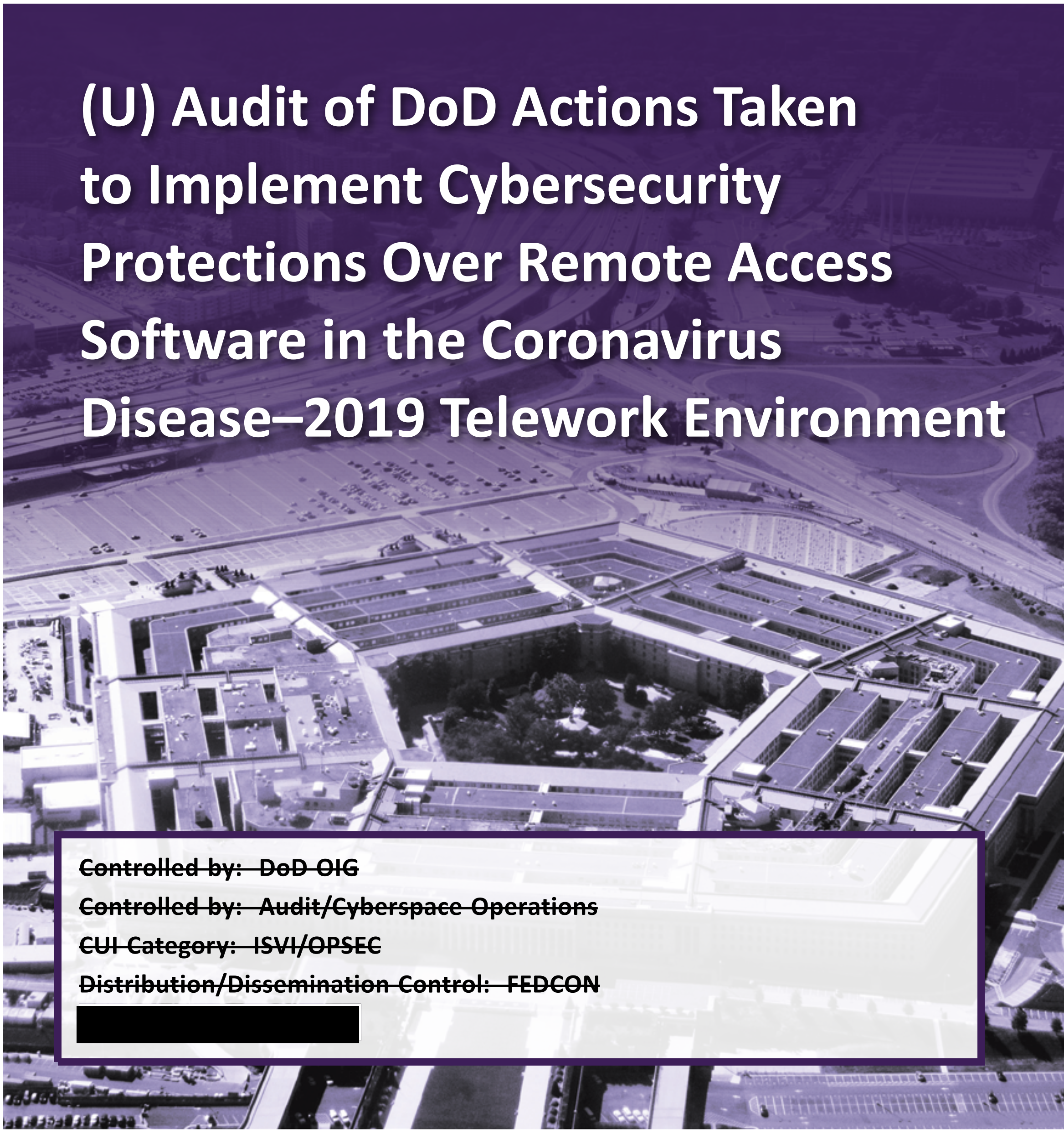
Report No. DODIG-2023-057

INSPECTOR GENERAL

U.S. Department of Defense

MARCH 24, 2023



(U) Audit of DoD Actions Taken to Implement Cybersecurity Protections Over Remote Access Software in the Coronavirus Disease–2019 Telework Environment

~~Controlled by: DoD OIG~~
~~Controlled by: Audit/Cyberspace Operations~~
~~CUI Category: ISVI/OPSEC~~
~~Distribution/Dissemination Control: FEDCON~~
[redacted]

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

(U) Results in Brief

(U) Audit of DoD Actions Taken to Implement Cybersecurity Protections Over Remote Access Software in the Coronavirus Disease–2019 Telework Environment

(U) March 24, 2023

(U) Objective

(U) The objective of this audit was to determine the actions taken by the DoD to configure remote access software used to facilitate telework during the coronavirus disease–2019 (COVID-19) pandemic to protect DoD networks and systems from potential malicious activity. We also determined the extent to which the DoD implemented security controls to protect remote connections to its networks.

(U) Background

(U) Remote access software allows personnel to access a computer or network from a geographical distance through an external network connection, such as the Internet. To facilitate telework, DoD personnel gained access to their organization's networks using approved remote access software.

(U) DoD policies require DoD Components to configure remote access software consistent with Federal and DoD cybersecurity policies, standards, and security controls. In addition, the Defense Information Systems Agency (DISA) publishes Security Requirement Guides and Security Technical Implementation Guides that provide guidance for configuring remote access software.

(U) Findings

(U) Network and system administrators for 7 of the 10 DoD Components that we assessed did not always implement all critical configuration settings and cybersecurity controls to reduce the risk of exposing DoD networks and systems to potential malicious activity.

(U) Findings (cont'd)

(U) If DoD Components do not consistently configure remote access software in accordance with Federal and DoD cybersecurity policies, standards, and security controls, malicious cyber actors could exploit vulnerable configuration settings; and compromise the confidentiality, integrity, and availability of DoD networks, systems, and data. It is important that officials responsible for authorizing the use of remote access software on DoD Component networks document an assessment of the impact to DoD employees, assets, and missions when DoD Components deviate from security requirements.

(U) Recommendations

(U) Among other recommendations, we recommend, that the Component Directors and Chief Information Officers implement the configurations controls identified in the report or formally accept the risks of not implementing the configuration settings. In addition, we recommend that the DISA Joint Service Provider Director direct network and system administrators to include mitigation timeframes for all vulnerabilities and develop plans of actions and milestones for all vulnerabilities not mitigated in a timely manner.

(U) Management Comments and Our Response

(U) Officials from the Marine Corps, Department of the Navy, U.S. Southern Command, and Defense Intelligence Agency, agreed with the recommendations and described actions planned and taken to resolve or close the recommendations. Comments from the Deputy Chief Information Officer for the Air Force and the Chief of the DISA Joint Service Provider Cyber Security Center partially addressed the specifics of the recommendations; therefore, we request additional comments from them within 30 days on the final report.

(U) Please see the Recommendations Table on the next page for the status of recommendations.

(U) Recommendations Table

(U) Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Chief Information Officer, Department of the Air Force	A.2.a, A.2.b	None	None
Director, Marine Corps Information Command, Control, Communications, and Computers	None	A.5.a, A.5.b	None
Chief Information Officer, Naval Surface Warfare Center – Panama City Division	None	None	A.3
Director, U.S. Southern Command – Joint Interagency Task Force South Command, Control, Communications, Computers, Cyber and Intelligence	None	None	A.1
Director, Defense Information Systems Agency Joint Service Provider	A.6	B.1	None
Chief Information Officer, Defense Intelligence Agency	None	A.4.a, A.4.b	None **(U)**

(U) Please provide Management Comments by April 24, 2023.

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

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

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

March 24, 2023

MEMORANDUM FOR DISTRIBUTION

SUBJECT: (U) Audit of DoD Actions Taken to Implement Cybersecurity Protections Over Remote Access Software in the Coronavirus Disease–2019 Telework Environment (Report No. DODIG-2023-057)

(U) This final report provides the results of the DoD Office of 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 report when preparing the final report. These comments are included in the report.

(U) This report contains three recommendations that are considered unresolved because management officials did not fully address the recommendations presented in the report. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section of this report, the recommendations remain open. We will track these recommendations until an agreement is reached on the actions that need to be taken to address the recommendations, and management submits adequate documentation showing that all agreed-upon actions are completed.

(U) This report contains five recommendations that are considered resolved. Therefore, as described in the Recommendations, Management Comments, and Our Response section of this report, we will close the recommendations when documentation showing that all agreed-upon actions to implement the recommendations are completed.

(U) This report contains two recommendations that are considered closed. Management comments and associated actions addressed the recommendation in this report, and we consider the recommendation closed.

(U) DoD Instruction 7650.03 requires that recommendations be resolved promptly. Therefore, please provide us within 30 days your response concerning specific actions in process or alternative corrective actions proposed on the recommendations. 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.

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

FOR THE INSPECTOR GENERAL:

Carol N. Gorman

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations and Acquisition,
Contracting, and Sustainment

(U) Distribution:

COMMANDER, U.S. SOUTHERN COMMAND
COMMANDER, U.S. STRATEGIC COMMAND
DIRECTOR, DEFENSE CONTRACT MANAGEMENT AGENCY
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE INTELLIGENCE AGENCY
DIRECTOR, DOD EDUCATION ACTIVITY
AUDITOR GENERAL, DEPARTMENT OF THE NAVY
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

(U) Contents

(U) Introduction

(U) Finding A. DoD Components Generally Configured Remote Access Software to Protect DoD Networks and Systems 6

(U) Finding B. DoD Components Generally Implemented Cybersecurity Controls to Protect DoD Networks and Systems 21

(U) Appendixes

(U) Contents (cont’d)

(U) Management Comments

(U) Introduction

(U) Objective

(U) The objective of this audit was to determine the actions taken by the DoD to configure remote access software used to facilitate telework during the coronavirus disease–2019 (COVID-19) pandemic to protect DoD networks and systems from potential malicious activity. We also determined the extent to which the DoD implemented security controls to protect remote connections to its networks.

(U) We conducted this audit in response to a request from the House Committee on Oversight and Reform to assess vulnerabilities created or intensified by the increased use of telework during the COVID-19 pandemic specific to the use of collaboration tools and remote access software. This report focuses on the DoD's use of remote access software, and we will issue a separate report focusing on the DoD's use of collaboration tools.[1] See Appendix A for a discussion on the scope and methodology, and Appendix B for our detailed sampling approach for selecting the DoD Components we assessed during this audit. See Appendix C for a copy of the request letter from the House of Representatives, Committee on Oversight and Reform. See the Glossary for the definitions of technical terms.

(U) Background

(U) Remote access software allows teleworking personnel to access a computer or network from a geographical distance through an external network connection, such as the Internet. The remote access methods that teleworkers most commonly use include tunneling, portals, remote desktop solutions, and direct application access.

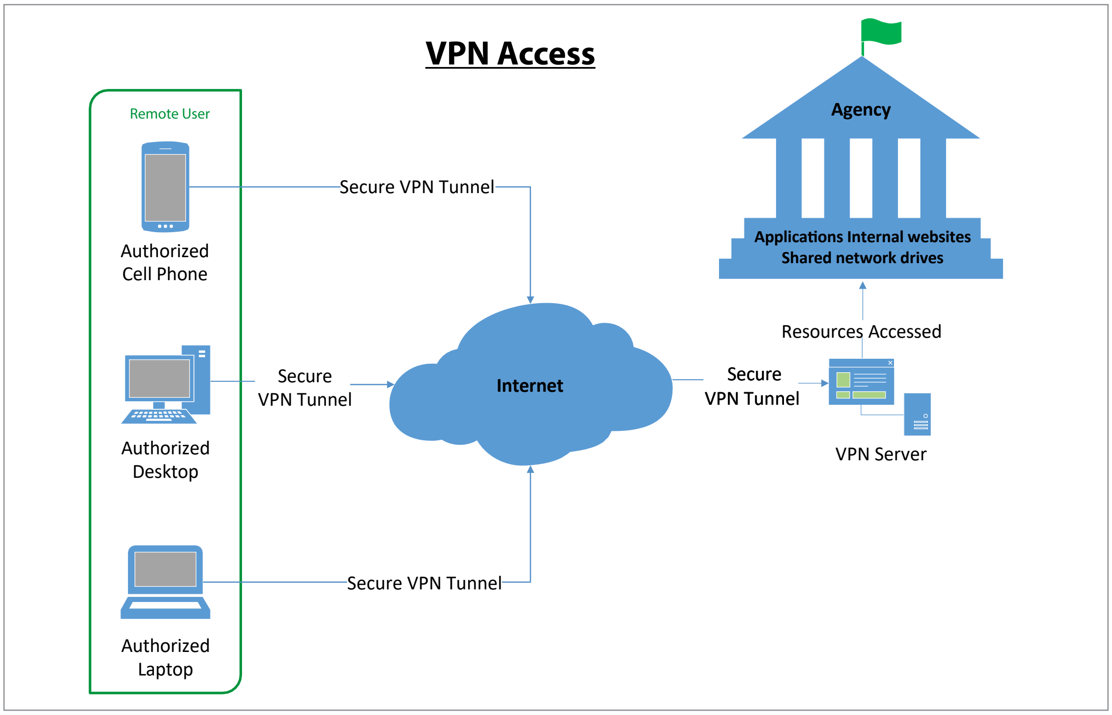
- (U) Tunneling – A secure connection to transmit information between networks. Tunnels are typically established through a virtual private network (VPN).
- (U) Portal – A server that offers access to one or more applications using a single centralized interface, such as a virtual desktop infrastructure (VDI).
- (U) Remote Desktop solution – Gives a teleworker the ability to remotely control a particular computer at an organization, most often the user's own computer.
- (U) Direct Application Access – Allows a user to access an application directly, such as webmail, without using remote access software.

[1] (U) On December 6, 2021, the DoD OIG announced the "Audit of DoD Actions Taken to Protect DoD Information When Using Collaboration Tools During the COVID-19 Pandemic" (Project No. D2022-D000CR-0038.000).

(U) Remote Access Software Approved to Support Maximum Telework

(U) On March 27, 2020, the Secretary of Defense directed maximum telework for personnel who use the DoD Non-Classified Internet Protocol Routing Network to perform their primary duties.[2] To facilitate telework, DoD personnel access their Component's network using approved remote access software, such as a VPN, to remotely connect a laptop or other device, which is generally government-furnished equipment. The VPN routes the device to a VPN gateway using the employee's Internet. Once a connection is established, an employee can access many of the organization's computing resources. Figure 1 shows an example of a VPN architecture.

(U) Figure 1. Virtual Private Network Architecture



(U) Source: The DoD OIG.

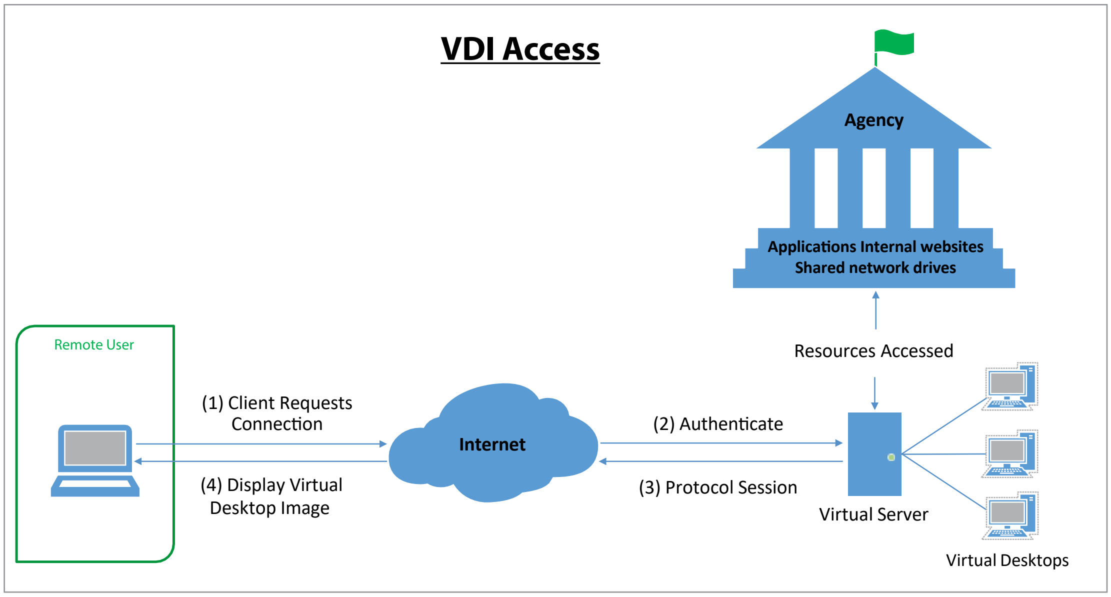
(U) The DoD's approved VPN solutions include Cisco AnyConnect, F5 VPN, and Pulse Secure VPN. The types of VPN most commonly used for DoD teleworkers are Internet Protocol Security and Secure Sockets Layer connections.[3]

[2] (U) Non-Classified Internet Protocol Routing Network is a network used by DoD personnel to exchange unclassified information.

[3] (U) Internet Protocol Security adds security features to the standard Internet Protocol to provide confidentiality and integrity services. A Secure Sockets Layer is a protocol used to protect private information during the transmission of data over the Internet. While both security controls can be configured to provide protections, such as confirming the identity of each endpoint device to ensure that data is sent from the expected device, there are differences between the security controls. For example, Internet Protocol Security can conceal the identities of communicating parties while Secure Sockets Layer cannot.

(U) As an alternative to VPN, some DoD Components use VDI. VDI allows a teleworker to remotely access a virtual desktop through a centralized server and display it on the teleworker's laptop. Once teleworkers access the virtual desktop, they can select applications to perform their work as usual. Figure 2 shows an example of a VDI architecture.

(U) Figure 2. Architecture for Virtual Desktop Infrastructure



(U) Source: The DoD OIG.

(U) The DoD's approved VDI solutions include VMware Horizon, Citrix Virtual Desktop, and Microsoft Azure Virtual Desktop.

