Systems Agency, stated that when developing the VPN Security Requirement Guide, they considered [redacted] The Risk Management Executive added that DISA agreed that a [redacted] is ideal for end-user connections to portals, logins, or services. However, he stated that DISA concluded that [redacted] at an enterprise level could have a negative impact or degrade security within the Department. For example, the DISA Risk Management Executive stated that some DoD Components use the "Always-On VPN" solutions, which limits exposure to threats that exist on a user's local network by automatically creating a VPN back to the organization's enterprise network. He stated also that the use of "Always-On VPN" ensures that only authorized devices can connect to an organization's network; and allows organizations to monitor devices when they are powered on and connected. While the DISA Risk Management Executive agrees that [redacted], he stated that [redacted]. Furthermore, the Risk Management Executive stated that [redacted] could impact an organization's ability to apply patch management solutions. Finally, he stated that DISA allows each organization the option to conduct their own risk assessment and [redacted].

Our Response

~~(CUI)~~ We agree that the use of "Always-On VPN" solutions may limit exposure to threats that exist on a user's local network. However, not all DoD Components use the "Always-On VPN" solutions. Therefore, a VPN inactivity limit should be required for those DoD Components. We also agree that a [redacted] is ideal for end-user connections to portals, logins, or services. However, the DISA Risk Management Executive did not provide details on the exposure risks associated with [redacted] or how DISA determined that [redacted] could expose devices to threats. Without those details, we are unable to conclude that doing so would have a negative impact on organizations within the Department. Therefore, we will request that the DoD CIO provide additional comments describing how DISA determined that [redacted] could negatively impact the security of DoD networks.

b. ~~(FOUO)~~ Direct the DoD Deputy Chief Information Officer for Information Enterprise to implement controls to [redacted]

Department of Defense Chief Information Officer Comments

~~(FOUO)~~ The DoD CIO did not agree or disagree, stating that the DoD CIO will direct the DoD Deputy Chief Information Officer for Enterprise to [redacted] while using [redacted].

Our Response

~~(FOUO)~~ Although the DoD CIO did not agree or disagree, his comments addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the DoD CIO provides documentation describing the actions taken by the DoD Deputy CIO for Information Enterprise to [redacted].

Recommendation 2

~~(CUI)~~ We recommend that the Deputy Commander, U.S. Army Cyber Command develop, implement, and enforce a plan to:

a. ~~(CUI)~~ Set [redacted] for virtual private network sessions.

Deputy Chief of Staff for the U.S Army Cyber Command Comments

~~(CUI)~~ Although not required to comment, the Deputy Chief of Staff, U.S. Army Cyber Command, stated that the [redacted]. In addition, he stated that, during an environment of maximum telework, [redacted].

Our Response

~~(CUI)~~ While we agree that VPN connections provide active protection of the DoD Information network, we disagree that VPN sessions must [redacted]. If [redacted] before the Army begins its patching process, endpoint devices will receive

~~(CUI)~~ a portion of the patches once the device reconnects to the Army's network. The Deputy Commander should provide comments describing how he will implement the recommendation.

b. ~~(CUI)~~ Mitigate [redacted].

Deputy Chief of Staff for the U.S Army Cyber Command Comments

~~(CUI)~~ Although not required to respond, the Deputy Chief of Staff for U.S. Army Cyber Command stated that mitigating [redacted] is basic hygiene and should be encouraged at all levels.

Our Response

~~(CUI)~~ We agree that mitigating [redacted] is basic hygiene and should be encouraged at all levels. We redirected the recommendation to the Deputy Commander, U.S. Army Cyber Command, who has the authority to implement the recommendation. The Deputy Commander should provide comments describing how he will implement the recommendation.

Recommendation 3

We recommend that the Army Deputy Chief of Staff for Personnel develop, implement, and enforce a plan to verify that DoD personnel complete telework agreement and the required DoD telework training before teleworking.

Recommendation 4

~~(CUI)~~ We recommend that the Commander, U.S. Fleet Cyber Command reconsider his decision to [redacted], and [redacted] in accordance with Navy and the Defense Information Systems Agency policies.

Commander for the U.S. Fleet Cyber Command Comments

~~(CUI)~~ The Commander, U.S. Fleet Cyber Command, agreed, stating that the U.S. Fleet Cyber Command, has already reconsidered the decision to extend the number of days user accounts remain inactive. The Commander stated that U.S. Fleet Cyber Command has reverted back to the Navy's and the DISA STIG requirements that requires agencies to [redacted]. He added that dormant accounts are being disabled and deleted in accordance with the interim timelines, which optimally balance mission requirements and cybersecurity concerns.

