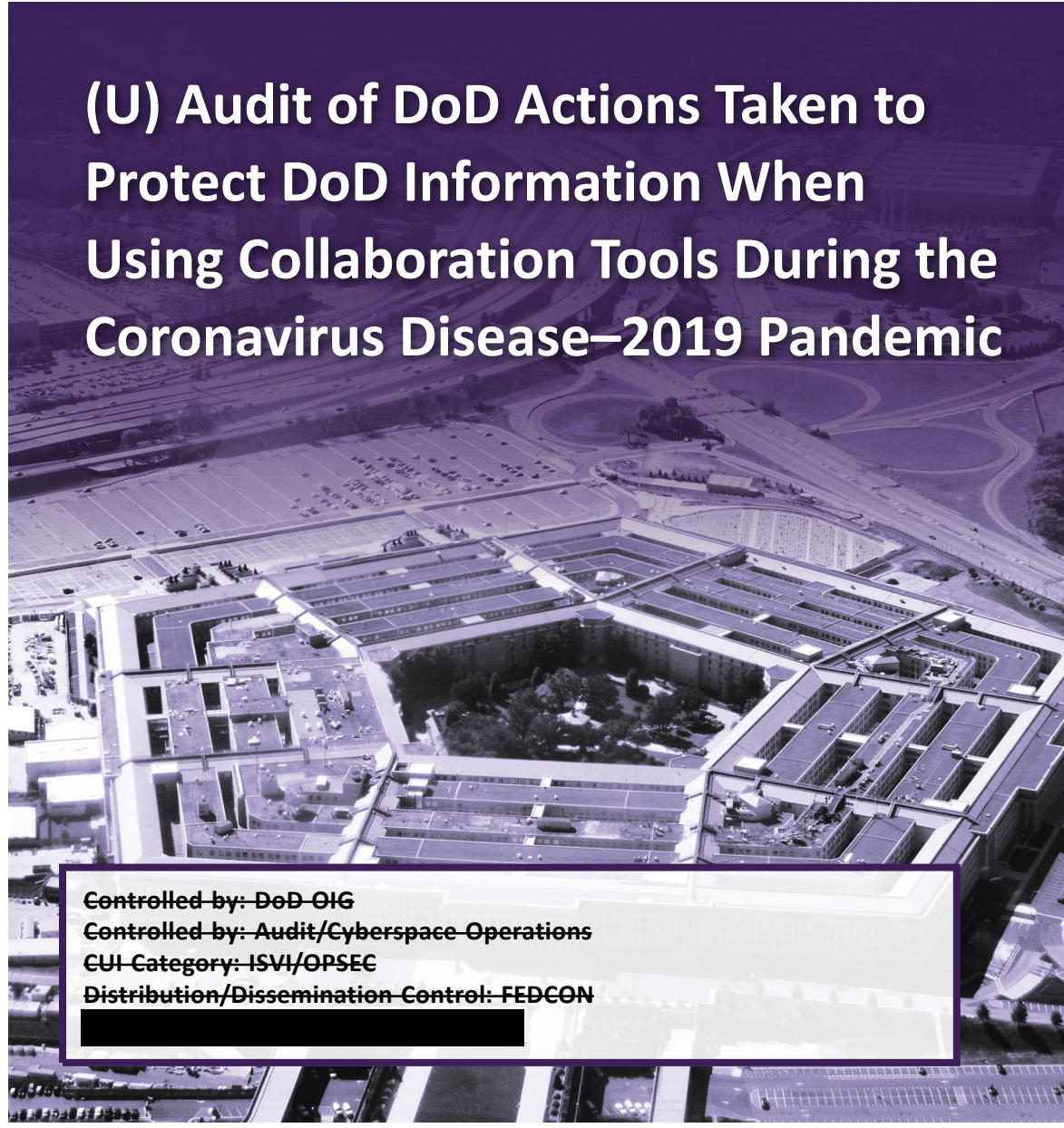


CUI

# INSPECTOR GENERAL

*U.S. Department of Defense*

JUNE 6, 2023



## (U) Audit of DoD Actions Taken to Protect DoD Information When Using Collaboration Tools During the Coronavirus Disease–2019 Pandemic

Controlled by: DoD-OIG  
Controlled by: Audit/Cyberspace Operations  
CUI Category: ISVI/OPSEC  
Distribution/Dissemination Control: FEDCON

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

CUI





# (U) Results in Brief

## *(U) Audit of DoD Actions Taken to Protect DoD Information When Using Collaboration Tools During the Coronavirus Disease–2019 Pandemic*

**(U) June 6, 2023**

### **(U) Objective**

(U) The objective of this audit was to determine whether the DoD's increased use of collaboration tools to facilitate telework during the coronavirus disease–2019 pandemic exposed DoD networks and systems to potential malicious activity. We also determined the extent to which the DoD implemented security controls and configuration settings to protect DoD networks when using collaboration tools.