(U) Cybersecurity Controls and Configuration Settings

(U) 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 DoD networks.
For example, network and system administrators could use cybersecurity controls such as multifactor authentication to increase the level of assurance in the authentication process. DoDI 8510.01 requires DoD Components to implement cybersecurity controls in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53.[4]

[4] (U) DoDI 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022. NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 5, Updated December 10, 2020.

(U) Configuration management, a subset of cybersecurity controls, is the process of maintaining compliance with cybersecurity requirements on information technology hardware and software by initializing, changing, and monitoring the configuration settings of the hardware and software. Configuration settings are a set of parameters that network and system administrators can change that affect the security posture and functionality of hardware and software. For example, system administrators can configure remote access software to prevent users from uploading files from their personal devices to the network. DoDI 8500.01 requires DoD Components to configure remote access software consistent with DoD cybersecurity policies, standards, and security controls.[5] In addition, DISA publishes Security Requirements Guides (SRGs) and Security Technical Implementation Guides (STIGs) that provide guidance for configuration settings.

(U) DoD Components and Remote Access Software Assessed

(U) We assessed 10 DoD Components that used remote access software. Table 1 shows the DoD Components we assessed and the remote access software used to support telework.

(U) Table 1. DoD Components and Remote Access Software Assessed

(U) DoD Component	Remote Access Software
U.S. Marine Corps (USMC)	Pulse Secure VPN
Naval Surface Warfare Center (NSWC) – Panama City Division (PCD)	Cisco AnyConnect
Department of the Air Force	F5 VPN
U.S. Southern Command (USSOUTHCOM) – Joint Interagency Task Force South (JIATFS)	VMware Horizon View
U.S. Strategic Command	VMware Horizon View
Defense Contract Management Agency (DCMA)	F5 VPN
Defense Information Systems Agency (DISA) Joint Service Provider (JSP)*	VMware Horizon View Citrix Virtual Desktop Route1 MobiKEY Cisco AnyConnect VPN
Defense Intelligence Agency (DIA)	Azure Virtual Desktop
Defense Media Activity	Citrix Virtual Desktop
DoD Education Activity (DoDEA)	Cisco AnyConnect (U)

* (U) The DoD OIG is a limited customer of DISA JSP. While DISA JSP provides services to information systems operated and managed by DoD Components, it only provides the DoD OIG network transport services for its Non-Classified and Secure Internet Protocol Router Networks connections to ensure secure network communication.

(U) Source: The DoD OIG.

[5] (U) DoDI 8500.01, "Cybersecurity," March 14, 2014 (Incorporating Change 1, October 7, 2019).

(U) Review of Internal Controls

(U) DoD Instruction (DoDI) 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.[6] We identified internal control weaknesses related to the configuration of remote access software and the security controls to protect access software. Specifically, USMC, NSWC-PCD, Air Force, USSOUTHCOM-JIATFS, DISA JSP, DIA, and DoDEA did not implement required configuration settings, and DISA JSP did not implement critical cybersecurity controls. We will provide a copy of the report to the senior official responsible for internal controls in the USMC, NSWC-PCD, Air Force, USSOUTHCOM-JIATFS, U.S. Strategic Command, DCMA, DISA JSP, DIA, Defense Media Activity, and DoDEA.

[6] (U) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013, (Incorporating Change 1, June 30, 2020).

(U) Finding A

(U) DoD Components Generally Configured Remote Access Software to Protect DoD Networks and Systems

(U) Network and system administrators for the 10 DoD Components we assessed generally configured remote access software used to facilitate telework during the COVID-19 pandemic to protect DoD networks and systems. Specifically, of the six configuration settings we assessed, network and system administrators at:

- (U) the U.S. Strategic Command, DCMA, and Defense Media Activity had all six configuration settings in place;
- (U) the USMC, NSWC-PCD, Air Force, DISA JSP, DIA, and DoDEA had five of the six configuration settings in place but did not disable inactive user accounts after 35 days; and
- (U) USSOUTHCOM-JIATFS had five configuration settings in place but did not prevent VDI users from uploading files from end-user devices to the network and did not scan the main virtual desktop of the VDI for malware.[7]

(U) If DoD Components do not consistently configure remote access software in accordance with DISA SRG and STIG requirements, malicious cyber actors could exploit vulnerable configuration settings and compromise the confidentiality, integrity, and availability of DoD networks, systems, and data.[8]

(U) In addition, Authorizing Officials (AOs) for the USMC, NSWC-PCD, Air Force, DISA JSP, DIA, DoDEA, and USSOUTHCOM-JIATFS did not formally document the assessment and acceptance of the risks of not implementing DoD configuration settings as required by DoDI 8510.01.[9] The AOs also did not implement compensating configuration settings to provide equivalent or comparable protection for the remote access software. While there may be valid operational needs for DoD Components to deviate from the required settings, it is important that AOs document an assessment of the impact to DoD employees, assets, and missions and acceptance of the risks. NIST SP 800-39 states that senior leaders and executives are ultimately responsible and accountable for risk decisions.[10] The AO's assessment can provide the senior leaders and executives the awareness and basis for the risk acceptance decision.

[7] (U) We identified two weaknesses in the Network Defense configuration category at USSOUTHCOM-JIATFS.

[8] (U) SRGs specify configuration settings for a technology family, such as VPNs. A technology family is a group of related technologies with common characteristics such as applications, networks, or operating systems.
(U) STIGs provide configuration settings DoD Components must follow for specific products used by the DoD, such as VMware Horizon.

[9] (U) For the purposes of this report, we consider a formal risk acceptance a document that includes the configuration requirement; a description of the weakness; the justification for accepting the risk; and the signature of the AO and the date the AO signed the document.

[10] (U) NIST SP 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View," March 2011.

(U) Requirements for Configuring Remote Access Software

(U) Remote access software generally receives higher exposure to external threats than technologies accessed from inside an organization's facilities. DoDI 8500.01 requires DoD Components to configure remote access software consistent with DoD cybersecurity policies, standards, and security controls. In addition, DISA publishes SRGs and STIGs that provide guidance for configuration settings.

(U) We assessed DoD Components' configuration settings for compliance with the applicable SRGs and STIGs. Table 2 identifies the configuration category, importance when configuring remote access software, and examples of the corresponding configuration settings from DISA security guides.

(U) Table 2. Configuration Categories and Their Importance

(U) Configuration Category	Importance When Configuring Remote Access Software	Example of Configuration Settings from DISA Security Guides
Access Management	Access management limits access to the remote access software to authorized users based on their roles and responsibilities. This includes when user accounts should be terminated or disabled after a defined period of inactivity. Outdated or unused accounts provide penetration points that may go undetected and be exploited by malicious actors to gain unauthorized access to compromise DoD networks.	Inactive accounts must be disabled after 35 days of inactivity.
Authentication	Authentication mechanisms verify user identities, processes, or devices as a prerequisite to allowing access to systems through remote access software. Malicious cyber actors can exploit authentication methods that do not use two or more different authentication factors, enforce a minimum password length, require complex passwords, limit unsuccessful log-on attempts, or automatically end-user sessions after a defined period of inactivity. A malicious actor is an individual that uses technology with the intent to cause harm.	User sessions must be re-authenticated after a maximum of 10 hours. **(U)**

(U) Table 2. Configuration Categories and Their Importance (cont'd)

(U) Configuration Category	Importance When Configuring Remote Access Software	Example of Configuration Settings from DISA Security Guides
Encryption	Encryption protects the confidentiality and integrity of DoD data in transit and at rest when accessed by remote access software. Data at rest refers to the state of information when it is not in process or in transit and is located on devices such as hard drives and workstations. DoD Components can protect the confidentiality of DoD data at rest by using encryption. Data in transit refers to the state of information when it is in process or in transit between devices or nodes. The confidentiality and integrity of data in transit must be protected to ensure that unauthorized parties and machines cannot read, copy, or modify the information.	Devices must be configured to encrypt information stored on and transmitted between devices to protect the confidentiality and integrity of the information.
Inactive User Sessions	Locking inactive user sessions prevents access to DoD Component systems when users stop work and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences.	The application must be configured to terminate an individual user's session after 15 minutes of inactivity. The user must re-authenticate and a new session must be established to continue work in the application.
Unsuccessful Logon Attempts	Locking user accounts after consecutive failed logon attempts prevents unauthorized individuals from gaining access to networks and systems.	The account lockout feature is set to three attempts or less to minimize the possibility of a successful password attack.
Network Defense	Network boundaries can use firewalls, antivirus software, and intrusion-detection tools to monitor and respond to unusual activity that may contain malicious code. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can be contained within compressed or hidden files and can be inserted into systems in a variety of ways, including web accesses, e-mail, e-mail attachments, and portable storage devices.	The antivirus software must scan all running processes, files, and subfolders, at least weekly. File transfers between the virtual machine and end-user device must not be allowed. **(U)**

(U) Source: The DoD OIG.

(U) DoD Components Generally Configured Remote Access Software to Protect Against Potential Malicious Activity

(U) Network and system administrators for the 10 DoD Components we assessed generally configured the remote access software used to facilitate telework during the COVID-19 pandemic to protect DoD networks and systems. Specifically, of the six configuration settings we assessed the USMC, NSWC-PCD, Air Force, USSOUTHCOM-JIATFS, DISA JSP, DIA, and DoDEA had five configuration settings in place. We did not identify any configuration weaknesses at the U.S. Strategic Command, DCMA, and Defense Media Activity. Table 3 shows the configuration weaknesses identified, by DoD Component.

(U) Table 3. Configuration Weaknesses Identified at DoD Components

(U) Configuration Weaknesses	DoD Components						
	USMC	NSWC-PCD	Air Force	USSOUTHCOM-JIATFS	DISA JSP	DIA	DoDEA
VDI Users Allowed to Upload Files to the Network from End-User Devices				x			
Configured VDI to Not Scan for Malware				x			
Inactive User Accounts Not Disabled After No More Than 35 Days of Inactivity	x	x	x		x	x	x (U)

(U) Source: The DoD OIG.

(U) USSOUTHCOM-JIATFS Did Not Prevent Users from Uploading Files to the Network from End-User Devices

(U) USSOUTHCOM-JIATFS network administrators did not prevent VMware Horizon users from uploading files to the network from end-user devices, including personal devices. The DISA VMware Horizon STIG requires that VMware Horizon prevent users from uploading files between VMware Horizon and an end-user device. To determine whether DoD Component network administrators configured VMware Horizon to prevent users from uploading files from end-user devices to the network, we virtually observed group policy configurations for disabling file uploads from end-user devices to VMware Horizon.

(U) The USSOUTHCOM-JIATFS Enterprise Operations Chief stated that network administrators misunderstood the VMware Horizon STIG configuration to prevent uploading files as redundant to another configuration. Specifically, the Enterprise Operations Chief stated that network administrators believed they had already prevented uploading files through a separate VMware Horizon STIG requirement that prevented users from copying and pasting information. However, preventing users from copying and pasting information does not prevent users from uploading files to VMware Horizon from an end-user device.

(U) Allowing file uploads to VMware Horizon from end-user devices, especially personal devices, puts the USSOUTHCOM-JIATFS network at greater risk of cyber attacks from malicious cyber actors who can intercept the transmission and deploy malicious code into word-processing software, spreadsheets, or image files. During our virtual site visit, we verified that network administrators reconfigured VMware Horizon to prevent uploading files from end-user devices by reviewing a screenshot of the configuration settings which disabled file transfer uploads. Therefore, we did not include a recommendation regarding this issue.

(U) USSOUTHCOM-JIATFS Did Not Scan the VDI for Malware

(U) USSOUTHCOM-JIATFS network administrators did not configure McAfee Endpoint Security, an antivirus software, to scan the main virtual desktop for malware.[11] The DISA McAfee Endpoint Security STIG requires that all disks, running processes, files, and subfolders be scanned, at a minimum, on a weekly basis.[12] To determine whether DoD Component network administrators scanned the VDI for malware, we virtually observed group policy configuration settings for antivirus scanning.

(U) The USSOUTHCOM-JIATFS Enterprise Operations Chief stated that network administrators did not scan the main virtual desktop because they did not want the file size of the main virtual desktop to grow and occupy too much storage space on USSOUTHCOM-JIATFS servers. However, not scanning the main virtual desktop increases the risk that undetected malware in the USSOUTHCOM-JIATFS main virtual desktop could compromise DoD networks and systems.

[11] (U) The main virtual desktop creates virtual sessions for end-users to telework.

[12] (CUI) [redacted]

(U) DoD Components Did Not Disable Inactive User Accounts After 35 Days

(U) USMC, NSWC-PCD, Air Force, DISA JSP, DIA, and DoDEA network and system administrators did not disable inactive user accounts after 35 days of inactivity. The DISA Windows 10 STIG requires that DoD Components disable user accounts after no more than 35 days of inactivity.[13] To determine whether DoD Components disabled inactive user accounts after 35 days, we virtually observed network settings to verify that network and system administrators implemented group policies in accordance with DoD requirements. Table 4 identifies the DoD Component, the timeframes for disabling inactive accounts, and whether the DoD Component formally accepted the risk for not disabling user accounts in accordance with the Windows 10 STIG requirements at the time of our site visit.

(U) Table 4. Disabled Inactive Account Timeframes at DoD Components

~~(CUI)~~ Component	When Components Disabled Inactive Accounts	Formally Accepted Risk
USMC	~~(CUI)~~ After [redacted] days of inactivity	No
NSWC-PCD	~~(CUI)~~ After [redacted] days of inactivity	No
Air Force	~~(CUI)~~ After [redacted] days of inactivity	No
DISA JSP	~~(CUI)~~ After [redacted] days of inactivity	No
DIA	~~(CUI)~~ After [redacted] days of inactivity	Yes
DoDEA	~~(CUI)~~ After [redacted] days of inactivity	No ~~(CUI)~~

(U) Source: The DoD OIG.

~~(CUI)~~ The NSWC-PCD Enterprise Architect stated that the NSWC-PCD Chief Information Officer (CIO) extended the threshold for disabling inactive user accounts at the beginning of the COVID-19 pandemic when users were not accessing the network for an extended period of time. The DISA JSP Desk Side Support Branch Chief stated that DISA JSP network and system administrators extended the threshold for disabling inactive user accounts to [redacted] days to accommodate DISA JSP clients who may have users inactive for more than 35 days because of the inability to remotely access networks and systems during the COVID-19 pandemic.

[13] (U) "Windows 10 Technical Implementation Guide: Version 2, Release: 3 Benchmark Date: 01 Nov 2021."

~~(CUI)~~ The USMC Cybersecurity Compliance Branch Deputy stated that the USMC revised its policy to extend the threshold for disabling inactive user accounts for deployed Marines or users assigned to temporary mission essential duties, which prevented them from accessing the Pulse Secure VPN. In addition, the Air Force System Design Engineer stated that Air Force network and system administrators followed Component-level policy to extend the threshold for disabling inactive user accounts to [redacted] days and that network and system administrators extended the threshold to prevent National Guard and Reserve users' accounts from being unnecessarily disabled. He also stated that he was unaware of the Windows 10 STIG requirement to deactivate user accounts after 35 days of inactivity.

~~(CUI)~~ The DIA Senior Principal Information Systems Security Engineer stated that the DIA CIO accepted the risk of temporarily extending the threshold for disabling inactive user accounts from [redacted] days to [redacted] days because at the beginning of the COVID-19 pandemic, the DIA did not have an agency-wide remote access software in place to enable telework. In November 2020, the AO approved DIA network and system administrators to begin testing Microsoft Azure Virtual Desktop as the DIA's agency-wide remote access software. The DIA Project Management Officer stated that Microsoft Azure Virtual Desktop would be available to a limited number of personnel until August 2022, which is when the DIA deployed the Microsoft Azure Virtual Desktop agency wide.

~~(CUI)~~ After our virtual site visit, DIA network and system administrators reset the threshold back to [redacted] days to align with DIA policy; however, this threshold still exceeded the 35-day STIG requirement. The Senior Principal Information Systems Security Engineer stated that the [redacted]-day threshold was intended to accommodate DIA Reservists and personnel who were deployed outside the continental United States.

(U) Outdated or unused accounts provide penetration points that may go undetected and be exploited by malicious actors to gain unauthorized access to compromise DoD networks. The longer an organization allows unused accounts to remain active, the greater this risk becomes. We acknowledge that it may have been necessary for DoD Components to revise their policy to temporarily extend the threshold for disabling inactive user accounts at the start of the COVID-19 pandemic. This extension was understandable given the unknowns regarding employee access to DoD systems and working environments. However, disabling inactive user accounts beyond the number of days outlined in the STIG requirement may no longer be appropriate, as the DoD has maximized telework for over 2 years and the working environment has solidified.

(U) Outdated or unused accounts provide penetration points that may go undetected and be exploited by malicious actors to gain unauthorized access to compromise DoD networks.

~~(CUI)~~ The DoDEA Global Customer Support Chief stated that DoDEA Customer Support Services administrators extended the threshold for disabling user accounts to prevent network and system administrators from having to reactivate teachers and other school staff after the summer break. After our virtual site visit, Customer Support Services administrators created a specific user group for non-educational staff to disable inactive accounts after [redacted] days in accordance with the Windows 10 STIG. In addition, Customer Support Services administrators created a separate group for teachers and other school staff to continue disabling inactive accounts after [redacted] days.

(U) Extending the threshold for disabling accounts for teachers and other school staff allows those users to access DoDEA networks over summer break to prepare for the upcoming school year without having to reactivate their accounts. The DoDEA AO accepted the risk of deviating from the Windows 10 STIG requirement by completing a risk acceptance document. Therefore, we did not include a recommendation to the DoDEA CIO on disabling inactive user accounts in this report.

(U) Authorizing Officials Did Not Consistently Document Accepting the Risks of Deviating from DoD Requirements

(U) Although DoDI 8510.01 allows AOs to accept the risk of not implementing configuration settings as required by the SRGs and STIGs, AOs for seven DoD Components (USMC, NSWC-PCD, Air Force, DISA JSP, DIA, DoDEA, and USSOUTHCOM-JIATFS) we assessed did not document accepting the risks of deviating from DoD requirements. According to NIST, before accepting a risk, AOs should assess the risk to determine whether it is within the organization's risk tolerance level, or whether network and system administrators need to mitigate the risk.[14] While there may be valid operational needs for DoD Components to deviate from DoD requirements, it is important that AOs document an assessment of the potential impact to DoD employees, assets, and missions; and the acceptance of the risks.