Our Response

~~(CUI)~~ Comments from the Commander, U.S. Fleet Cyber Command, addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Commander provides documentation showing that network administrators configured group policies to disable or remove user accounts after [redacted] of inactivity as required by the DISA policies.

Recommendation 5

~~(CUI)~~ We recommend that the Navy Chief Information Officer direct the Commander, U.S. Fleet Cyber Command to identify mitigating efforts for preventing malicious cyber actors from exploiting inactive user accounts older than [redacted].

Navy Chief Information Officer Comments

~~(CUI)~~ The Navy CIO agreed, stating that the Commander of U.S. Fleet Cyber Command would identify the mitigating efforts for preventing malicious cyber actors from exploiting inactive user accounts older than [redacted].

Our Response

~~(CUI)~~ Although the Navy CIO agreed, comments from the Navy CIO did not address the specifics of the recommendation; therefore, the recommendation is unresolved. The Navy CIO did not identify the actions that the Commander, U.S. Fleet Cyber Command, will take to prevent the exploitation of inactive user accounts older than [redacted]. As stated in the report, while the Commander is authorized to accept the risk, [redacted]. The Navy CIO should provide additional comments describing how he will implement the recommendation.

Recommendation 6

~~(FOUO)~~ We recommend that the Air Force Chief Information Officer develop, implement, and enforce a plan to [redacted].

Air Force Chief Information Officer Comments

~~(FOUO)~~ The Air Force CIO agreed, stating that the Air Force Information Network Vulnerability Management guidance establishes identification, notification, and remediation procedures and the requirement to [redacted]. He also stated that there is a conflict between the Command Cyber Readiness Inspection and U.S. Cyber Command requirements for creating a plan of action and milestones. Specifically, he stated that the Command Cyber Readiness Inspection requirements indicated 90 days regardless of [vulnerability] criticality, while the [redacted].[34] The Air Force CIO stated that a thorough review of Department of Air Force, U.S. Cyber Command, and other DoD Information Network level vulnerability management guidance is necessary to identify conflicts with the guidance and determine a standardized requirement for resolving and reporting vulnerabilities across the force. He also stated that [redacted] in the Air Force Concept of Operations for the Air Force Information Network by October 30, 2021.

Our Response

~~(FOUO)~~ Comments from the Air Force CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We agree that there is a conflict between the Command Cyber Readiness Inspection and U.S. Cyber Command requirements for creating a plan of action and milestones. The Air Force CIO should direct his concerns to the U.S. Cyber Command and DISA to reconcile the conflict between vulnerability management guidance. We will close the recommendation once the Air Force CIO provides documentation showing that the Concept of Operations for the Air Force information network includes a [redacted]

34 ~~(FOUO)~~ [redacted]

Recommendation 7

We recommend that the Air Force Deputy Chief of Staff for Manpower, Personnel, and Services verify that DoD personnel completed telework agreements and the required DoD telework training before teleworking.

Air Force Chief Information Officer Comments

The Air Force CIO, responding for the Air Force Deputy Chief of Staff for Manpower, Personnel and Services, agreed, stating that all DoD personnel should complete telework agreements and the required DoD telework training before teleworking. The Air Force CIO suggested that we revise the recommendation to require the Air Force Deputy Chief of Staff for Manpower, Personnel, and Services to develop and issue guidance, including verification procedures, to ensure that DoD personnel completed telework agreements and the required DoD telework training before teleworking. The Air Force CIO also stated that the responsibility for ongoing verification of training and completed agreements resides with commanders and directors and a revised recommendation will provide the Air Force Deputy Chief of Staff for Manpower, Personnel, and Services the flexibility to develop guidance to meet the recommendation.

Our Response

Although the Air Force CIO agreed, he did not address the specifics of the recommendation; therefore, the recommendation is unresolved. DoD Instruction 1035.01 already requires supervisors to approve telework requests, which includes signing the telework agreements and verifying that personnel completed telework training. However, if the Air Force Deputy Chief of Staff for Manpower, Personnel, and Services wants to supplement existing DoD guidance by developing procedures to verify that personnel completed telework agreements and the required DoD telework training before teleworking, that would meet intent of the recommendation. Therefore, the Air Force CIO should provide additional comments describing how the Air Force Deputy Chief of Staff for Manpower, Personnel, and Services will ensure that the recommendation is implemented.[35]

[35] DoD Instruction 1035.01, "Telework Policy," April 4, 2012, Incorporating Change 1, April 7, 2020. DD Form 2946, "Department of Defense Telework Agreement," December 2011.

Appendix A

Scope and Methodology

We conducted this performance audit from May 2020 through January 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.

To determine whether DoD Components maintained network protections in the COVID-19 maximum telework environment, we interviewed officials from the:

- Office of the DoD Chief Information Officer;
- Army, Army OTJAG;
- Navy, Naval Information Warfare Systems Command;
- Air Force, Air Force Cyberspace Capabilities Center;
- DLA;
- DISA, and
- DoD Telework Readiness Task Force.

We reviewed:

- cybersecurity controls, guidelines, policies, procedures, and instructions related to remote access usage;
- risk, change, and configuration management;
- protections of CUI;
- telework agreements;
- cybersecurity risk assessments;
- vulnerability scans;
- lists of patches, updates, and network settings; and
- plans of action and milestones.

To identify and verify the effectiveness of cybersecurity controls implemented to protect DoD networks during maximum telework, we interviewed project managers and system administrators from the Army, Navy, Air Force, and the DLA. We also reviewed Federal laws and DoD policy concerning information risk management, configuration management, remote access, and protection of CUI.

We used a nonstatistical approach to select the three individual components within the Army, Navy, and Air Force. In June 2020, we conducted a data call on the telework eligible DoD personnel before and during the COVID-19 pandemic. We selected the following Components and sub-Components for our audit.

- Army – Office of the Judge Advocate General;
- Navy – Naval Information Warfare Systems Command;
- Air Force – Cyberspace Capabilities Center; and
- DLA.

We selected a statistical sample from the universe of users using the "RAND" function in Microsoft Excel to eliminate selection bias. Next, we randomized the list of users. We used the control testing methodology in the Journal of Public Inquiry, Fall/Winter 2012-2013 to determine our sample size based on the population of users at each DoD Component. We repeated this methodology for each DoD Component.

We statistically selected 153 of 27,791 users from the Army Office of the Judge Advocate General, Naval Information Warfare Systems Command, Air Force Cyberspace Capabilities Center, and the DLA to determine whether users complied with DoD requirements for telework during the maximized telework period. The 153 users were the sum of the users selected for testing across the four DoD Components we assessed. We selected up to 45 users per DoD Component, based on our control testing methodology. If there were no exceptions, the control test passed and we concluded with 90-percent confidence that the error rate in the population is less than or equal to 5 percent. If we identified one or more exceptions, the control test failed, and, therefore, we could not conclude with 90-percent confidence that the error rate in the population was less than or equal to 5 percent.

Use of Computer-Processed Data

We used computer-processed data from systems and networks maintained by the Army OTJAG, Naval Information Warfare System Command, Air Force Cyberspace Capabilities Center, and the DLA to develop a universe of users who were eligible to telework during the COVID-19 pandemic at the four Components. Specifically, we used a manually developed list of OTJAG telework eligible personnel using information provided by OTJAG supervisors. To assess the reliability of the data, we compared the list to the users listed in in the Automated Time Attendance and Production System and OTJAG active directory. We then reviewed telework agreements and telework training certificates for OTJAG users. Therefore, the

list of users was sufficiently reliable to test whether eligible teleworkers had an approved telework agreement and completed the required telework training. As reported in our findings, we used the data to:

- generate a sample of users to validate telework agreements and training certificates; and
- develop recommendations for implementing controls to verify that personnel completed telework agreements and required training before teleworking.

The Naval Information Warfare System Command gave us a list of users who were eligible to telework during the COVID-19 pandemic from its time keeping system, the Navy Enterprise Resource Planning. Naval Information Warfare System Command payroll administrative personnel generated a list of teleworkers using approved time records that included telework codes.[36] We used the list to select a sample of personnel to verify their authorization to telework before the DoD maximized its telework environment. We reviewed telework agreements for completeness and telework training certificates to verify personnel completed required training.

In addition, the DLA gave us a list of users who were eligible to telework during the pandemic from its Employee Activity Guide for Labor Entry Telework Management system to generate a list of personnel that teleworked during the pandemic. We used the list to select a sample of personnel to verify that teleworkers were authorized to telework before the DoD maximized its telework environment. We compared approved telework agreements and telework training certificates to the list of authorized teleworkers.

We used a manually developed Microsoft Excel spreadsheet from the Air Force Cyberspace Capabilities Center to determine the universe of telework eligible users. The spreadsheet was not sufficiently reliable because the Air Force Cyberspace Capabilities Center did not identify whether the list of eligible teleworkers was generated from a Federal or DoD system that tracked eligible teleworkers. We compared the list of Cyberspace Capabilities Center telework eligible personnel to telework agreements and telework training certificates.

[36] Telework codes are approved, designated codes that are used when an employee is allowed to perform work at an approved alternative worksite such as home or a telework center.

Use of Technical Assistance

The DoD OIG Quantitative Methods Division provided assistance in developing the nonstatistical sampling methodology that we used to select a sample of user telework agreements.