(U) While there may be valid operational needs for DoD Components to deviate from DoD requirements, it is important that AOs document an assessment of the potential impact to DoD employees, assets, and missions; and the acceptance of the risks.

[14] (U) Risk tolerance is the level of risk or the degree of uncertainty that is acceptable to an organization.

(U) In addition, when the AOs at the USMC, NSWC-PCD, Air Force, DISA JSP, DIA, DoDEA, and USSOUTHCOM-JIATFS informed us that certain configuration settings deviated from the SRG and STIG requirements, we asked if compensating controls were implemented in place of the configuration requirements that would have provided equivalent or comparable protection for the remote access software. None of the DoD Components implemented compensating controls.

(U) If AOs do not document the assessment and acceptance of risk, future management may not be aware of all instances where configuration settings were not followed, which could expose DoD networks and systems to potential malicious activity. NIST SP 800-39 states that senior leaders and executives are ultimately responsible and accountable for risk decisions. To make an informed risk decision, the senior leaders and executives rely on the AO assessment. In addition, future management may not have all the necessary information to reassess the impact of the risk on operational needs and whether noncompliant configuration settings remain appropriate. We directed Recommendations A.1, A.2, A.3, A.4, A.5, and A.6 to the respective CIOs and Directors to formally accept the risk if they did not configure their remote access software to comply with DoD requirements or develop compensating controls to protect remote access software.

(U) Improper Configuration Settings Could Increase the Risk of Cyber Attacks

(U) According to Executive Order 14028, the United States faces persistent and increasingly sophisticated malicious cyber attacks.[15] The use of potentially vulnerable services, such as VPNs and VDIs, amplifies the threat to individuals and organizations in a maximum telework environment. DoD Components that do not consistently configure remote access software in accordance with SRG and STIG requirements increase the risk for malicious cyber actors to insert malicious code, such as malware, on the DoD network by exploiting file uploads from end-user devices.

> *(U) The use of potentially vulnerable services, such as VPNs and VDIs, amplifies the threat to individuals and organizations in a maximum telework environment.*

(U) Not configuring systems in accordance with SRG and STIG requirements increases the risk of compromising the confidentiality, integrity, and availability of DoD networks and systems and allow a malicious cyber actor to gain unauthorized access that could jeopardize mission operations. As the DoD workforce continues to use remote access software to facilitate telework, DoD Components should implement basic cyber hygiene practices to protect DoD networks and systems from potential malicious activity.

[15] (U) Executive Order 14028, "Improving the Nation's Cybersecurity," May 12, 2021.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation A.1

(U) We recommend that the Director of the U.S. Southern Command – Joint Interagency Task Force South Command, Control, Communications, Computers, Cyber and Intelligence direct its network administrators to scan the VMware Horizon main virtual desktop for malware in accordance with the McAfee Endpoint Security Technical Implementation Guide, develop compensating controls, or formally accept the risk of not scanning the main virtual desktop.

(U) U.S. Southern Command – Joint Interagency Task Force South Command, Control, Communications, Computers, Cyber and Intelligence Director Comments

(U) The USSOUTHCOM-JIATFS Command, Control, Communications, Computers, Cyber and Intelligence Director agreed, stating that USSOUTHCOM-JIATFS implemented a standard operating procedure to conduct weekly scans of the VMware Horizon main virtual desktop for malware.

(U) Our Response

(U) Comments from the Director addressed the specifics of the recommendation. We verified that USSOUTHCOM-JIATFS developed a standard operating procedure to conduct scans of its virtual desktops on a weekly basis. In December 2022, we verified through screenshots of scan settings and activity logs, that USSOUTHCOM-JIATFS was conducting the weekly scans. Therefore, the recommendation is closed.

(U) Recommendation A.2

(U) We recommend that the Chief Information Officer of the Department of the Air Force:

a. **(U) Revise its policy to align with the Windows 10 Security Technical Implementation Guide requirement for disabling inactive user accounts after no more than 35 days.**

b. **(U) Direct network and system administrators to disable inactive user accounts after no more than 35 days of inactivity in accordance with the Windows 10 Security Technical Implementation Guide, develop compensating controls, or formally accept the risk of not disabling the inactive user accounts.**

(U) Deputy Chief Information Officer of the Department of the Air Force Comments

~~(CUI)~~ The Deputy CIO of the Department of the Air Force, responding for the CIO, partially agreed, stating that the Chief Information Security Officer for the Department of the Air Force will review and update, if necessary, guidance related to disabling inactive user accounts by [redacted]. The Deputy CIO noted that Air Force guidance was based on a U.S. Cyber Command (USCYBERCOM) Operation Order (OPORD).[16]

(U) Our Response

(U) Comments from the Deputy CIO partially addressed the recommendations; therefore, the recommendations are unresolved. Reviewing and updating the policy, **if necessary** [emphasis added], will not reduce the risk of malicious actors exploiting penetration points and gaining unauthorized access to DoD networks. The longer the Air Force allows unused accounts to remain active, the greater the risk becomes.

(U) While OPORDs can take precedence over STIGs if USCYBERCOM determines that a specific STIG control is not applicable to a system or network, the OPORD guidance should not create additional risks to the protection of DoD systems, networks, and data. We requested a copy of the USCYBERCOM OPORD in January 2023 and again in February 2023. However, as of the issuance of this report, we have not received a copy.

(U) Without a review of the OPORD, we cannot determine whether USCYBERCOM agreed that the Air Force did not need to disable user accounts after no more than 35 days of inactivity. Therefore, we request that, within 30 days, the Deputy CIO of the Air Force provide the USCYBERCOM OPORD that the Air Force used to develop its guidance and provide additional comments to the final report describing the specific actions that the Chief Information Security Officer will take to align the Air Force policy with Windows 10 STIG requirements to disable inactive user accounts after no more than 35 days of inactivity.

[16] (U) An operation order (OPORD) is a directive issued by a commander to individuals, units, or organizations to complete a specific action or mission.

(U) Recommendation A.3

(U) We recommend that the Chief Information Officer of the Naval Surface Warfare Center – Panama City Division direct network and system administrators to disable inactive user accounts after no more than 35 days of inactivity in accordance with the Windows 10 Security Technical Implementation Guide, develop compensating controls, or formally accept the risk of not disabling the inactive user accounts.

(U) Commander of the Naval Sea Systems Command Comments

~~(CUI)~~ The Commander of the Naval Sea Systems Command, responding for the NSWC-PCD CIO, agreed, stating that NSWC-PCD implemented the Windows 10 STIG requirements to disable inactive accounts after no more than 35 days of inactivity. The Commander subsequently provided supporting documentation in February 2023 showing that it runs a script on a daily basis to identify and disable inactive accounts after [redacted] days of activity.

(U) Our Response

~~(CUI)~~ Comments from the Commander addressed the specifics of the recommendation. In February 2023, we verified, through screenshots of policy settings, that NSWC-PCD updated its network settings to disable inactive accounts after [redacted] days of inactivity. Therefore, the recommendation is closed.

(U) Department of the Navy Deputy Chief Information Security Officer Comments

(U) Although not required to comment, the Department of the Navy Deputy Chief Information Security Officer stated that NSWC personnel cannot formally accept risk for the Navy and that the recommendation should be redirected to the Navy Deputy CIO or Navy Authorizing Official.

(U) Our Response

(U) Since the NAVSEA Commander directed NSWC-PCD to implement the recommendation and decided not to accept the risk of not disabling inactive user accounts, we did not redirect the recommendation to the Department of the Navy Deputy CIO.

(U) Recommendation A.4

(U) We recommend that the Chief Information Officer of the Defense Intelligence Agency:

a. **(U) Revise its policy to align with the Windows 10 Security Technical Implementation Guide requirement for disabling inactive users after no more than 35 days.**

b. **(U) Direct network and system administrators to disable inactive user accounts after no more than 35 days of inactivity in accordance with the Windows 10 Security Technical Implementation Guide, develop compensating controls, or formally accept the risk of not disabling the inactive user accounts.**

(U) Defense Intelligence Agency Chief Information Security Officer Comments

~~(CUI)~~ The DIA Chief Information Security Officer, responding for the CIO, agreed, stating that the DIA plans to revise its policy to disable inactive civilian and contractor accounts after [redacted] days of inactivity. However, the Chief Information Security Officer stated that the DIA completed a Risk Acceptance Request to disable military and Defense Attaché Officers accounts after [redacted] days of inactivity.

(U) Our Response

~~(CUI)~~ Comments from the Chief Information Security Officer addressed the specifics of the recommendations; therefore, the recommendations are resolved but open. In February 2023, we verified that the Chief Information Security Officer approved a risk acceptance request to disable military and Defense Attaché Officers accounts after [redacted] days of inactivity. We will close the recommendations once the Chief Information Security Officer provides the revised policy and supporting documentation, such as screenshots of group policy settings, showing that the DIA updated its inactive user account setting to disable civilian and contractor accounts after [redacted] days of inactivity.

(U) Recommendation A.5

(U) We recommend that the Director of the Marine Corps Information Command, Control, Communications, and Computers:

a. **(U) Revise the organization's policy to align with the Windows 10 Security Technical Implementation Guide requirement for disabling inactive users after no more than 35 days.**

b. **(U) Direct network and system administrators to disable inactive user accounts after no more than 35 days of inactivity in accordance with the Windows 10 Security Technical Implementation Guide, develop compensating controls, or formally accept the risk of not disabling the inactive user accounts.**

(U) Marine Corps Information Command, Control, Communications, and Computers Office of the Deputy Commandant for Information Technical Director Comments

~~(CUI)~~ The Technical Director in the Office of the Deputy Commandant for Marine Corps Information Command, Control, Communications and Computers (IC4), responding for the Marine Corps IC4 Director, agreed, stating that Marine Corps policy guidance would be updated to reflect the 35-day requirement in the Windows 10 STIG by [redacted]. The Technical Director also stated that Marine Corps Cyber Command will disable inactive user accounts after [redacted] days by [redacted]. The Technical Director added that Marine Corps Cyber Command will conduct a risk assessment for any exceptions to the inactive user [redacted]-day policy by [redacted], and implement a waiver process for inactive user accounts that are not disabled after [redacted] days by [redacted].

(U) Our Response

~~(CUI)~~ Comments from the Technical Director addressed the specifics of the recommendations; therefore, the recommendations are resolved but open. We will close the recommendations once the Technical Director provides supporting documentation showing that the Marine Corps revised its organizational policy to disable inactive user accounts within [redacted] days; screenshots of group policy settings showing that the Marine Corps updated its inactive user account setting to disable accounts after [redacted] days of inactivity; and we verify that Marine Corps Cyber Command implemented a waiver process for inactive user accounts that are not disabled after [redacted] days.

(U) Recommendation A.6

(U) We recommend that the Director of the Defense Information Systems Agency Joint Service Provider direct network and system administrators to disable inactive user accounts after no more than 35 days of inactivity in accordance with the Windows 10 Security Technical Implementation Guide, develop compensating controls, or formally accept the risk of not disabling the inactive user accounts

(U) Director of the Defense Information Systems Agency Joint Service Provider Comments

~~(CUI)~~ The Chief of the DISA JSP Cyber Security Center, responding for the DISA JSP Director, stated that as of [redacted], the JSP Accounts Management Team complied with the Windows 10 STIG requirement to disable inactive user accounts after no more than 35 days of inactivity. The Chief also stated that JSP AO will ensure that the acceptance of any risks that deviate from DoD requirements are documented by [redacted].

(U) Our Response

~~(CUI)~~ Comments from the Chief did not address the specifics of the recommendation; therefore, the recommendation is unresolved. At the time of the audit, DISA JSP did not comply with the Windows 10 STIG requirements to deactivate inactive user accounts. While the Chief stated that DISA JSP began complying with the STIG requirements in [redacted], DISA JSP did not describe the actions it would take or provide documentation to show ongoing compliance with the Window 10 STIG requirement to disable inactive user accounts after no more than 35 days of inactivity.

~~(CUI)~~ On February 6, 2023, the Acting Chief of the DISA JSP Cyber Security Center stated that the JSP AO determined that JSP had implemented all DoD requirements related to remote access software, and therefore, no risk acceptance was required.[17] Therefore, we request that within 30 days, the Chief of the DISA JSP Cyber Security Center state whether he agrees or disagrees with the recommendation and provide documentation, such as screenshots of group policy settings, showing that DISA JSP updated its inactive user account setting to disable accounts after [redacted] days of inactivity.

[17] (U) The Chief of the DISA JSP Cyber Security Center departed the agency shortly after providing comments to the draft report.

(U) Finding B

(U) DoD Components Generally Implemented Cybersecurity Controls to Protect DoD Networks and Systems

(U) Network and system administrators for the 10 DoD Components we assessed generally implemented cybersecurity controls to protect remote connections to DoD networks. Specifically, of the 10 DoD Components assessed, 9 DoD Components implemented all of the cybersecurity controls that we considered critical to protect remote access connections to DoD networks. The remaining DoD Component, DISA JSP, implemented eight of the nine controls we assessed.

~~(CUI)~~ DISA JSP administrators did not consistently implement the control on vulnerability identification and mitigation. Specifically, DISA JSP administrators did not mitigate all known [redacted] vulnerabilities relating to remote access software. If a vulnerability cannot be mitigated, the DoD requires the Component to develop a plan of action and milestones (POA&Ms); however, DISA JSP did not develop POA&Ms. [redacted].

(U) Cybersecurity Controls Assessed

(U) DoDI 8510.01 requires DoD Components to implement cybersecurity controls in accordance with the NIST SP 800-53. To determine whether DoD Components protected remote connections, we assessed each DoD Components' implementation of NIST SP 800-53 cybersecurity controls that we considered critical to protect remote access connections to DoD networks. Table 5 identifies the cybersecurity controls and their importance.

(U) Table 5. Cybersecurity Controls and Their Importance

(U) Cybersecurity Control	Importance of Cybersecurity Control
Vulnerability Identification and Mitigation	Identifying and mitigating vulnerabilities includes scanning networks and systems to identify potential weaknesses, such as network vulnerabilities, that can be exploited on a computer or network. Identifying and mitigating network and system vulnerabilities reduces a malicious cyber actor's ability to gain unauthorized access to networks and systems, introduce malware, and steal critical DoD information that could compromise national security. DoD Components can identify and mitigate vulnerabilities on DoD remote access software to prevent malicious cyber actors who target unsecure remote connection points from stealing sensitive information. **(U)**

(U) Table 5. Cybersecurity Controls and Their Importance (cont'd)

(U) Cybersecurity Control	Importance of Cybersecurity Control
Continuous Monitoring and Audit Record Generation	Organizations continuously monitor systems by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. System monitoring capabilities are achieved through tools and techniques including audit record monitoring software. Audit records include the type of event that occurred; when the event occurred; where the event occurred; source of the event; and the outcome of the event. Continuous monitoring provides DoD Components with constant situational awareness of their system security and privacy posture to support risk management decisions.
Security Alerts, Advisories, and Directives	Supply chain partners, service providers, and other supporting organizations issue security advisories and directives. For example, DoD Components receive alerts about remote access software vulnerabilities from Cisco Systems Incorporated and the U.S. Cyber Command. DoD Components can reduce the risk of malicious cyber actors exploiting vulnerabilities by complying with security advisors and directives to mitigate vulnerabilities in a timely manner.
Enforcing Multifactor Authentication	Multifactor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as something you know, something you have, or something you are. Incorporating a physical authenticator, such as a Common Access Card, increases the level of assurance in the authentication process.
Authenticator Management	Authenticators include passwords, certificates, and identification badges. Authenticator management includes revoking authenticators when no longer needed. Outdated or unused authenticators provide penetration points that may go undetected and be exploited by malicious actors to gain unauthorized access to, and compromise, DoD networks.
Protecting Information at Rest	Information at rest refers to the state of information when it is not in process or in transit, and is located on system components. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Not protecting information at rest may allow malicious cyber actors to compromise the confidentiality and integrity of DoD information.
Confidentiality and Integrity of Transmitted Information	Protecting the confidentiality and integrity of transmitted information can be achieved by physical means or by employing encryption techniques. Without encrypting transmitted information, unprotected communication paths are exposed to the possibility of interception and modification by malicious cyber actors.
Boundary Protection	Boundary protection controls can be implemented through the use of gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture. Without boundary protection controls, DoD Components may not have security architecture that monitors and controls communications at the external and internal boundaries of the information system.
Malicious Code Protection	Organizations monitor entry and exit points to detect and eliminate malicious code that could compromise sensitive DoD information. **(U)**

(U) Source: The DoD OIG.

(U) The DISA JSP Did Not Mitigate Known Vulnerabilities to Protect DoD Networks

~~(CUI)~~ DISA JSP network administrators did not mitigate all known [redacted] vulnerabilities in accordance with DoD requirements. In addition, the Information System Owners did not develop POA&Ms for vulnerabilities that DISA JSP network administrators were not able to mitigate. DoD Instruction 8531.01 states that DoD Components should consider the risk of all vulnerabilities when implementing the appropriate mitigation actions.[18] Furthermore, NIST SP 800-53 requires organizations to periodically scan Federal information systems for vulnerabilities, and to develop POA&Ms if an identified vulnerability cannot be mitigated in a timely manner.

~~(CUI)~~ To determine whether DISA JSP network administrators mitigated remote access software vulnerabilities in a timely manner, we compared remote access software scan results to identify whether any vulnerabilities from March 2022 remained unmitigated in June 2022. A DISA JSP June 2022 scan revealed that [redacted] remote access software vulnerabilities identified in a March 2022 scan remained unmitigated. The [redacted] vulnerabilities included [redacted] vulnerabilities. For example, [redacted]. [redacted].[19] In addition, DISA JSP network administrators did not develop POA&Ms for the [redacted] unmitigated vulnerabilities.