Prior Coverage

During the last 5 years, the DoD Office of Inspector General (OIG) issued two reports discussing the DoD's preparedness for natural disasters and the protection of controlled unclassified information. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/reports.html/.

DoD OIG

Report No. DODIG-2019-086, "Audit of the DoD's Preparation for Natural Disaster," May 16, 2019

> The DoD OIG determined that the DoD developed a framework for natural disaster preparedness, which includes guidance, scenario exercise, and corrective action programs. In addition, Joint Chiefs of Staff, Office of the Assistant Secretary of Defense for Homeland Defense and Global Security, U.S. Northern Command, U.S. Army Corps of Engineers, and the DLA developed policies and procedures to plan and prepare for natural disaster events. Furthermore, the DoD Components developed after-action reports to incorporate lessons learned into future operations.

Report No. DODIG-2019-105, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems," July 23, 2019

> The DoD OIG determined that DoD contractors did not consistently implement DoD-mandated system security controls for safeguarding Defense information. In addition, DoD Component contracting offices and requiring activities did not verify that contractor's networks and systems met security requirements or that contractors implemented minimum security controls for protecting CUI. Furthermore, DoD Component contracting offices and requiring activities did not implement processes and procedures to track which contractors maintain on their networks and systems.

Appendix B

Federal and DoD Cybersecurity Guidance

NIST and DoD guidance establishes cybersecurity standards for protecting DoD networks that support telework activities. The standards apply to network and application security, configuration management, risk management, and data protection. The guidance is designed to prevent and reduce vulnerabilities that malicious cyber actors can use to compromise DoD networks. Table 3 contains a description of NIST and DoD guidance.

Table 3. NIST and DoD Guidance

NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, Updated as of January 22, 2015
NIST SP 800-53 provides guidelines for selecting security controls used by organizations and information systems that support executive agencies of the U.S. Government. The guidelines apply to all components of an information system that process, store, or transmit Federal information.
NIST SP 800-114, "User's Guide to Telework and Bring Your Own Device Security," July 2016
NIST SP 800-114 provides information to users on security considerations for several types of remote access solutions and makes recommendations for securing a variety of telework, remote access, and bring your own device technologies.
NIST SP 800-77, Revision 1, "Guide to Internet Protocol Security VPNs," June 2020
NIST SP 800-77 provides guidance for mitigating risks associated with the transmission of sensitive information across networks by implementing Internet Protocol Security services. Internet Protocol Security are the standards for ensuring private communication over public networks, and is typically used to encrypt network traffic between hosts to create a VPN.
DoD Instruction 5200.48, "Controlled Unclassified Information," March 6, 2020
DoD Instruction 5200.48 requires DoD agencies to establish a CUI processes, policies, and procedures for sharing, marking, safeguarding, storing, disseminating, destroying, and managing of the CUI. CUI is information that requires safeguarding or dissemination controls in accordance with laws, regulations, and Government-wide policies. DoD personnel are authorized to access CUI while teleworking but must ensure that the CUI is safeguarded by marking, storing, disseminating, and destroying information that is not cleared for public release in accordance with DoD Instruction 5200.48.
DoD Instruction 1035.01, "Telework Policy," April 4, 2012, Incorporating Change 1, April 7, 2020
DoD Instruction 1035.01 establishes the policy, responsibilities, and procedures for DoD telework programs. It discusses the telework eligibility requirements for DoD employees, which includes a signed telework agreement between the employee and the supervisor, and telework training, which is required before an employee is authorized to telework.
DoD Instruction 8531.01, "DoD Vulnerability Management," September 15, 2020
DoD Instruction 8531.01 establishes policy, assigns responsibilities, and provides procedures for DoD vulnerability management, and response to vulnerabilities identified in all software, firmware, and hardware within the DoD Information Network.
Windows 10 Security Technical Implementation Guide, Version 1, Release 23, June 17, 2020
The Windows 10 Security Technical Implementation Guide is a tool to improve the security of DoD information systems that use Windows 10. The STIG complies with and implements applicable DoD cybersecurity policies, standards, and security controls.

Source: The DoD OIG.

Management Comments

Chief Information Officer, Department of Defense

~~CUI~~

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

FEB 1 2 2021

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Review of DoD Inspector General "Audit of Maintaining Cybersecurity in COVID-19 Telework Environment" (D2020-D000CR-0119.000) Draft Report

This is the Department of Defense (DoD) Chief Information Officer (CIO) response to the DoD Inspector General Report, Audit of Maintaining Cybersecurity in COVID-19 Telework Environment" (D2020-D000CR-0119.000) Draft Report.