~~(CUI)~~ [redacted].[20] [redacted]. The Continuous Monitoring Branch Chief stated that he believed it was impractical to address all vulnerabilities for the approximately [redacted]. However, by only focusing on mitigating [redacted] across all DISA JSP assets, regardless of criticality, system administrators did not mitigate [redacted] remote access software vulnerabilities, including [redacted] vulnerabilities, which malicious actors could exploit to gain access to DoD information. While we understand that the DISA JSP manages a large amount of assets, it still needs to ensure that network administrators patch all vulnerabilities, [redacted].

[18] (U) DoD Instruction 8531.01, "DoD Vulnerability Management," September 15, 2020.

[19] (U) Cisco Systems Incorporated is the vender for Cisco AnyConnect VPN.

[20] (U) An information assurance vulnerability alert is a notification that is generated when an information assurance vulnerability may result in an immediate and potentially severe threat to DoD systems and information.

(U) Unmitigated Vulnerabilities Could Increase the Risk of Cyber Attacks

(U) DoD Components that do not fully implement NIST cybersecurity controls to protect remote access software used to facilitate telework increase the risk of exposing DoD networks to potential malicious activity.

(U) According to the Cybersecurity and Infrastructure Security Agency, the COVID-19 pandemic brought a significant increase in teleworking since March 2020, which increased attacks from malicious cyber actors. DoD Components that do not fully implement NIST cybersecurity controls to protect remote access software used to facilitate telework increase the risk of exposing DoD networks to potential malicious activity. Specifically, malicious cyber actors could exploit remote access software vulnerabilities to steal DoD information, which could put the United States at a disadvantage against its adversaries.

(U) To maintain the cybersecurity posture of remote access software, DoD Components should identify and mitigate vulnerabilities in a timely manner or develop POA&Ms to decrease the risk that malicious actors could exploit known remote access software weaknesses. Without a POA&M, DISA JSP network administrators may be unable to identify and correct network weaknesses, establish risk mitigation activities, or determine how long a vulnerability remained unmitigated. As the DoD workforce continues to use remote access software to facilitate telework, DoD Components should remain alert and attentive to known system vulnerabilities and cyber attacks that may threaten DoD information stored on end-user devices and transmitted across DoD networks.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation B.1

(U) We recommend that the Director of the Defense Information Systems Agency Joint Service Provider direct network and system administrators to revise the vulnerability management program to include mitigation timeframes for all vulnerabilities and develop plans of actions and milestones for all vulnerabilities that cannot be mitigated in a timely manner.

(U) Director of the Defense Information Systems Agency Joint Service Provider Comments

(U) The Chief of the DISA JSP Cyber Security Center, responding for the DISA JSP Director, agreed, stating that the Continuous Monitoring Branch will update the vulnerability management process to ensure that vulnerabilities are mitigated within a timeframe specified by the Authorizing Official and develop POA&Ms for vulnerabilities that cannot be mitigated in a timely manner. The Chief stated that the Continuous Monitoring Branch directed the Information Security Officer to create POA&Ms for any remaining vulnerabilities.

(U) Our Response

~~(CUI)~~ Comments from the Chief addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Chief provides supporting documentation, such as policy showing that DISA JSP's vulnerability management program includes mitigation timeframes for all vulnerabilities and POA&Ms for the [redacted] vulnerabilities we identified in the report that DISA JSP could not mitigate in a timely manner.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from December 2021 through September 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) To understand the process used to configure and protect DoD remote access software, we interviewed officials from the:

- (U) DoD Office of the Chief Information Officer;
- (U) Defense Information Systems Agency;
- (U) Army Office of the Chief Information Officer;
- (U) Army Cyber Command;
- (U) Army Network Enterprise Technology Command;
- (U) Naval Network Warfare Command;
- (U) Navy Cyber Defense Operations Command; and
- (U) U.S. Fleet Cyber Command.

(U) We interviewed project managers and information system security personnel at the selected DoD Components to identify security controls and configuration settings implemented to protect DoD networks and systems from potential malicious activity. Additionally, we reviewed Federal laws and DoD policy concerning configuration management, remote access, and cybersecurity controls.

(U) We selected a nonstatistical sample of 13 of 94 remote access software solutions used by 10 DoD Components to evaluate whether DoD Components implemented security controls to protect remote connections to DoD networks. Of the 10 DoD Components that we assessed, 3 were Military Services, 2 were Combatant Commands, 3 were DoD Agencies, and 2 were DoD Field Activities.[21]

[21] (U) DoD Field Activities provide support services to the DoD.

(U) To determine whether the DoD Components implemented security controls and configured their remote access software to protect DoD networks, we:

- (U) virtually observed configuration and security control settings for remote access software to verify compliance with NIST SP 800-53 and the DISA SRGs and STIGs;
- (U) obtained screenshots of configuration and security control settings for remote access software;
- (U) obtained and analyzed network vulnerability scan results to verify that the DoD Components mitigated identified vulnerabilities for remote access software in a timely manner; and
- (U) obtained and reviewed system security plans, cybersecurity risk assessments, and plans of action and milestones, as well as guidelines, policies, procedures, and instructions related to remote access software.

(U) Internal Control Assessment and Compliance

(U) We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we assessed the control environment for remote access software related to:

- (U) configuration management;
- (U) access management and authentication;
- (U) encryption for data stored on systems (at rest) and data transmitted across the network (in transit);
- (U) network boundary protection (including antivirus application security); and
- (U) vulnerability identification and mitigation.

(U) However, because our review was limited to these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

(U) Use of Computer-Processed Data

(U) We did not use computer-processed data to perform this audit.

(U) Use of Technical Assistance

(U) The DoD OIG Quantitative Methods Division provided assistance in developing the nonstatistical sampling methodology that we used to select the DoD Components and to compare network vulnerability scans.

(U) Prior Coverage

(U) During the last 5 years, the Government Accountability Office (GAO) and the DoD OIG issued three reports discussing cybersecurity controls for remote access software. Unrestricted GAO reports can be accessed at http://www.gao.gov. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/reports.html/.

(U) GAO

(U) Report No. GAO-21-583, "COVID-19: Selected Agencies Overcame Technology Challenges to Support Telework but Need to Fully Assess Security Controls," September 30, 2021

> (U) The GAO found that while all 12 agencies reported that they continued activities intended to help ensure the security of their information and systems, not all agencies fully addressed relevant Federal guidance for securing the systems that support remote access for telework. Specifically, two agencies had not fully documented relevant security controls, while four agencies had not fully documented remedial actions taken to reduce identified weaknesses. In addition, five agencies did not assess the operating effectiveness of all relevant controls for remote access systems.

(U) DoD OIG

(U) Report No. DODIG-2021-064, "Audit of Maintaining Cybersecurity in the Coronavirus Disease–2019 Telework Environment," March 29, 2021

> ~~(CUI)~~ The DoD OIG determined that DoD Components did not consistently maintain network protections with required cybersecurity controls during maximum telework. The DoD OIG recommended that the DoD CIO direct DISA to amend the DISA VPN SRG to [redacted]. DISA created a new VPN SRG requirement, [redacted], to address this recommendation.

(U) Report No. DODIG-2021-065, "Evaluation of Access to Department of Defense Information Technology and Communications During the Coronavirus Disease–2019 Pandemic," March 30, 2021

(U) The DoD OIG determined that the DoD transitioned 88.2 percent of respondents to full- or part-time telework during the COVID-19 pandemic. In addition, it found that the DoD experienced initial challenges because not all DoD Components had fully tested the capability of their information systems to support maximum telework and had not met the March 2020 deadline to conduct telework exercises with personnel as required by the DoD Implementation Plan for Pandemic Influenza and the DoD Telework Policy.

(U) Appendix B

(U) Sampling Approach

(U) We used a nonstatistical sampling approach to select the DoD Components and remote access software to review for this audit. To determine the universe of DoD Components using remote access software, we sent a questionnaire requesting that the Military Services, Combatant Commands, DoD Agencies, and DoD Field Activities identify the remote access software solutions used and the number of authorized users per solution. We combined the responses to create a consolidated universe of 94 remote access software used by DoD Components that did aligned with our definition of remote access software.[22] To eliminate redundancy, we removed DoD Components who relied on the DISA JSP to manage their remote access software.

(U) The following 36 DoD Components reported using remote access software.

- (U) Department of the Army
- (U) Department of the Navy
- (U) Department of the Air Force
- (U) U.S. Africa Command
- (U) U.S. European Command
- (U) U.S. Northern Command
- (U) U.S. Special Operations Command
- (U) U.S. Southern Command
- (U) U.S. Strategic Command
- (U) U.S. Transportation Command
- (U) Joint Staff
- (U) Defense Advanced Research Projects Agency
- (U) Defense Contract Audit Agency
- (U) Defense Contract Management Agency
- (U) Defense Counterintelligence and Security Agency
- (U) Defense Commissary Agency
- (U) Defense Finance and Accounting Service
- (U) Defense Health Agency

[22] (U) For the purpose of this audit, we defined remote access software as any software that gives an authorized person the ability to access a computer or network from a geographical distance through an external network connection, such as the Internet.

- (U) Defense Travel Management Office
- (U) Defense Human Resources Activity
- (U) Defense Intelligence Agency
- (U) Defense Information Systems Agency, Headquarters
- (U) Defense Information Systems Agency, Joint Service Provider
- (U) Defense Logistics Agency
- (U) Defense Media Activity
- (U) Defense Security Cooperation Agency
- (U) Defense Threat Reduction Agency
- (U) Defense Technology Security Administration
- (U) Department of Defense Education Activity
- (U) Joint Forces Headquarters–Department of Defense Information Network
- (U) Missile Defense Agency
- (U) National Geospatial-Intelligence Agency
- (U) National Reconnaissance Office
- (U) National Security Agency
- (U) Office of Local Defense Community Cooperation
- (U) Uniformed Services University of the Health Sciences

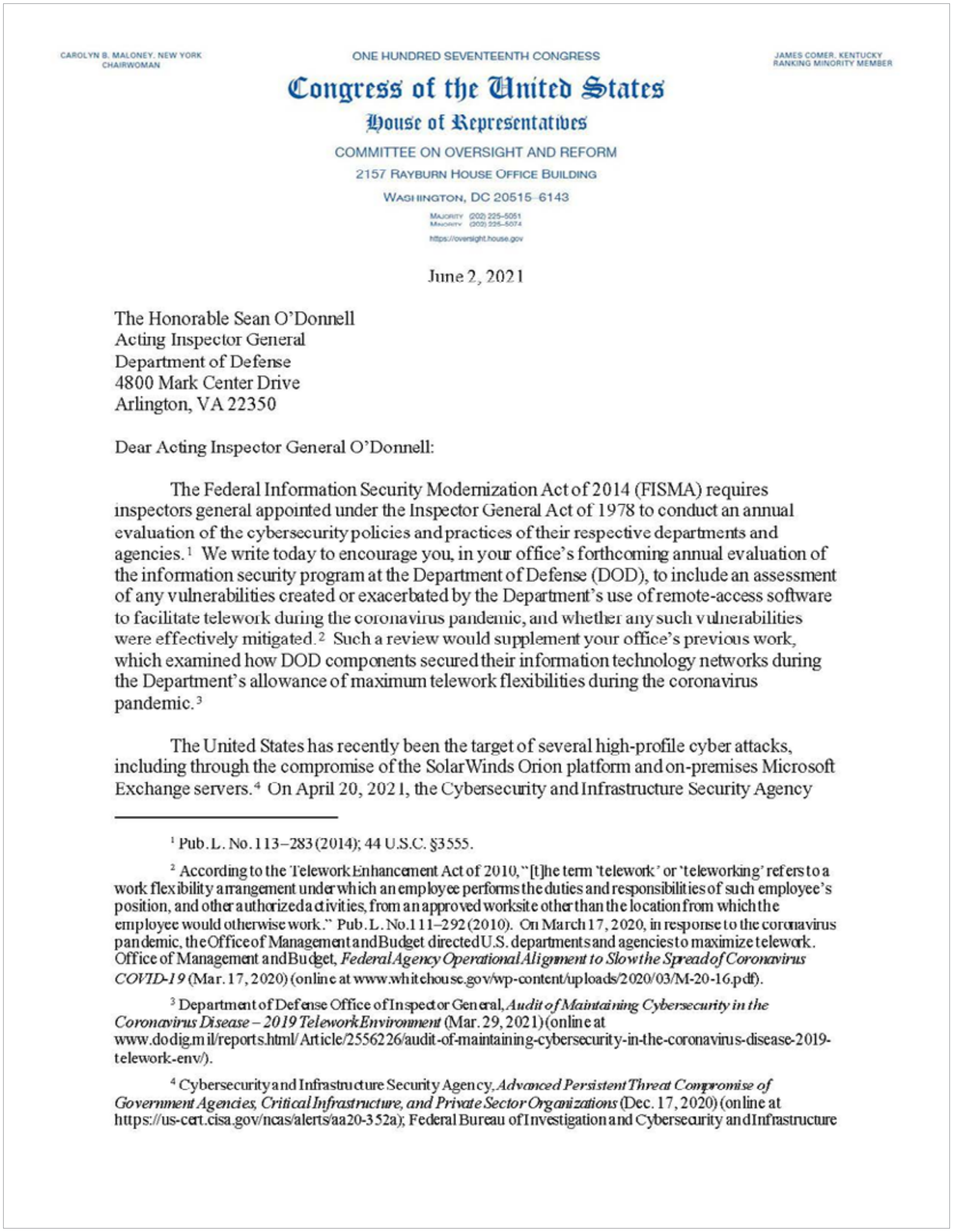
(U) We then categorized the remote access software solutions into the following tiers based on the number of users.

- (U) Low – 5,000 or fewer users
- (U) Medium – 5,001 to 30,000 users
- (U) High – 30,001 or more users

(U) We selected a nonstatistical sample from the universe of remote access software using the "RAND" [random] function in Microsoft Excel to eliminate selection bias. We then sorted the selection, for each tier, from highest to lowest based on the assigned random values. We selected nine remote access software solutions; four were from the low tier, three were from the medium tier, and two were from the high tier. We also judgmentally selected the DISA JSP for our sample selection based on the responses to our questionnaire, which showed that the DISA JSP manages four remote access software for multiple DoD Components.

(U) Appendix C

(U) House of Representatives, Committee on Oversight and Reform, Congressional Request Letter



CAROLYN B. MALONEY, NEW YORK
CHAIRWOMAN

ONE HUNDRED SEVENTEENTH CONGRESS

Congreſs of the United States
House of Repreſentatives

COMMITTEE ON OVERSIGHT AND REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5051
MINORITY (202) 225–5074
https://oversight.house.gov

JAMES COMER, KENTUCKY
RANKING MINORITY MEMBER

June 2, 2021

The Honorable Sean O'Donnell
Acting Inspector General
Department of Defense
4800 Mark Center Drive
Arlington, VA 22350

Dear Acting Inspector General O'Donnell:

The Federal Information Security Modernization Act of 2014 (FISMA) requires inspectors general appointed under the Inspector General Act of 1978 to conduct an annual evaluation of the cybersecurity policies and practices of their respective departments and agencies.[1] We write today to encourage you, in your office's forthcoming annual evaluation of the information security program at the Department of Defense (DOD), to include an assessment of any vulnerabilities created or exacerbated by the Department's use of remote-access software to facilitate telework during the coronavirus pandemic, and whether any such vulnerabilities were effectively mitigated.[2] Such a review would supplement your office's previous work, which examined how DOD components secured their information technology networks during the Department's allowance of maximum telework flexibilities during the coronavirus pandemic.[3]

The United States has recently been the target of several high-profile cyber attacks, including through the compromise of the SolarWinds Orion platform and on-premises Microsoft Exchange servers.[4] On April 20, 2021, the Cybersecurity and Infrastructure Security Agency

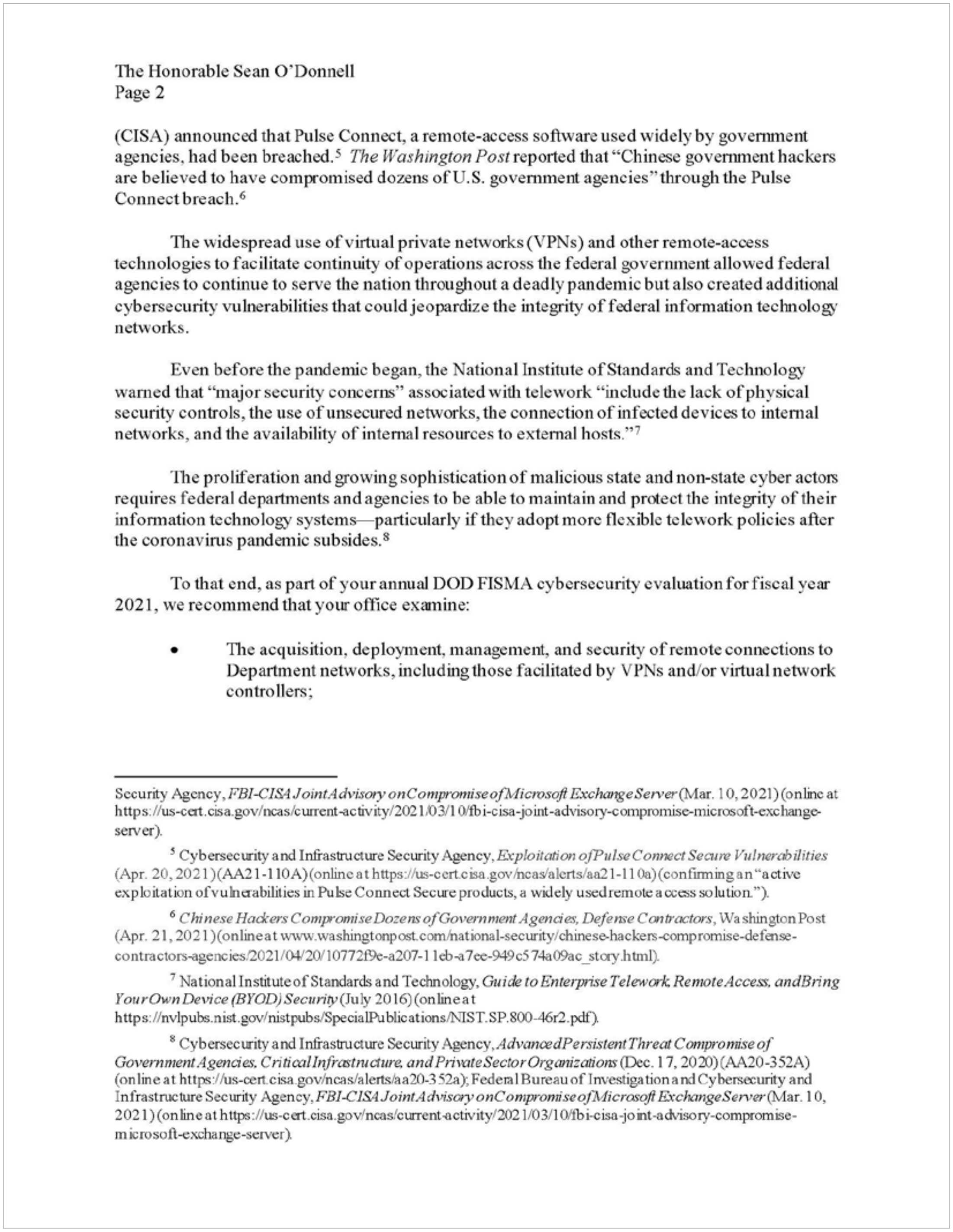
[1] Pub. L. No. 113–283 (2014); 44 U.S.C. §3555.

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

[3] Department of Defense Office of Inspector General, *Audit of Maintaining Cybersecurity in the Coronavirus Disease – 2019 Telework Environment* (Mar. 29, 2021) (online at www.dodig.mil/reports.html/Article/2556226/audit-of-maintaining-cybersecurity-in-the-coronavirus-disease-2019-telework-env/).

[4] Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (online at https://us-cert.cisa.gov/ncas/alerts/aa20-352a); Federal Bureau of Investigation and Cybersecurity and Infrastructure

(U) House of Representatives, Committee on Oversight and Reform, Congressional Request Letter (cont'd)



The Honorable Sean O'Donnell
Page 2

(CISA) announced that Pulse Connect, a remote-access software used widely by government agencies, had been breached.[5] *The Washington Post* reported that "Chinese government hackers are believed to have compromised dozens of U.S. government agencies" through the Pulse Connect breach.[6]

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

Even before the pandemic began, the National Institute of Standards and Technology warned that "major security concerns" associated with telework "include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, and the availability of internal resources to external hosts."[7]

The proliferation and growing sophistication of malicious state and non-state cyber actors requires federal departments and agencies to be able to maintain and protect the integrity of their information technology systems—particularly if they adopt more flexible telework policies after the coronavirus pandemic subsides.[8]

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

- The acquisition, deployment, management, and security of remote connections to Department networks, including those facilitated by VPNs and/or virtual network controllers;

Security Agency, *FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server* (Mar. 10, 2021) (online at https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server).

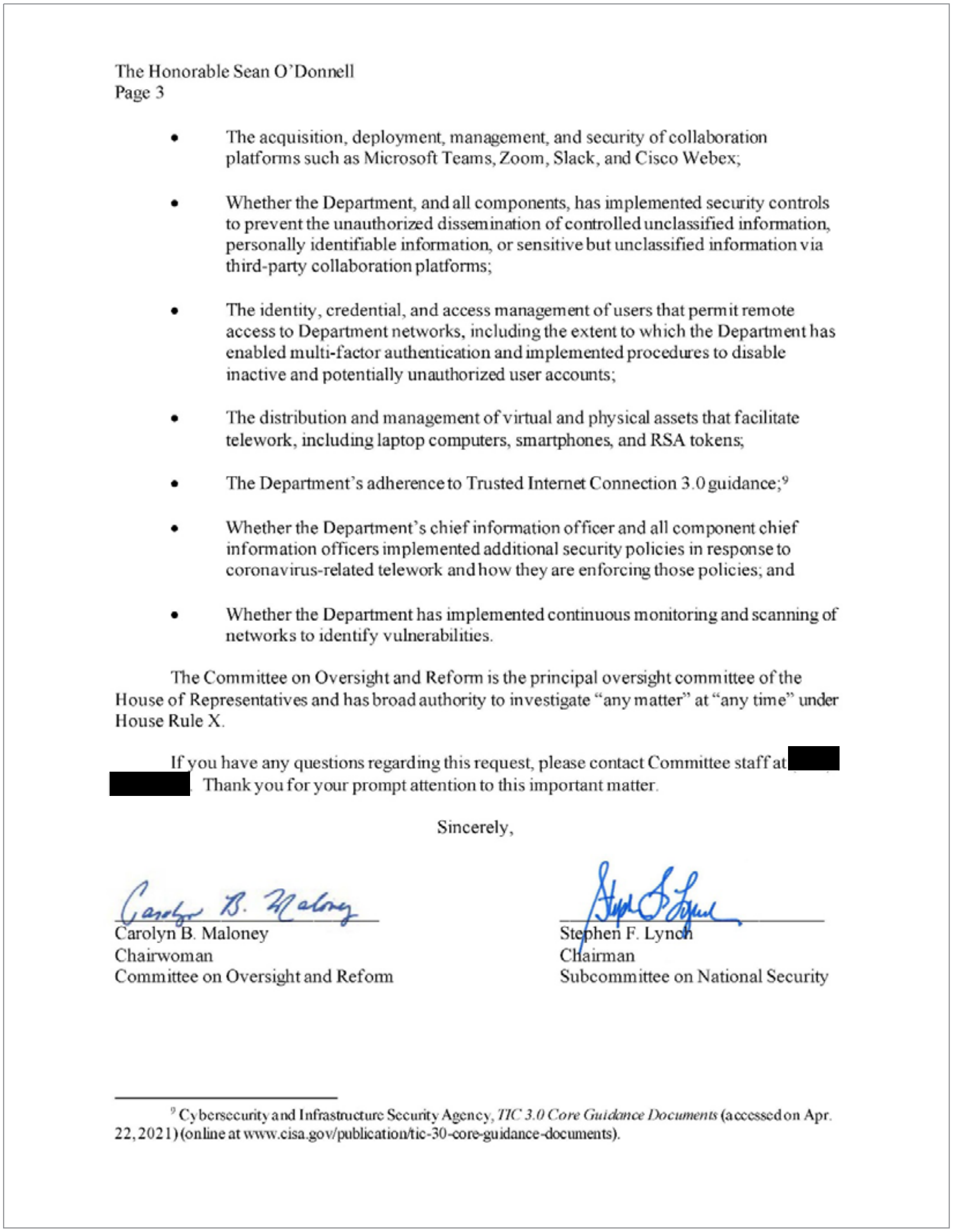
[5] Cybersecurity and Infrastructure Security Agency, *Exploitation of Pulse Connect Secure Vulnerabilities* (Apr. 20, 2021) (AA21-110A) (online at https://us-cert.cisa.gov/ncas/alerts/aa21-110a) (confirming an "active exploitation of vulnerabilities in Pulse Connect Secure products, a widely used remote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

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

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

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

(U) House of Representatives, Committee on Oversight and Reform, Congressional Request Letter (cont'd)



The Honorable Sean O'Donnell
Page 3

- The acquisition, deployment, management, and security of collaboration platforms such as Microsoft Teams, Zoom, Slack, and Cisco Webex;
- Whether the Department, and all components, has implemented security controls to prevent the unauthorized dissemination of controlled unclassified information, personally identifiable information, or sensitive but unclassified information via third-party collaboration platforms;
- The identity, credential, and access management of users that permit remote access to Department networks, including the extent to which the Department has enabled multi-factor authentication and implemented procedures to disable inactive and potentially unauthorized user accounts;
- The distribution and management of virtual and physical assets that facilitate telework, including laptop computers, smartphones, and RSA tokens;
- The Department's adherence to Trusted Internet Connection 3.0 guidance;[9]
- Whether the Department's chief information officer and all component chief information officers implemented additional security policies in response to coronavirus-related telework and how they are enforcing those policies; and
- Whether the Department has implemented continuous monitoring and scanning of networks to identify vulnerabilities.

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

If you have any questions regarding this request, please contact Committee staff at [redacted]. Thank you for your prompt attention to this important matter.

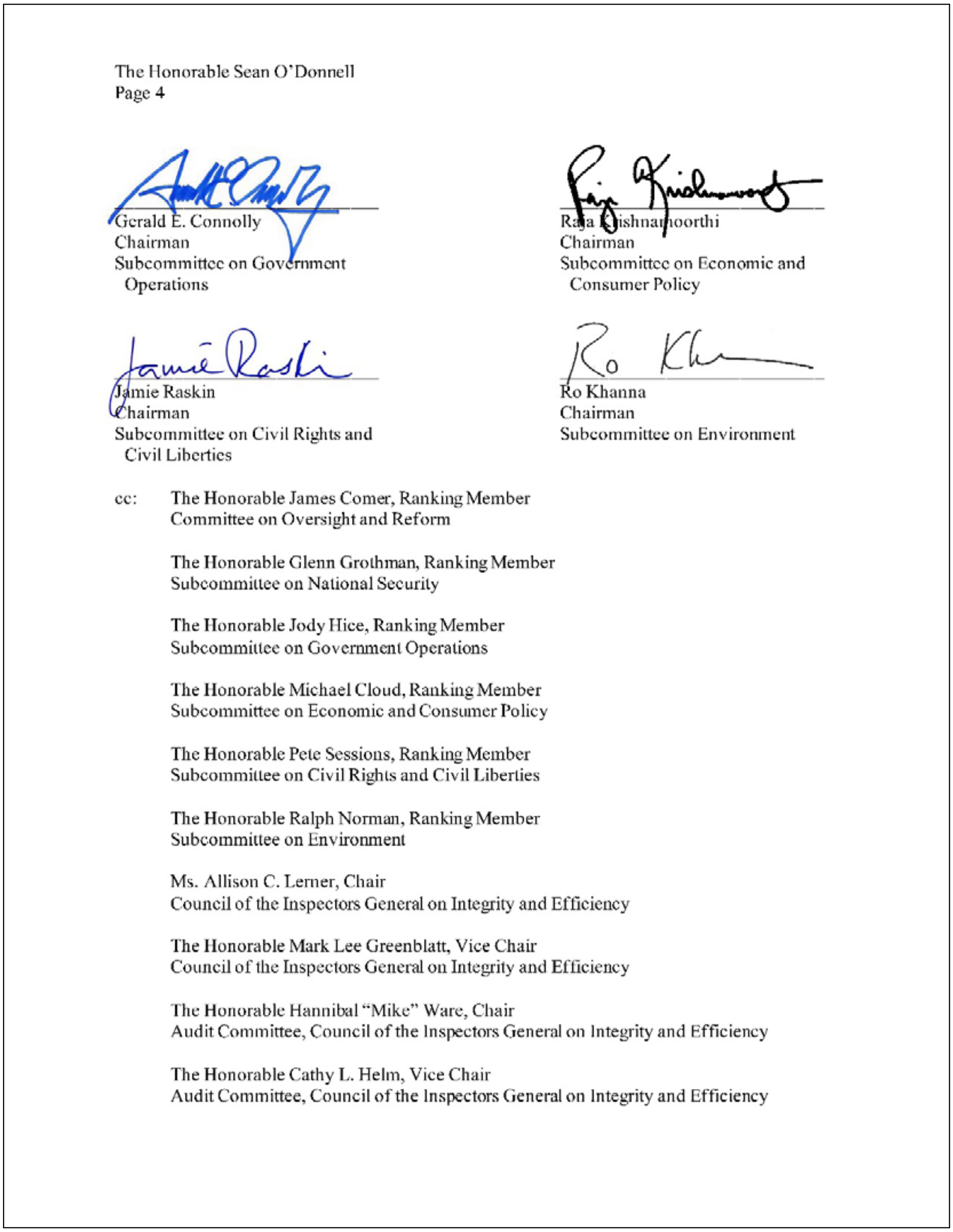
Sincerely,

Carolyn B. Maloney
Carolyn B. Maloney
Chairwoman
Committee on Oversight and Reform

Stephen F. Lynch
Chairman
Subcommittee on National Security

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

(U) House of Representatives, Committee on Oversight and Reform, Congressional Request Letter (cont'd)



The Honorable Sean O'Donnell
Page 4

Gerald E. Connolly
Chairman
Subcommittee on Government
Operations

Raja Krishnamoorthi
Chairman
Subcommittee on Economic and
Consumer Policy

Jamie Raskin

Jamie Raskin
Chairman
Subcommittee on Civil Rights and
Civil Liberties

Ro Kh

Ro Khanna
Chairman
Subcommittee on Environment

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

The Honorable Glenn Grothman, Ranking Member
Subcommittee on National Security

The Honorable Jody Hice, Ranking Member
Subcommittee on Government Operations

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

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

The Honorable Ralph Norman, Ranking Member
Subcommittee on Environment

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

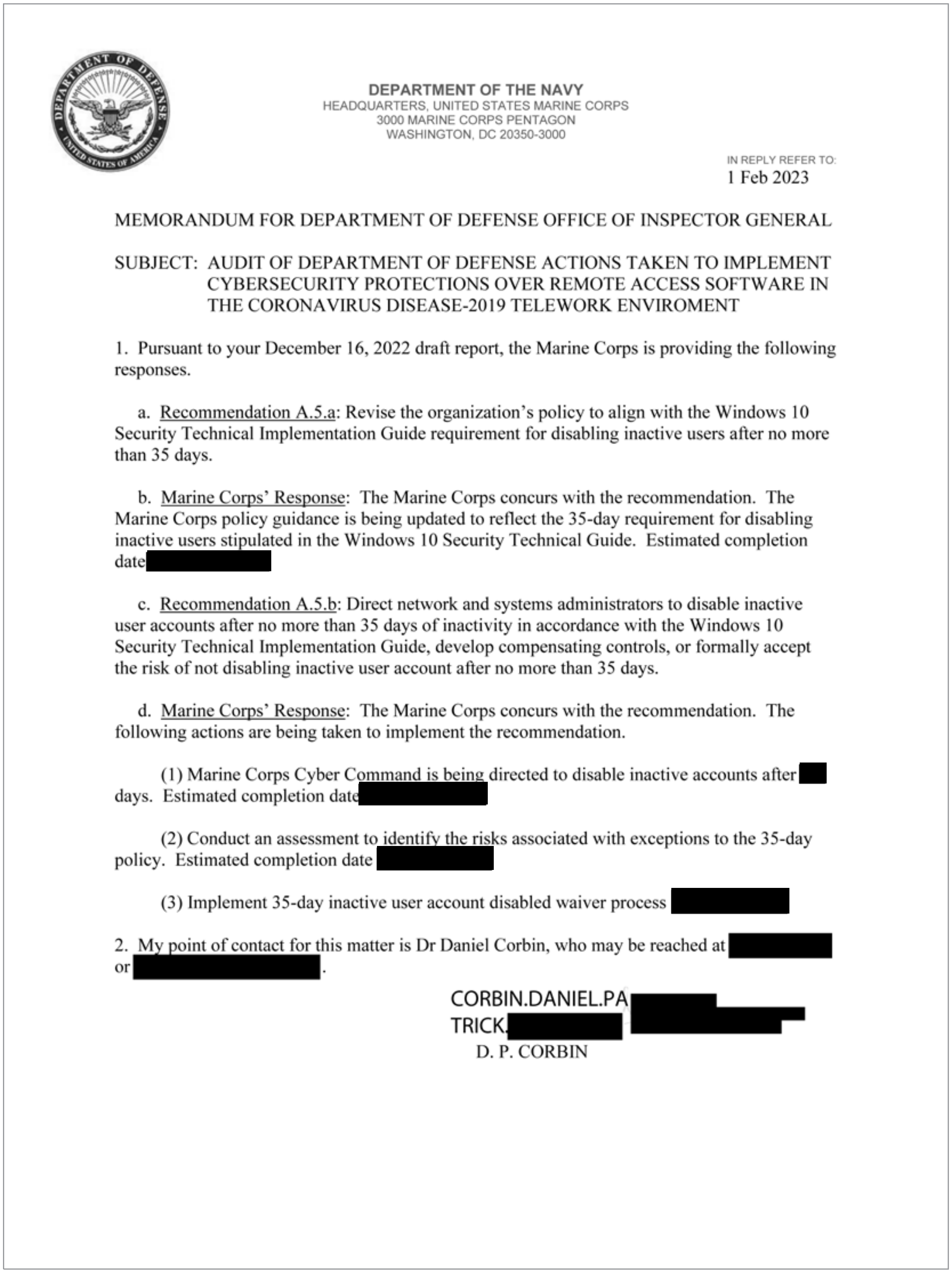
The Honorable Mark Lee Greenblatt, Vice Chair
Council of the Inspectors General on Integrity and Efficiency

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

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

(U) Management Comments

(U) Marine Corps Information Command, Control, Communications, and Computers



DEPARTMENT OF THE NAVY
HEADQUARTERS, UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:
1 Feb 2023

MEMORANDUM FOR DEPARTMENT OF DEFENSE OFFICE OF INSPECTOR GENERAL

SUBJECT: AUDIT OF DEPARTMENT OF DEFENSE ACTIONS TAKEN TO IMPLEMENT CYBERSECURITY PROTECTIONS OVER REMOTE ACCESS SOFTWARE IN THE CORONAVIRUS DISEASE-2019 TELEWORK ENVIROMENT

1. Pursuant to your December 16, 2022 draft report, the Marine Corps is providing the following responses.

a. Recommendation A.5.a: Revise the organization's policy to align with the Windows 10 Security Technical Implementation Guide requirement for disabling inactive users after no more than 35 days.

b. Marine Corps' Response: The Marine Corps concurs with the recommendation. The Marine Corps policy guidance is being updated to reflect the 35-day requirement for disabling inactive users stipulated in the Windows 10 Security Technical Guide. Estimated completion date [redacted]

c. Recommendation A.5.b: Direct network and systems administrators to disable inactive user accounts after no more than 35 days of inactivity in accordance with the Windows 10 Security Technical Implementation Guide, develop compensating controls, or formally accept the risk of not disabling inactive user account after no more than 35 days.

d. Marine Corps' Response: The Marine Corps concurs with the recommendation. The following actions are being taken to implement the recommendation.