DoD IG RECOMMENDATION 1.a.: ~~(CUI)~~ Direct the Defense Information Systems Agency to review the language in the Virtual Private Network Security Requirements Guide (VPN SRG) and revise the guide to include specific language [redacted]

DoD CIO RESPONSE 1.a.: The DoD CIO disagrees with revising the VPN SRG to include the addition of specific language that [redacted] DISA concluded that [redacted] could have a negative impact on the organizations within the Department. Further explanation is provided within the attached response from DISA.

DoD IG RECOMMENDATION 1.b.: Direct the DoD Deputy Chief Information Officer for Information Enterprise to [redacted]

DoD CIO RESPONSE 1.b.: The DoD CIO will direct the DoD Deputy Chief Information Officer for Information Enterprise to [redacted]

A security review to verify "CONTROLLED UNCLASSIFED INFORMATION" (CUI) markings in the report has been completed and there are no additional recommendations. The point of contact for this matter is [redacted]. He can be reached at [redacted] or [redacted].

John B. Sherman
Acting

Attachment:
As stated

~~CUI~~

Risk Management Executive, Defense Information Systems Agency

DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

3 February 2021

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Audit of Maintaining Cybersecurity in the Coronavirus Disease–2019 Telework Environment (Project No. D2020-D000CR-0119.000)

Thank you for providing the opportunity to comment on the draft audit report. As requested, the Defense Information Systems Agency (DISA) reviewed the language in the Virtual Private Network (VPN) Security Requirements Guide (SRG). We disagree with adding specific language requiring DoD components [redacted] When developing the VPN SRG, we considered [redacted] for which a [redacted] We concluded that [redacted] could have a negative impact on the organizations within the Department. Including a [redacted] several concerns; some of which actually degrade security.

The first problem this creates is it immediately impacts those organizations who have opted to leverage "Always-On" VPN solutions such as Microsoft's Always-On VPN. An "Always-On" VPN limits exposure to threats that exist on the user's local network because all traffic is tunneled back to the enterprise. When users are remote and they connect to any Internet-connected network, their Windows devices automatically create a VPN back to the organization's enterprise network gateway in the background. This eliminates user-based enforcement aspect of using a VPN since it is enforced automatically and it also enables endpoint device authentication. This approach provides organizations the assurance of knowing their devices are always tunneled back to the organization and subjected to the protections in their network security stacks; enabling them to monitor devices at all times when they are powered on and connected.

[redacted] up VPN resources and disconnect the user from the network. However, other STIG requirements [redacted] Disconnecting a host from a [redacted] This actually creates an opportunity for exposure to the host, locally or from the Internet, depending on the infrastructure of the remote environment. Each organization will be different in terms of the mitigations they have (e.g., security software on the endpoints) and what their priorities are with respect risk, cost, resources, and mission.

[redacted]

Risk Management Executive, Defense Information Systems Agency (cont'd)

As described in the DoD IG report, some organizations may be resource-constrained. [redacted]

In conclusion, DISA agrees that as a general rule of thumb [redacted] However, VPNs account for more than just user activity. In our opinion, [redacted] may be overly restrictive and can result in negative impacts to DoD Components. Many factors will contribute to each [redacted] As such we have opted to allow each organization the latitude to conduct their own risk assessment and [redacted]

There is no significant monetary benefit to implementing this recommendation. If you have questions, my point of contact is [redacted], email: [redacted].

GREENWELL.ROGER.SCOTT.SR[redacted] Digitally signed by GREENWELL.ROGER.SCOTT.SR[redacted] Date: 2021.02.03 16:41:14 -05'00'

ROGER S. GREENWELL
Risk Management Executive/
Authorizing Official

2

Chief Information Officer, Department of the Army

DEPARTMENT OF THE ARMY
OFFICE OF THE CHIEF INFORMATION OFFICER
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

SAIS-CSP

MEMORANDUM FOR Department of Defense Office of Inspector General (DoDIG), 4800 Mark Center Drive, Alexandria, VA 22350-1500

SUBJECT: Draft Report, Audit of Maintaining Cybersecurity in the Coronavirus Disease-2019 Telework Environment (Project No. D2020-D000CR-0119.000)

1. The Chief Information Officer response to the subject draft report is enclosed.

2. The point of contact for this memorandum is [redacted], [redacted] or [redacted].

JOSEPH.CHRISTOPHER.A.JR.[redacted]
Digitally signed by JOSEPH.CHRISTOPHER.A.JR.[redacted]
Date: 2021.02.12 15:07:38 -05'00'

Encl

CHRISTOPHER A. JOSEPH JR.
Acting Division Chief
Policy and Risk Governance Division

Chief Information Officer, Department of the Army (cont'd)

Inspector General, Department of Defense Draft Report,
Audit of Maintaining Cybersecurity in the Coronavirus Disease-2019 Telework Environment (Project No. D2020-D000CR-0119.000)

Army Chief Information Officer Reply to Recommendation 2

DoDIG Recommendation 2

~~(CUI)~~ We recommend that the Army Chief Information Officer develop, implement, and enforce a plan to:

a. ~~(CUI)~~ Set [redacted] for virtual private network sessions.
b. Mitigate [redacted]
c. Verify that DoD personnel complete telework agreements and the required DoD telework training before teleworking.