(1) Marine Corps Cyber Command is being directed to disable inactive accounts after [redacted] days. Estimated completion date [redacted]

(2) Conduct an assessment to identify the risks associated with exceptions to the 35-day policy. Estimated completion date [redacted]

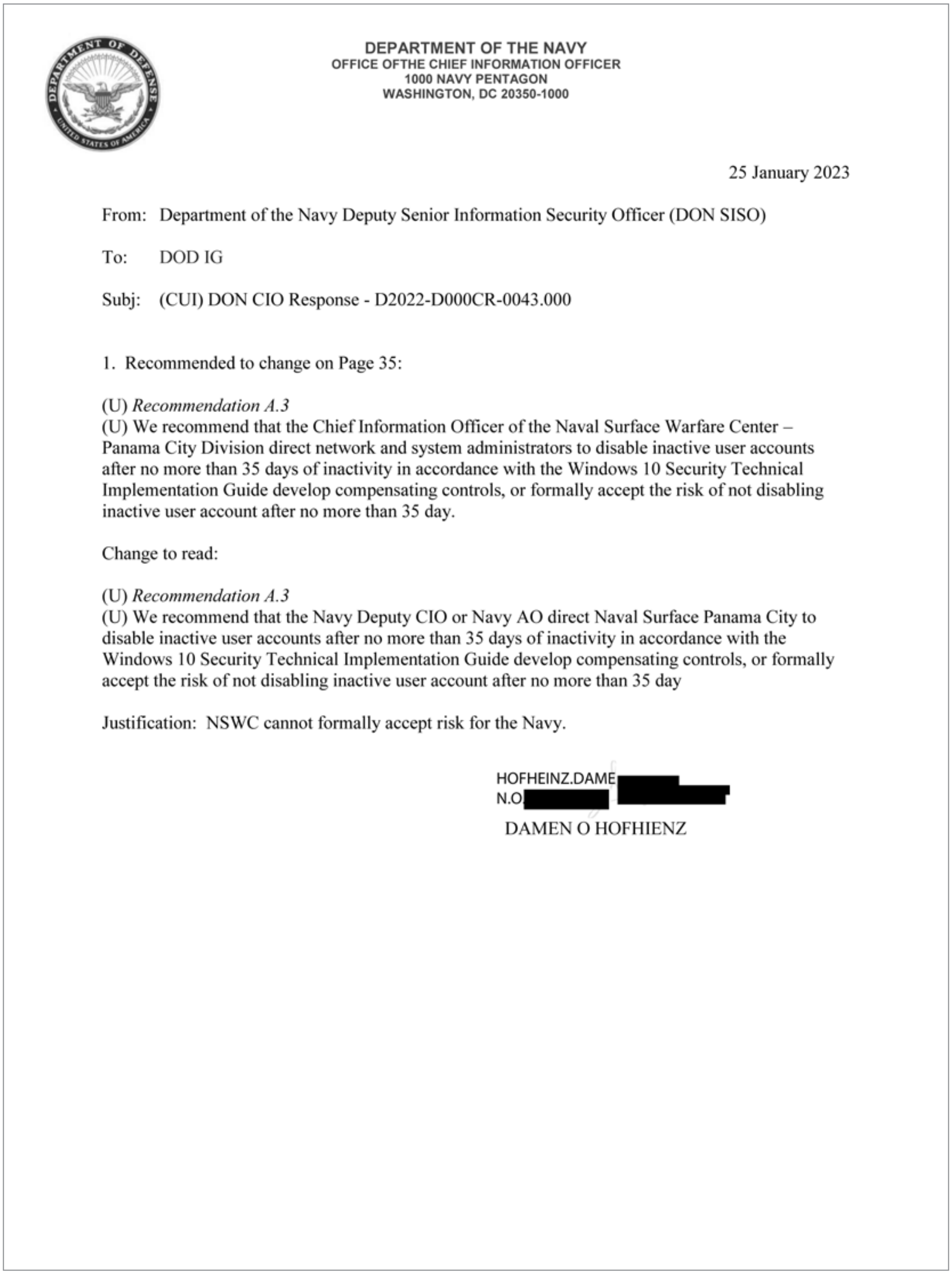
(3) Implement 35-day inactive user account disabled waiver process [redacted]

2. My point of contact for this matter is Dr Daniel Corbin, who may be reached at [redacted] or [redacted].

CORBIN.DANIEL.PA [redacted]
TRICK.[redacted]
D. P. CORBIN

(U) Department of the Navy

Final Report Reference



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

25 January 2023

From: Department of the Navy Deputy Senior Information Security Officer (DON SISO)

To: DOD IG

Subj: (CUI) DON CIO Response - D2022-D000CR-0043.000

1. Recommended to change on Page 35:

(U) *Recommendation A.3*
(U) We recommend that the Chief Information Officer of the Naval Surface Warfare Center – Panama City Division direct network and system administrators to disable inactive user accounts after no more than 35 days of inactivity in accordance with the Windows 10 Security Technical Implementation Guide develop compensating controls, or formally accept the risk of not disabling inactive user account after no more than 35 day.

Recommendation A.3 on page 17

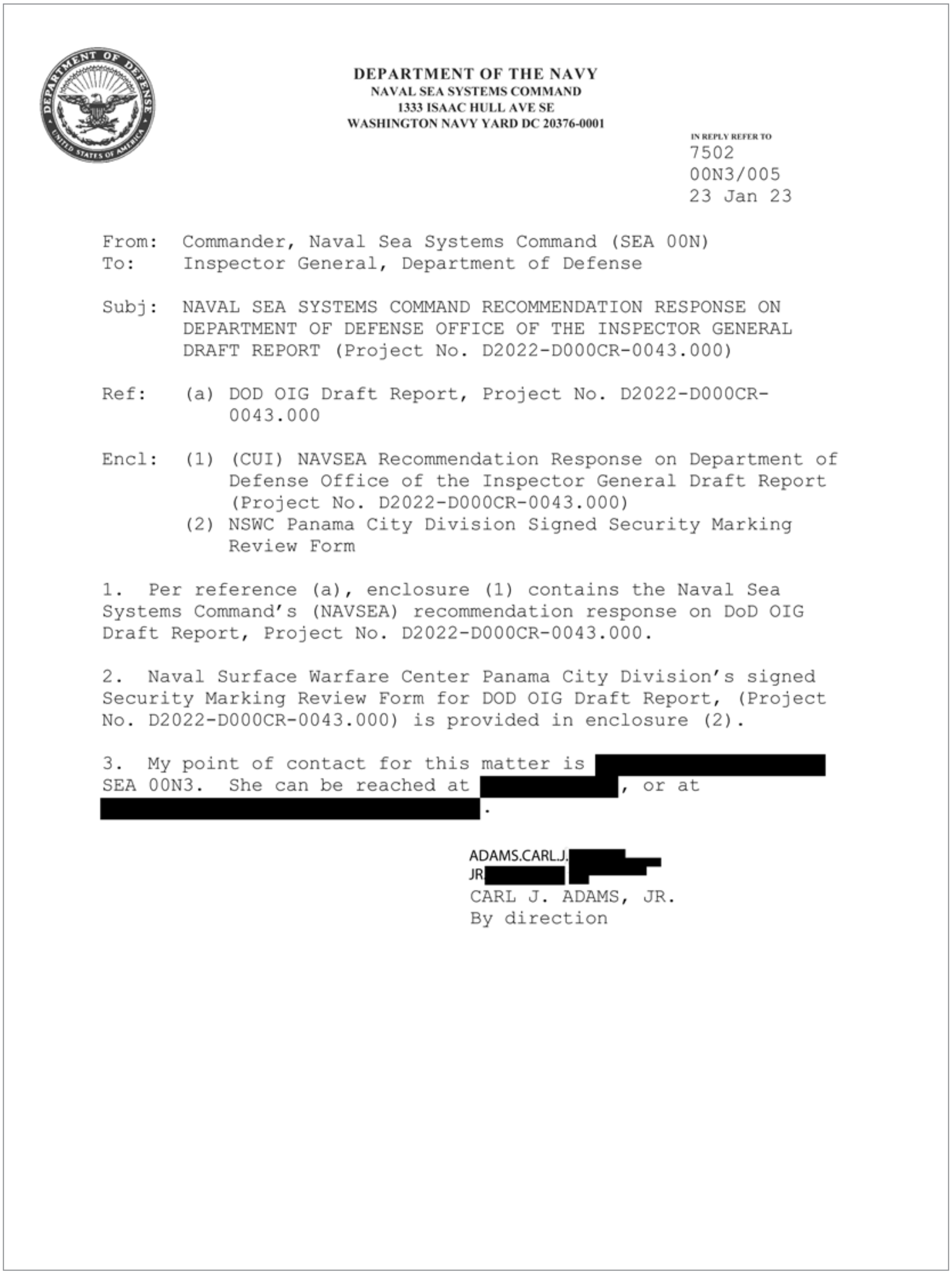
Change to read:

(U) *Recommendation A.3*
(U) We recommend that the Navy Deputy CIO or Navy AO direct Naval Surface Panama City to disable inactive user accounts after no more than 35 days of inactivity in accordance with the Windows 10 Security Technical Implementation Guide develop compensating controls, or formally accept the risk of not disabling inactive user account after no more than 35 day

Justification: NSWC cannot formally accept risk for the Navy.

HOFHEINZ.DAME[redacted]
N.O[redacted]
DAMEN O HOFHIENZ

(U) Naval Sea Systems Command



DEPARTMENT OF THE NAVY
NAVAL SEA SYSTEMS COMMAND
1333 ISAAC HULL AVE SE
WASHINGTON NAVY YARD DC 20376-0001

IN REPLY REFER TO
7502
00N3/005
23 Jan 23

From: Commander, Naval Sea Systems Command (SEA 00N)
To: Inspector General, Department of Defense

Subj: NAVAL SEA SYSTEMS COMMAND RECOMMENDATION RESPONSE ON DEPARTMENT OF DEFENSE OFFICE OF THE INSPECTOR GENERAL DRAFT REPORT (Project No. D2022-D000CR-0043.000)

Ref: (a) DOD OIG Draft Report, Project No. D2022-D000CR-0043.000

Encl: (1) (CUI) NAVSEA Recommendation Response on Department of Defense Office of the Inspector General Draft Report (Project No. D2022-D000CR-0043.000)
(2) NSWC Panama City Division Signed Security Marking Review Form

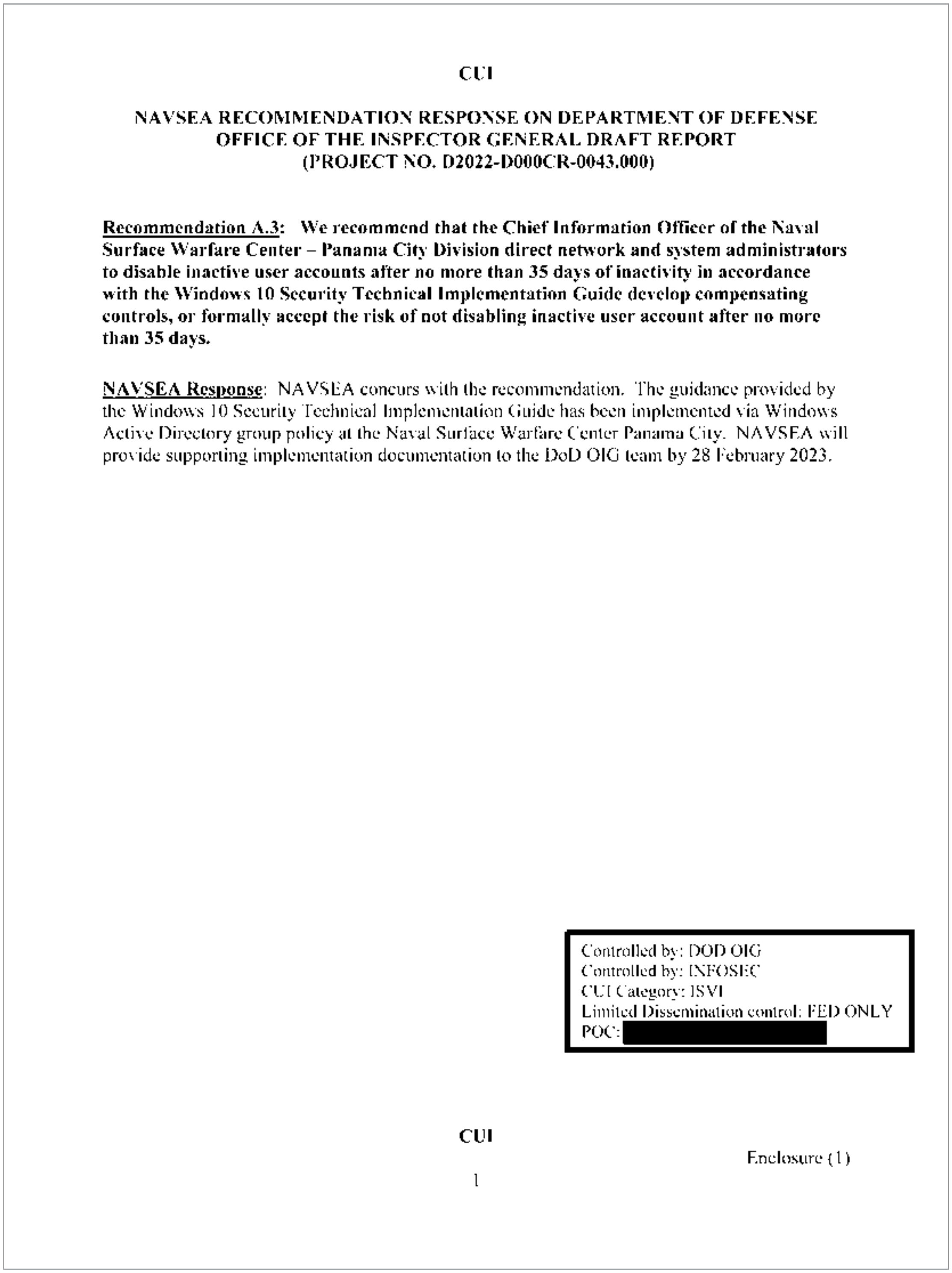
1. Per reference (a), enclosure (1) contains the Naval Sea Systems Command's (NAVSEA) recommendation response on DoD OIG Draft Report, Project No. D2022-D000CR-0043.000.

2. Naval Surface Warfare Center Panama City Division's signed Security Marking Review Form for DOD OIG Draft Report, (Project No. D2022-D000CR-0043.000) is provided in enclosure (2).

3. My point of contact for this matter is [redacted] SEA 00N3. She can be reached at [redacted], or at [redacted].

ADAMS.CARL.J.[redacted]
JR[redacted]
CARL J. ADAMS, JR.
By direction

(U) Naval Sea Systems Command (cont'd)



CUI

NAVSEA RECOMMENDATION RESPONSE ON DEPARTMENT OF DEFENSE OFFICE OF THE INSPECTOR GENERAL DRAFT REPORT (PROJECT NO. D2022-D000CR-0043.000)

Recommendation A.3: We recommend that the Chief Information Officer of the Naval Surface Warfare Center – Panama City Division direct network and system administrators to disable inactive user accounts after no more than 35 days of inactivity in accordance with the Windows 10 Security Technical Implementation Guide develop compensating controls, or formally accept the risk of not disabling inactive user account after no more than 35 days.

NAVSEA Response: NAVSEA concurs with the recommendation. The guidance provided by the Windows 10 Security Technical Implementation Guide has been implemented via Windows Active Directory group policy at the Naval Surface Warfare Center Panama City. NAVSEA will provide supporting implementation documentation to the DoD OIG team by 28 February 2023.

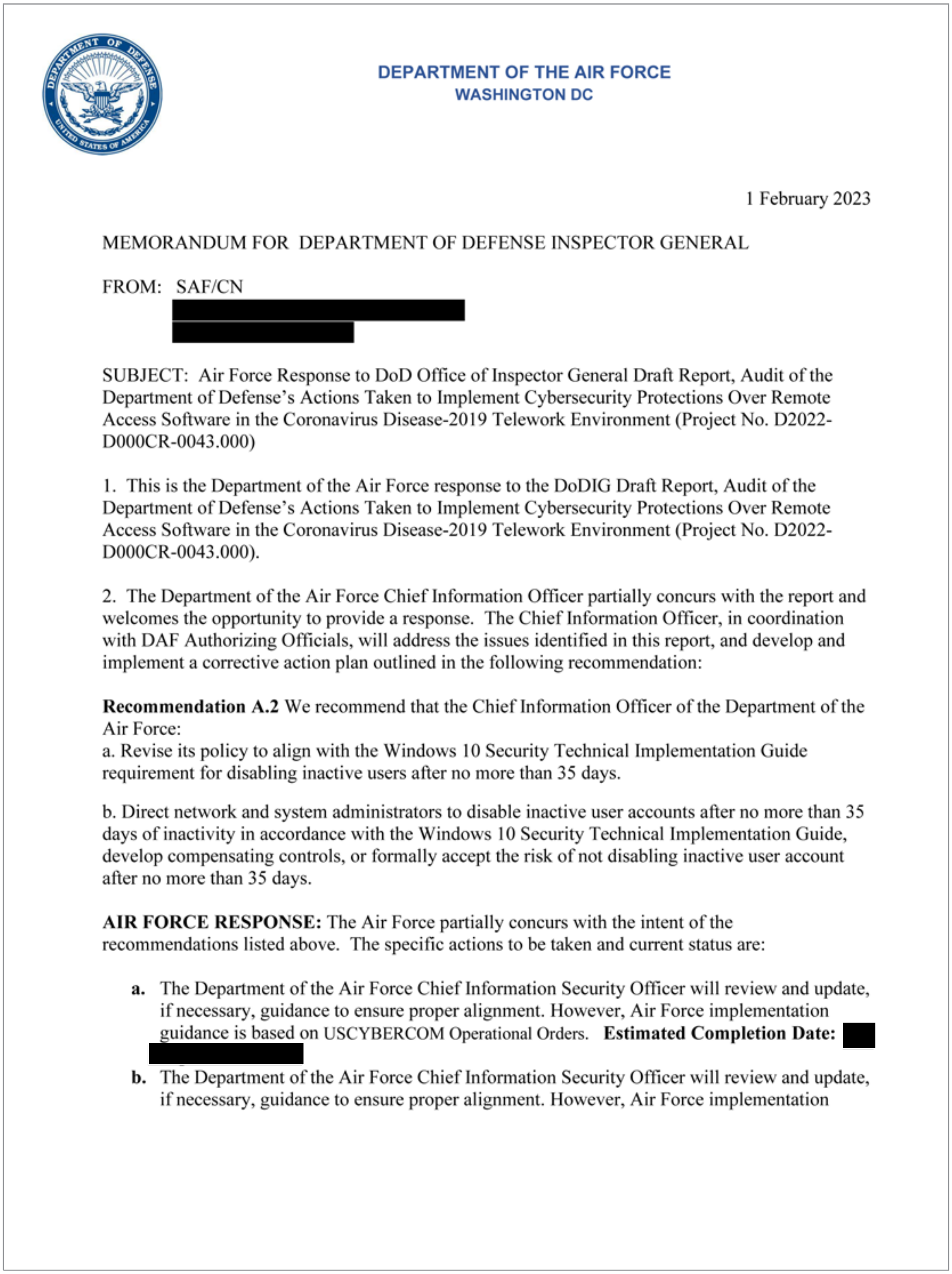
Controlled by: DOD OIG
Controlled by: INFOSEC
CUI Category: ISVI
Limited Dissemination control: FED ONLY
POC: [redacted]

CUI

Enclosure (1)

1

(U) Department of the Air Force



DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

1 February 2023

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

FROM: SAF/CN
[redacted]

SUBJECT: Air Force Response to DoD Office of Inspector General Draft Report, Audit of the Department of Defense's Actions Taken to Implement Cybersecurity Protections Over Remote Access Software in the Coronavirus Disease-2019 Telework Environment (Project No. D2022-D000CR-0043.000)

1. This is the Department of the Air Force response to the DoDIG Draft Report, Audit of the Department of Defense's Actions Taken to Implement Cybersecurity Protections Over Remote Access Software in the Coronavirus Disease-2019 Telework Environment (Project No. D2022-D000CR-0043.000).

2. The Department of the Air Force Chief Information Officer partially concurs with the report and welcomes the opportunity to provide a response. The Chief Information Officer, in coordination with DAF Authorizing Officials, will address the issues identified in this report, and develop and implement a corrective action plan outlined in the following recommendation:

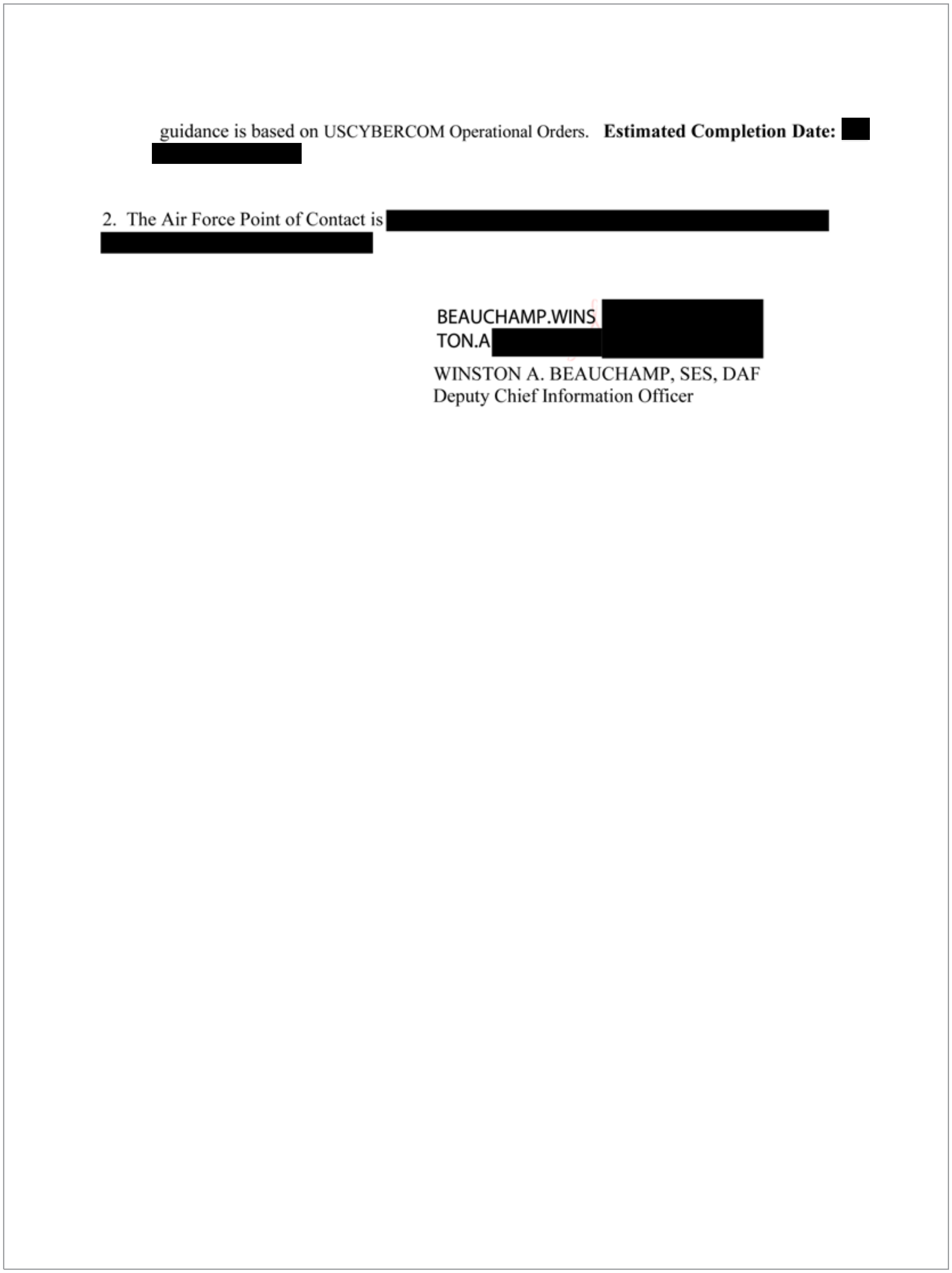
Recommendation A.2 We recommend that the Chief Information Officer of the Department of the Air Force:
a. Revise its policy to align with the Windows 10 Security Technical Implementation Guide requirement for disabling inactive users after no more than 35 days.

b. Direct network and system administrators to disable inactive user accounts after no more than 35 days of inactivity in accordance with the Windows 10 Security Technical Implementation Guide, develop compensating controls, or formally accept the risk of not disabling inactive user account after no more than 35 days.

AIR FORCE RESPONSE: The Air Force partially concurs with the intent of the recommendations listed above. The specific actions to be taken and current status are:

- **a.** The Department of the Air Force Chief Information Security Officer will review and update, if necessary, guidance to ensure proper alignment. However, Air Force implementation guidance is based on USCYBERCOM Operational Orders. **Estimated Completion Date:** [redacted]
- **b.** The Department of the Air Force Chief Information Security Officer will review and update, if necessary, guidance to ensure proper alignment. However, Air Force implementation

(U) Department of the Air Force (cont'd)



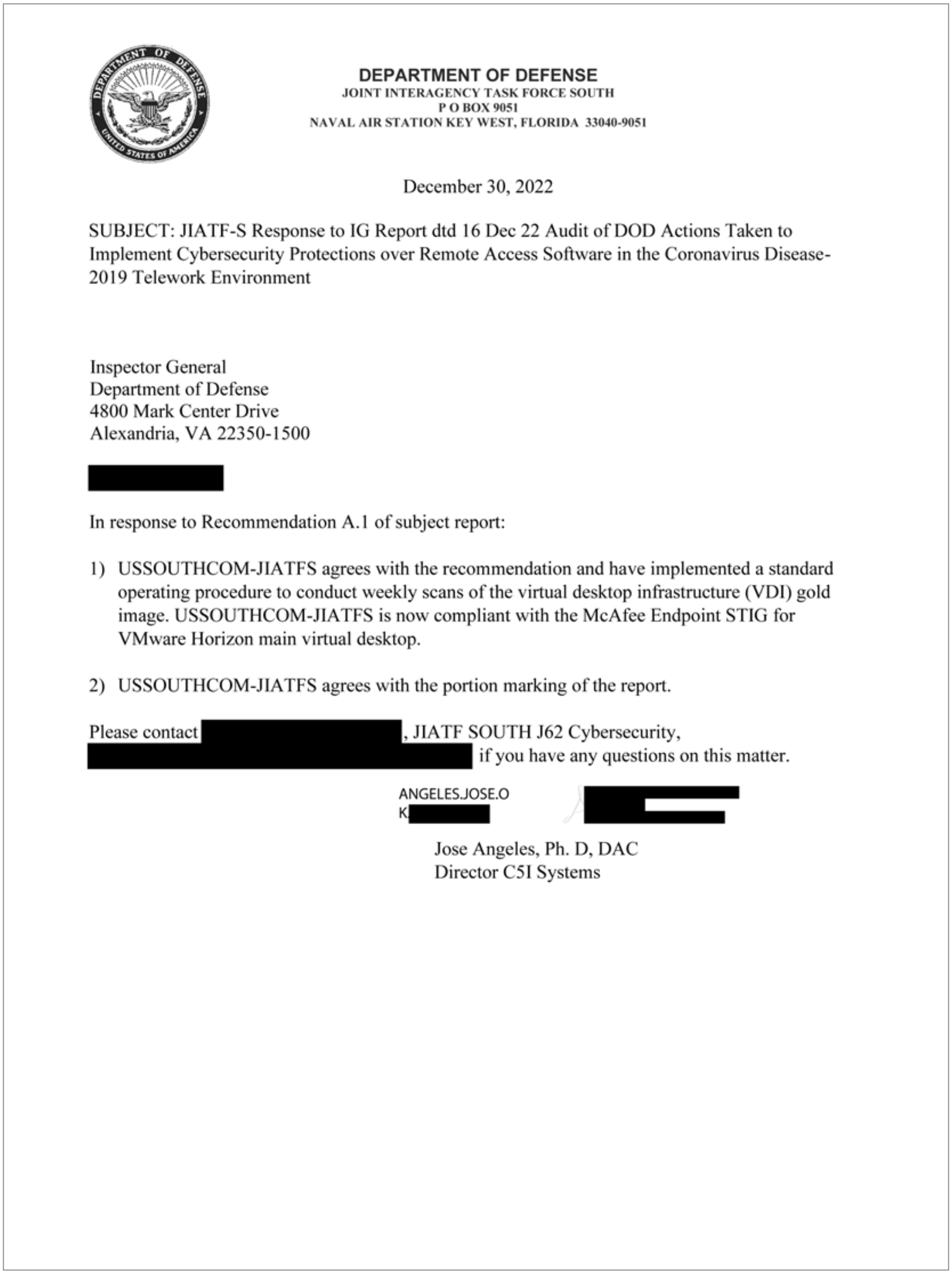
guidance is based on USCYBERCOM Operational Orders. **Estimated Completion Date:** [redacted]

2. The Air Force Point of Contact is [redacted]

BEAUCHAMP.WINS
TON.A [redacted]

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

(U) U.S. Southen Command - Joint Interagency Task Force South



DEPARTMENT OF DEFENSE
JOINT INTERAGENCY TASK FORCE SOUTH
P O BOX 9051
NAVAL AIR STATION KEY WEST, FLORIDA 33040-9051

December 30, 2022

SUBJECT: JIATF-S Response to IG Report dtd 16 Dec 22 Audit of DOD Actions Taken to Implement Cybersecurity Protections over Remote Access Software in the Coronavirus Disease-2019 Telework Environment

Inspector General
Department of Defense
4800 Mark Center Drive
Alexandria, VA 22350-1500

[redacted]

In response to Recommendation A.1 of subject report:

1) USSOUTHCOM-JIATFS agrees with the recommendation and have implemented a standard operating procedure to conduct weekly scans of the virtual desktop infrastructure (VDI) gold image. USSOUTHCOM-JIATFS is now compliant with the McAfee Endpoint STIG for VMware Horizon main virtual desktop.

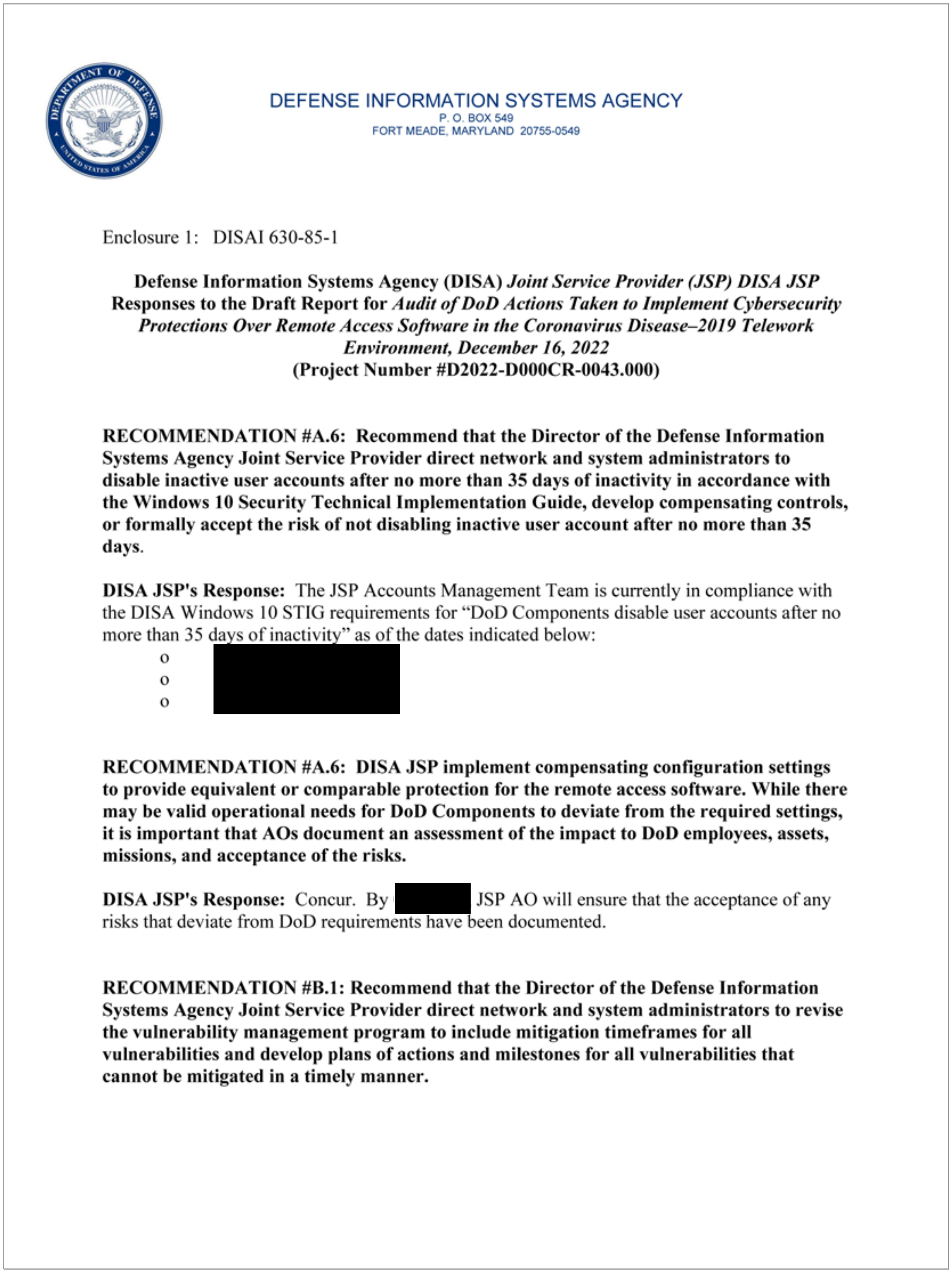
2) USSOUTHCOM-JIATFS agrees with the portion marking of the report.

Please contact [redacted], JIATF SOUTH J62 Cybersecurity, [redacted] if you have any questions on this matter.

ANGELES.JOSE.O
K[redacted] [redacted]

Jose Angeles, Ph. D, DAC
Director C5I Systems

(U) Defense Information Systems Agency Joint Service Provider



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

Enclosure 1: DISAI 630-85-1

Defense Information Systems Agency (DISA) ***Joint Service Provider (JSP) DISA JSP*** **Responses to the Draft Report for** ***Audit of DoD Actions Taken to Implement Cybersecurity Protections Over Remote Access Software in the Coronavirus Disease–2019 Telework Environment, December 16, 2022*** **(Project Number #D2022-D000CR-0043.000)**

RECOMMENDATION #A.6: Recommend that the Director of the Defense Information Systems Agency Joint Service Provider direct network and system administrators to disable inactive user accounts after no more than 35 days of inactivity in accordance with the Windows 10 Security Technical Implementation Guide, develop compensating controls, or formally accept the risk of not disabling inactive user account after no more than 35 days.