Army Chief Information Officer Comments to Recommendation 2:

a. Recommendations 2a. and 2b. should not be addressed to the Army Chief Information Officer. These recommendations should be addressed to Army Cyber Command (ARCYBER).

Rationale: In accordance with Army Regulation 25-2, Army Cybersecurity, ARCYBER has the responsibility to plan and direct cybersecurity protective measures on the Army's portion of the DODIN at the strategic and operational levels.

b. Recommendation 2c. should not be addressed to the Army Chief Information Officer. This recommendation should be addressed to DCS G-1, specifically AG-1CP. AG-1CP agrees with the redirection of 2C to the Office of the DCS, G-1, but with a modification to the DoDIG's recommendation, based on existing HR authorities.

"Recommendation: AG-1CP recommends the Office of the DCS, G-1 remind Commands that supervisors are required to ensure their employees complete telework agreements and complete DoD telework training before authorizing their employees to telework."

Rationale: The Telework Enhancement Act of 2010 and DoDI 1035.01, Telework Policy, already require supervisors to ensure their employees complete telework agreements (DD Form 2946) and telework training as a condition for telework participation. AG-1CP does not have the authority to enforce or verify existing telework requirements, as that authority is delegated from the Agency Head (DoD) to the Component Head (Secretary of the Army) to Commands for further delegation to the appropriate supervisory level. AG-1CP can send a message to Commands requesting they remind supervisors of the existing requirements.

Chief Information Officer, Department of the Navy

DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

22 February 2021

FOR: Department of Defense Office of Inspector General

FROM: Mr. Aaron D. Weis, Special Assistant for Information Management/Chief Information Officer

SUBJ: DoD Inspector General Draft report on Audit of Maintaining Cybersecurity in the Coronavirus Disease–2019 Telework Environment Project No. D2020-D000CR-0119.000

The Department of the Navy Chief Information Officer concurs with recommendation 4 of the DoD Inspector General Draft report on Audit of Maintaining Cybersecurity in the Coronavirus Disease–2019 Telework Environment Project No. D2020-D000CR-0119.000

My point of contact for this recommendation is [redacted], [redacted], [redacted].

WEIS.AARON.D.[redacted] Digitally signed by WEIS.AARON.D.[redacted] Date: 2021.02.22 16:45:20 -05'00'

Aaron D. Weis
Department of the Navy
Chief Information Officer

Chief Information Officer, Department of the Air Force

DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

18 February 2021

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

FROM: SAF/CN
1800 Air Force Pentagon Suite 4E226
Washington, DC 20330

SUBJECT: Air Force Response to DoD Office of Inspector General Draft Report, Audit of Maintaining Cybersecurity in the Coronavirus Disease-2019 Telework Environment (Project No. D2020-D000CR-0119.000)

1. This is the Department of the Air Force response to the DoDIG Draft Report, Audit of Maintaining Cybersecurity in the Coronavirus Disease-2019 Telework Environment (Project No. D2020-D000CR-0119.000).

2. The Department of the Air Force Chief Information Officer generally concurs with the report and welcomes the opportunity to provide a response. The Chief Information Officer and the Deputy Chief of Staff for Manpower, Personnel, and Services in coordination with the MAJCOMs will correct issues identified in this report, and develop and implement a corrective action plan outlined in the following recommendations:

RECOMMENDATION 5: The DODIG recommends the Air Force Chief Information Officer develop, implement, and enforce a [redacted]

AIR FORCE RESPONSE: The Air Force concurs with the requirement to develop, implement, and enforce a plan to mitigate vulnerabilities in a timely manner. Methods and Procedures Technical Order (MPTO) 00-33A-1109, AIR FORCE INFORMATION NETWORK (AFIN) VULNERABILITY MANAGEMENT, published 26 January 2021, establishes the identification, notification, and remediation procedures and timelines to mitigate vulnerabilities in a timely manner. Enforcement of this technical order is a command responsibility. However, the limited information included in the draft report as derived from the 83rd NOS CCRI (Aug 2020) revealed a conflict between guidance on the creation of the POA&M, with the CCRI requirements outlining 90 days regardless of criticality, and U.S. Cyber Command Tasking Order 14-0290 requiring a POA&M or correction of critical findings within 15 days. Therefore, the Air Force believes a thorough review of DAF, USCYBERCOM, and other DoDIN level vulnerability management guidance is required to identify conflicts and determine a standardized requirement for resolution and/or reporting across the force. This guidance is to be included in our Concept of Operations (CONOPs) for the AFIN by 30 Oct 2021.

Chief Information Officer, Department of the Air Force (cont'd)

RECOMMENDATION 6: The DODIG recommends the Deputy Chief of Staff for Manpower, Personnel, and Services verify that DoD personnel completed telework agreements and the required DoD telework training before teleworking.

AIR FORCE RESPONSE: The Air Force concurs with the requirement that all DoD personnel completed telework agreements and the required DoD telework training before teleworking. The Air Force suggests that this recommendation be reworded to state "We recommend that the Air Force Deputy Chief of Staff for Manpower, Personnel, and Services (AF/A1) develop and issue guidance, including verification procedures, to ensure that DoD personnel completed telework agreements and the required DoD telework training before teleworking" as the Air Staff role in this area is to provide policy guidance. Responsibility for ongoing verification of training and completed agreements resides with commanders and directors. This change provides AF/A1 the flexibility to develop effective guidance to meet this recommendation. The proposed corrective action is a review and update to AFI 36-816, "Civilian Telework Program" with an estimated completion date of 30 March 2022.

3. The Air Force Point of Contact is [redacted], [redacted], [redacted], or email [redacted].

BEAUCHAMP.WINSTON.A[redacted]
Digitally signed by BEAUCHAMP.WINSTON.A[redacted]
Date: 2021.02.18 10:22:40 -05'00'

WINSTON A. BEAUCHAMP, SES, DAF
Deputy Chief Information Officer

Deputy Commander, U.S. Army Cyber Command

CUI

DEPARTMENT OF THE ARMY
U.S. ARMY CYBER COMMAND
930 15TH STREET
FORT GORDON, GEORGIA 30905-5228

ARCC-IR

MEMORANDUM FOR DOD Inspector General Audit of Maintaining Cybersecurity in the Coronavirus Disease-2019 Telework Environment, Attention: [redacted], Program Director for Audit Cyberspace Operations, 4800 Mark Center Drive, Alexandria, VA 22350-1500

SUBJECT: Project No. D2020-D000CR-0119.000, Draft Audit Report on "Audit of Maintaining Cybersecurity in the Coronavirus Disease-2019 Telework Environment," 12 January 2021

1. (U) ARCYBER/NETCOM concurs in part with Recommendation 2 as stated in the report, with the following comments:

a. ~~(CUI)~~ **Recommendation:** Set [redacted] for virtual private network sessions. **Response:** Concur with comment.

(1) NETCOM is [redacted] Especially in an environment of maximum telework, [redacted]

(2) The Army will follow DISA STIG guidance and, at this time, there [redacted]

b. **Recommendation:** Mitigate [redacted] **Response:** Concur with comment. This is basic hygiene and should be encouraged at all levels. Recommend the grading criteria fall in line with the DoD scorecard.

c. **Recommendation:** Verify that DoD personnel complete telework agreements and the required DoD telework training before teleworking. **Response:** Concur with comment. This is more appropriately an HQDA G-1 responsibility.

2. (U) The ARCYBER point of contact for this action is [redacted], Director of Internal Review [redacted], or [redacted], or [redacted], Senior Auditor at [redacted] or [redacted].

JONES.RAYMOND.DEAN [redacted] Digitally signed by JONES.RAYMOND.DEAN [redacted] Date: 2021.02.22 10:33:49 -05'00'

RAYMOND D. JONES
Deputy Chief of Staff, ARCYBER

CUI

Commander, U.S. Fleet Cyber Command, Department of the Navy

DEPARTMENT OF THE NAVY
COMMANDER, U.S. FLEET CYBER COMMAND/
9800 SAVAGE ROAD, SUITE 6586
FORT GEORGE G. MEADE MARYLAND 20755-6586

3000
Ser N00/096
26 Feb 21

From: Commander, U.S. Fleet Cyber Command/Commander, U.S. TENTH Fleet
To: Office of Inspector General, U.S. Department Of Defense

Subj: AUDIT OF MAINTAINING CYBERSECURITY IN THE CORONAVIRUS DISEASE-2019 TELEWORK ENVIRONMENT
(Project No. D2020-D000CR-0119.000)