DISA JSP's Response: The JSP Accounts Management Team is currently in compliance with the DISA Windows 10 STIG requirements for "DoD Components disable user accounts after no more than 35 days of inactivity" as of the dates indicated below:

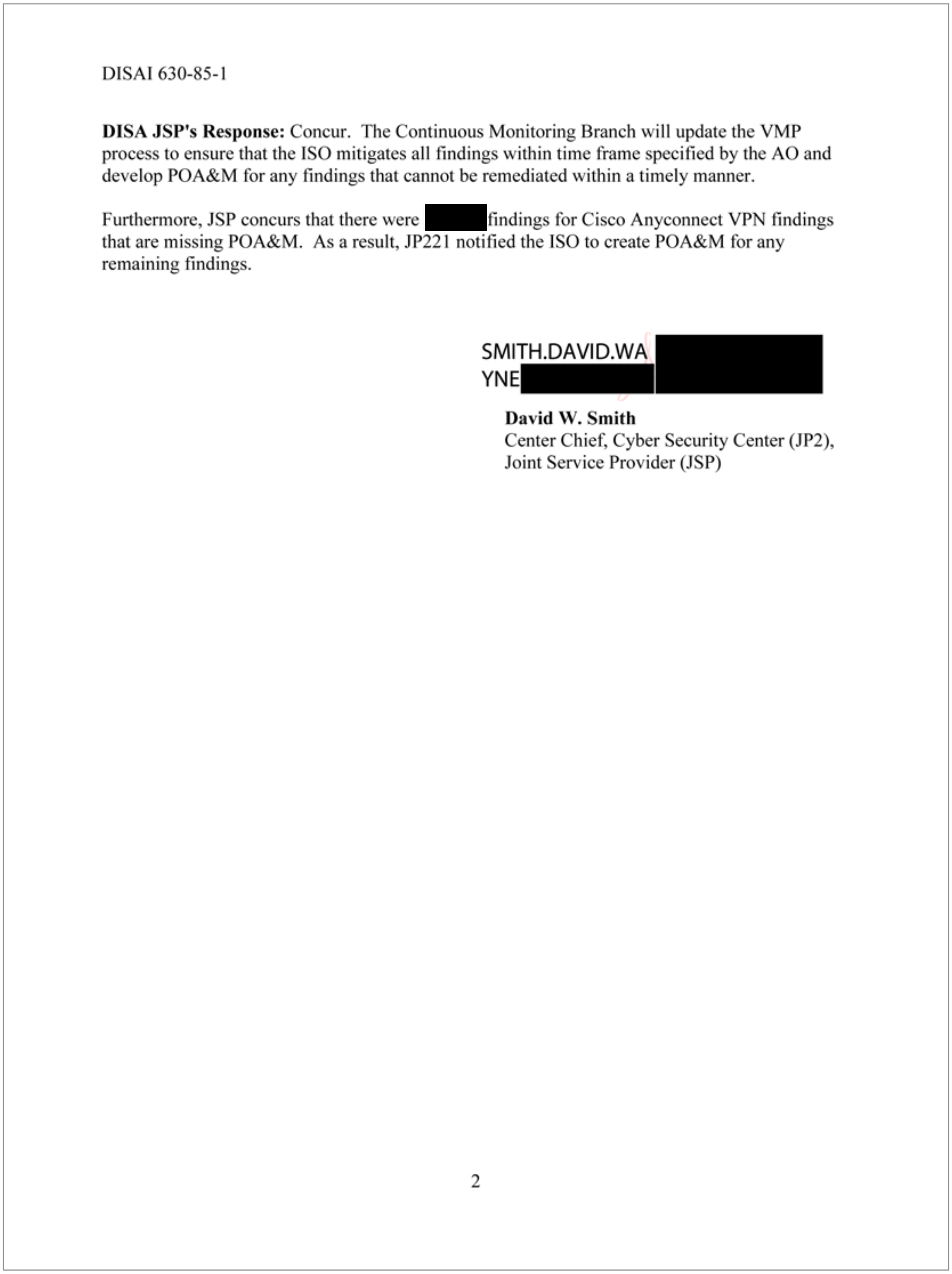
o [redacted]
o
o

RECOMMENDATION #A.6: DISA JSP implement compensating configuration settings to provide equivalent or comparable protection for the remote access software. While there may be valid operational needs for DoD Components to deviate from the required settings, it is important that AOs document an assessment of the impact to DoD employees, assets, missions, and acceptance of the risks.

DISA JSP's Response: Concur. By [redacted] JSP AO will ensure that the acceptance of any risks that deviate from DoD requirements have been documented.

RECOMMENDATION #B.1: Recommend that the Director of the Defense Information Systems Agency Joint Service Provider direct network and system administrators to revise the vulnerability management program to include mitigation timeframes for all vulnerabilities and develop plans of actions and milestones for all vulnerabilities that cannot be mitigated in a timely manner.

(U) Defense Information Systems Agency Joint Service Provider (cont'd)



DISAI 630-85-1

DISA JSP's Response: Concur. The Continuous Monitoring Branch will update the VMP process to ensure that the ISO mitigates all findings within time frame specified by the AO and develop POA&M for any findings that cannot be remediated within a timely manner.

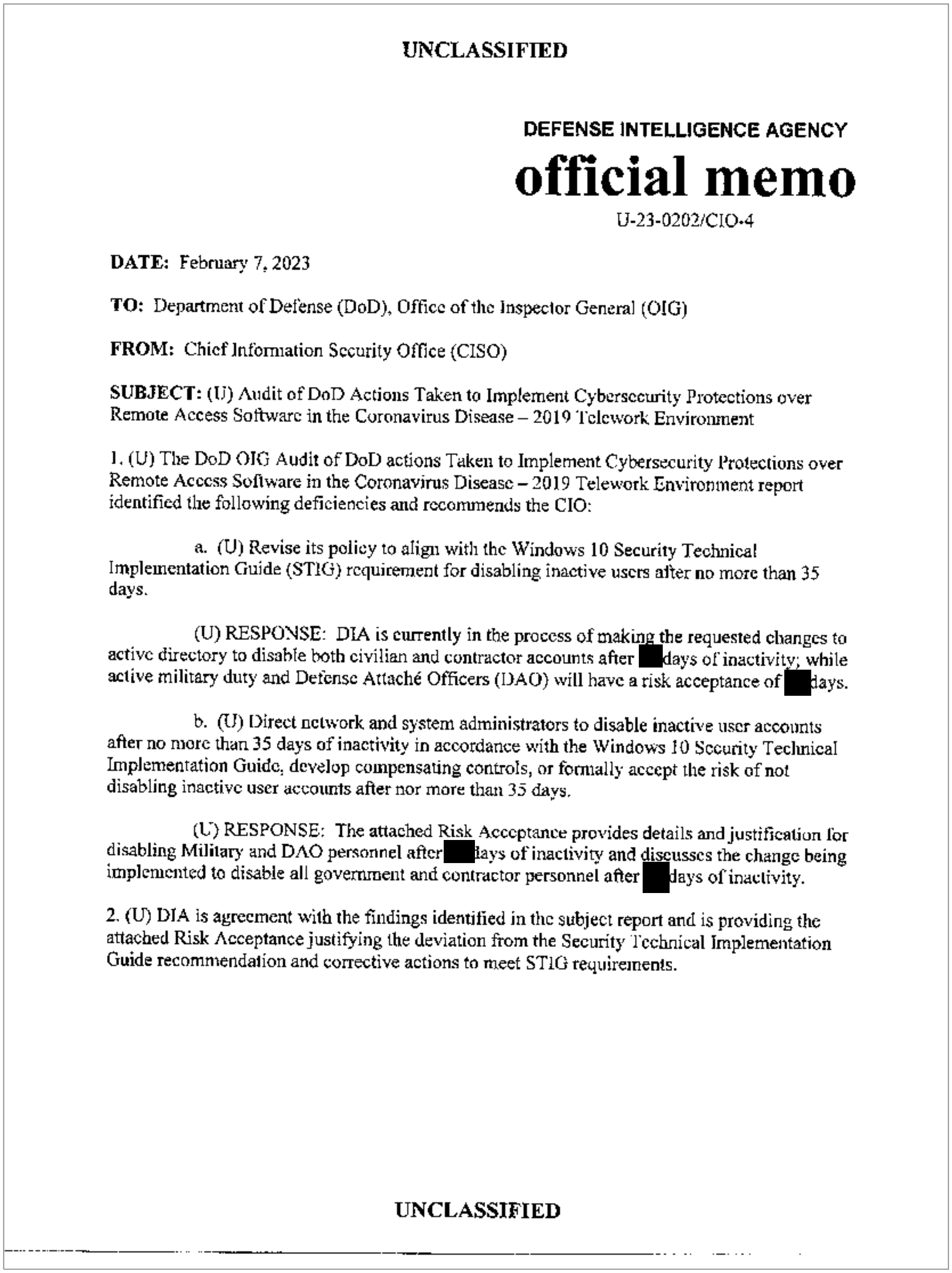
Furthermore, JSP concurs that there were [redacted] findings for Cisco Anyconnect VPN findings that are missing POA&M. As a result, JP221 notified the ISO to create POA&M for any remaining findings.

SMITH.DAVID.WA [redacted]
YNE [redacted]

David W. Smith
Center Chief, Cyber Security Center (JP2),
Joint Service Provider (JSP)

2

(U) Defense Intelligence Agency



UNCLASSIFIED

DEFENSE INTELLIGENCE AGENCY
official memo
U-23-0202/CIO-4

DATE: February 7, 2023

TO: Department of Defense (DoD), Office of the Inspector General (OIG)

FROM: Chief Information Security Office (CISO)

SUBJECT: (U) Audit of DoD Actions Taken to Implement Cybersecurity Protections over Remote Access Software in the Coronavirus Disease – 2019 Telework Environment

1. (U) The DoD OIG Audit of DoD actions Taken to Implement Cybersecurity Protections over Remote Access Software in the Coronavirus Disease – 2019 Telework Environment report identified the following deficiencies and recommends the CIO:

a. (U) Revise its policy to align with the Windows 10 Security Technical Implementation Guide (STIG) requirement for disabling inactive users after no more than 35 days.

(U) RESPONSE: DIA is currently in the process of making the requested changes to active directory to disable both civilian and contractor accounts after [redacted] days of inactivity; while active military duty and Defense Attaché Officers (DAO) will have a risk acceptance of [redacted] days.

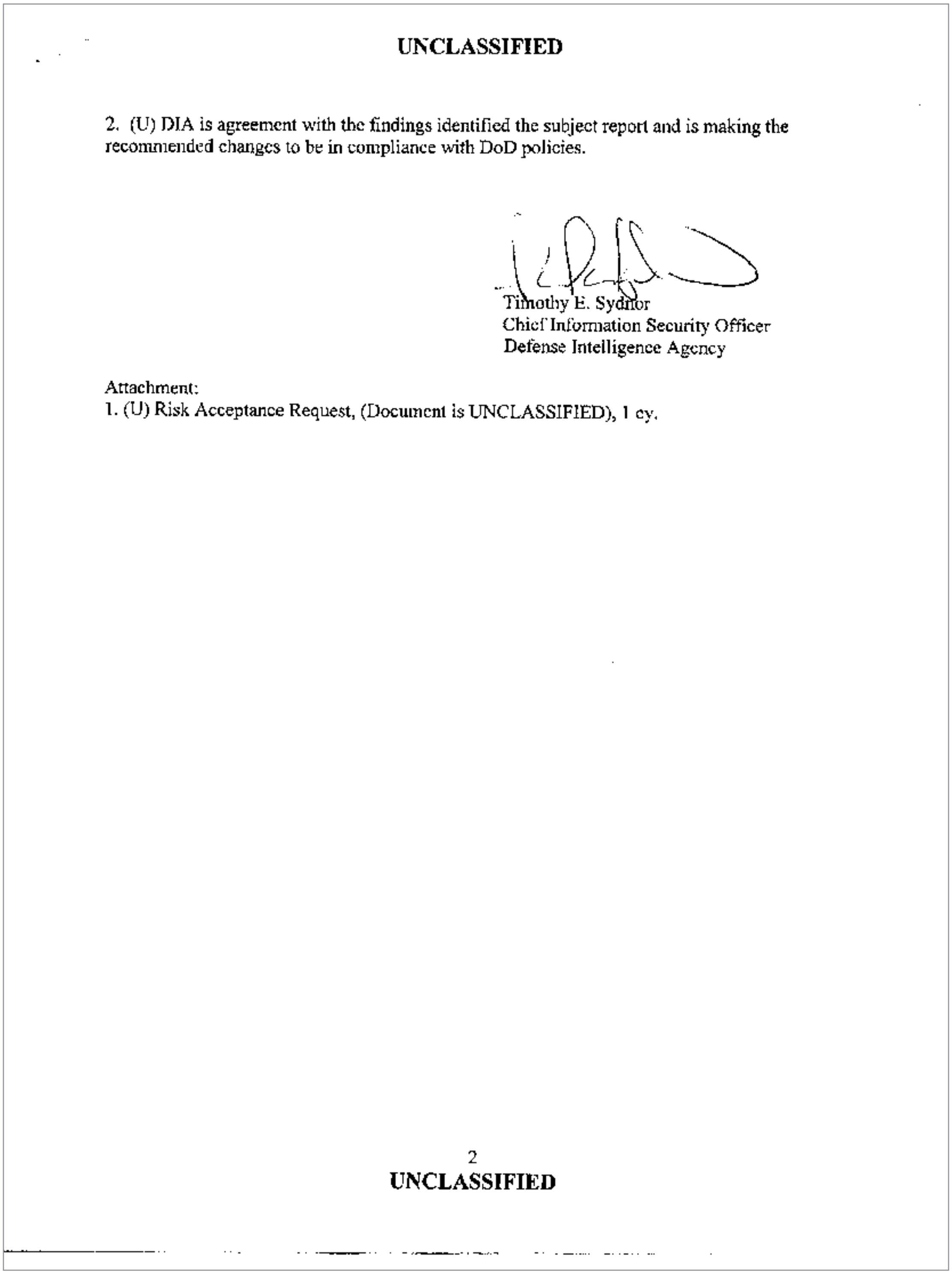
b. (U) Direct network and system administrators to disable inactive user accounts after no more than 35 days of inactivity in accordance with the Windows 10 Security Technical Implementation Guide, develop compensating controls, or formally accept the risk of not disabling inactive user accounts after nor more than 35 days.

(U) RESPONSE: The attached Risk Acceptance provides details and justification for disabling Military and DAO personnel after [redacted] days of inactivity and discusses the change being implemented to disable all government and contractor personnel after [redacted] days of inactivity.

2. (U) DIA is agreement with the findings identified in the subject report and is providing the attached Risk Acceptance justifying the deviation from the Security Technical Implementation Guide recommendation and corrective actions to meet STIG requirements.

UNCLASSIFIED

(U) Defense Intelligence Agency (cont'd)



UNCLASSIFIED

2. (U) DIA is agreement with the findings identified the subject report and is making the recommended changes to be in compliance with DoD policies.

Timothy E. Sydnor
Chief Information Security Officer
Defense Intelligence Agency

Attachment:
1. (U) Risk Acceptance Request, (Document is UNCLASSIFIED), 1 cy.

2
UNCLASSIFIED

(U) Acronyms and Abbreviations

(U) AO	Authorizing Official
(U) CIO	Chief Information Officer
(U) COVID-19	Coronavirus Disease–2019
(U) DCMA	Defense Contract Management Agency
(U) DIA	Defense Intelligence Agency
(U) DISA	Defense Information Systems Agency
(U) DoDEA	DoD Education Activity
(U) GAO	Government Accountability Office
(U) IAVA	Information Assurance Vulnerability Alert
(U) JIATFS	Joint Interagency Task Force South
(U) JSP	Joint Service Provider
(U) NIST	National Institute of Standards and Technology
(U) NSWC-PCD	Naval Surface Warfare Center – Panama City Division
(U) OPORD	Operation Order
(U) POA&M	Plan of Action and Milestone
(U) SP	Special Publication
(U) SRG	Security Requirements Guide
(U) STIG	Security Technical Implementation Guide
(U) USCYBERCOM	U.S. Cyber Command
(U) USMC	U.S. Marine Corps
(U) USSOUTHCOM	U.S. Southern Command
(U) VDI	Virtual Desktop Infrastructure
(U) VPN	Virtual Private Network

(U) Glossary

(U) Availability. Ensuring timely and reliable access to and use of information.

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

(U) Configuration Management. The process of maintaining compliance with cybersecurity requirements on information technology hardware and software by initializing, changing, and monitoring the configuration settings of the hardware and software

(U) 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.

(U) Direct Application Access. Allows a user to directly access an application without using remote access software. A common example of direct application access is webmail.

(U) DoD Field Activities. Provide support services to the DoD.

(U) End-User Device. A personal computer, smart phone, or removable storage media, such as a memory card or external hard drive that can store information.

(U) Government-Furnished Equipment. Property that is in the possession of, owned, acquired, or leased, by the government.

(U) Information Assurance Vulnerability Alert. A notification that is generated when an information assurance vulnerability may result in an immediate and potentially severe threat to DoD systems and information.

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

(U) Internet Protocol Security. A protocol that adds security features to the standard Internet Protocol to provide confidentiality and integrity services.

(U) Non-Classified Internet Protocol Routing Network. A network used by DoD personnel to exchange unclassified information.

(U) Pandemic. A global outbreak of a disease that can infect people and spread between people sustainably.

(U) 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.

(U) Plan of Action and Milestone. A document that identifies tasks that need to be accomplished, the resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

(U) Portal. A server that offers access to one or more application through a single, centralized interface.

(U) 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.

(U) Remote Access Software. Software that gives an authorized person the ability to access a computer or network from a geographical distance through an external network connection, such as the Internet.

(U) Remote Desktop Solution. Gives the authorized user the ability to remotely control a particular computer at an organization, most often, the user’s own computer.

(U) Risk Tolerance. The level of risk or the degree of uncertainty that is acceptable to an organization.

(U) 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.

(U) Secure Sockets Layer. A protocol used to protect private information during the transmission of data over the Internet.

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

(U) 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.

(U) Technology Family. A group of related technologies with common characteristics such as applications, networks, or operating systems.

(U) Telework. The ability for an organization's employees and contractors (also known as teleworkers) to conduct work from locations other than the organization's facilities.

(U) Tunneling. Offers a secure connection to transmit information between networks. Tunnels are typically established through a virtual private network.

(U) Virtual Desktop Infrastructure. A software that remotely accesses a desktop through a centralized server and displays it on a teleworker's laptop.

(U) Virtual Private Network. A software that remotely connects an employee's device to the organization's network.

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

Whistleblower Protection

U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, 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

CUI

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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

CUI