1. Commander, Fleet Cyber Command (FCC) has reviewed the subject report and provides the following formal response:

a. The FCC General Counsel indicated that he "finds no basis to maintain the legacy marking of "FOUO" or to apply the CUI marking for sections in the draft report related to the Navy, specifically including references to policies implemented by U.S. Fleet Cyber Command.

b. Recommendation 3 states, ***" We recommend that the Commander, U.S. Fleet Cyber Command reconsider his decision to*** [redacted] ***in accordance with Navy and the Defense Information Systems Agency policies."***

c. Commander, FCC Response: Commander concurs with comment: FCC agrees with this recommendation and has already reconsidered the decision to [redacted] accordance with Navy and the Defense Information Systems Agency policies and reverted back to [redacted] Dormant accounts under the affected policies are being disabled and deleted per interim timelines which optimally balance mission requirements and cyber security concerns. When max telework policies are relaxed and routine network access is restored, policies will revert to standing OPNAV mandates.

M. H. WELSH
Chief of Staff

Acronyms and Abbreviations

CIO	Chief Information Officer
COVID-19	Coronavirus Disease–2019
CUI	Controlled Unclassified Information
CVR	Commercial Virtual Remote
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
NIST	National Institute of Standards and Technology
SP	Special Publication
OTJAG	Office of the Judge Advocate General
VDI	Virtual Desktop Infrastructure
VPN	Virtual Private Network

Glossary

Active Directory. A Microsoft technology used to manage computers and other devices on a network that allows network administrators to create and manage groups of computers, users, and computer interaction within a network.

Availability. Ensuring timely and reliable access to and use of information.

Commercial Virtual Remote Environment. Platform created by the DoD to move towards large-scale telework posture in response to the COVID-19 emergency. The tool provides the DoD with collaboration capabilities to facilitate continuity of operations.

Confidentiality. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Management. A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

Controlled Unclassified Information. Information created or possessed on behalf of the Government that requires safeguarding or dissemination controls according to applicable laws, regulations, and Government-wide policies.

Cyber Attack. An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure, destroying the integrity of the data, or stealing controlled information.

Endpoint Device. The term is used for Internet-connected hardware on a network. Endpoint devices can include desktop or laptop computers, as well as portable devices such as tablets and smartphones.

Host-Based Security. A set of capabilities that provide a framework to implement a wide-range of security solutions on hosts. This framework includes a trusted agent and a centralized management function that together provide automated protection to detect, respond, and report host-based vulnerabilities and incidents.

Integrity. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Internet Protocol Security. A framework of open standards for ensuring private, secure communications over networks, using cryptographic security services.

Pandemic. A worldwide spread of a new disease that occurs when a new virus emerges and spreads around the world, and most people do not have immunity.

Patch. A "repair job" for a piece of programming; also known as a "fix." A patch is the immediate solution that is provided to users; it can sometimes be downloaded from the software maker's web site.

Phishing. A form of social engineering that uses email or malicious websites to solicit personal information by posing as a trustworthy organization.

Plan of Action and Milestones. Facilitates a disciplined and structured approach to tracking risk mitigation activities. Also, describes the current disposition of any discovered vulnerabilities and system findings, and includes a communication service provider's intended corrective actions for those findings.

Remote Access. Access to an organization's nonpublic information system by an Authorized user (or information system) communicating through an external, Non-organization-controlled network.

Risk Management. The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities, (ii) assessing risk, (iii) responding to risk once determined, and (iv) monitoring risk over time.

Safeguards. Protective measures prescribed to meet the security requirements (for example, confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Security Requirements Guide. Collection of requirements that mitigate sources of security vulnerabilities consistently and commonly encountered across information technology systems and applications.

Secure Sockets Layer. A secure protocol developed for sending information securely over the Internet, where only the user's computer and the secure server are able to recognize the data.

Security Technical Implementation Guide. Implementation guide geared to a specific product and version. Contains all requirements that have been flagged as applicable for the product which have been selected on a DoD baseline.

Social Engineering. An attack that uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems.

Telework. The ability for an organization's employees and contractors to conduct work from locations other than the organization's facilities.

Telework Codes. Approved, designated codes that are used when an employee is allowed to perform work at an approved alternative worksite such as home or a telework center.

Virtual Desktop Infrastructure. A technology that refers to the use of virtual machines to provide and manage virtual desktops. VDI hosts desktop environments on a centralized server and deploys them to end-users on request.

Virtual Private Network. A protected information system link using security controls to give the impression of a dedicated line.

Vulnerability. Weakness in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat.


INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
INTEGRITY
EFFICIENCY

Whistleblower Protection
U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible waste, fraud, and abuse in government programs. For more information, please visit the Whistleblower webpage at http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whisteblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoD OIG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098