### **(U) Background**

(U) Collaboration tools include applications that allow employees to conduct meetings and work together virtually regardless of their physical location. Organizations use collaboration tools to boost productivity and connect users while teleworking. In April 2020, to support increased telework during the pandemic, the DoD Chief Information Officer (CIO) directed DoD Components to use collaboration tools provided by the Defense Information Systems Agency (DISA). If the enterprise tools did not fully meet the needs of DoD Components, the DoD could use alternative tools, or submit a tool to the DoD CIO and U.S. Cyber Command for approval.

### **(U) Findings**

(U) Four of the nine DoD Components that we assessed did not complete required steps outlined in a DoD Instruction before deploying collaboration tools on

### **(U) Findings (cont'd)**

(U) Component networks. Additionally, network and system administrators for four of the nine DoD Components we assessed did not ensure that all critical configuration settings or cybersecurity controls were implemented to reduce the risk of exposing DoD networks and systems to potential malicious activity.

(U) These issues occurred because DoD Component administrators incorrectly believed that the assessment and authorization performed by the Federal Risk Authorization and Management Program, and provisional authorization to operate issued by DISA, negated the need for the required reciprocity steps and that the configuration controls for the collaboration tools already aligned with the applicable cybersecurity requirements.

(U) Operating collaboration tools without required cybersecurity controls increases the risk that malicious cyber actors could exploit vulnerable configuration settings and cybersecurity controls, compromising information shared using these collaboration tools.

### **(U) Recommendations**

(U) We made 13 recommendations to address the findings in this report. Among other recommendations, we recommend that the DoD CIO issue guidance that specifically states that deploying a collaboration tool with a provisional authorization does not eliminate the need to perform the required cybersecurity reciprocity process. In addition, we recommend that the Components ensure their collaboration tools comply with DoD instructions and configure, or renegotiate changes with the vendor to configure, their tools to meet DoD requirements.



# (U) Results in Brief

---

## *(U) Audit of DoD Actions Taken to Protect DoD Information When Using Collaboration Tools During the Coronavirus Disease-2019 Pandemic*

### **(U) Management Comments and Our Response**

(U) Officials from the Defense Finance and Accounting Service, Defense Logistics Agency, and Defense Threat Reduction Agency agreed with the recommendations and described actions planned and taken to resolve or close the recommendations. Comments from the DoD CIO partially addressed the recommendations and the Army Cyber Command did not respond to a recommendation; therefore, the recommendations are unresolved. We request additional comments within 30 days. 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 Defense	A.1.a	A.1.b	None
Chief Information Officer, Defense Finance and Accounting Service	None	B.1.a, B.1.b	None
Authorizing Official, Defense Finance and Accounting Service	None	A.2	None
Chief Information Officer, Defense Logistics Agency	None	C.1	B.2
Authorizing Official, Defense Logistics Agency	None	None	A.3
Chief Information Officer, Defense Threat Reduction Agency	None	B.3.c	B.3.a, B.3.b
Authorizing Official, Defense Threat Reduction Agency	None	None	A.4
Authorizing Official, U.S. Army Cyber Command	A.5	None	None

**(U)**

(U) Please provide Management Comments by July 6, 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.





CUI

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

June 6, 2023

(U) MEMORANDUM FOR CHIEF INFORMATION OFFICER OF THE DEPARTMENT  
OF DEFENSE

DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE  
DIRECTOR, DEFENSE LOGISTICS AGENCY  
DIRECTOR, DEFENSE THREAT REDUCTION AGENCY  
DIRECTOR, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY  
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

(U) SUBJECT: Audit of DoD Actions Taken to Protect DoD Information When Using  
Collaboration Tools During the Coronavirus Disease-2019 Pandemic  
(Report No. DODIG-2023-079)

(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 two 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 the 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 six 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 we receive documentation showing that all agreed-upon actions to implement the recommendations are completed.

(U) This report contains five recommendations that are considered closed. Management comments and associated actions addressed the recommendations 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. For the resolved recommendations, within 90 days please provide us documentation showing that the agreed-upon action has been completed. Your response should be sent as a PDF file to either [audcso@dodig.mil](mailto:audcso@dodig.mil) if unclassified or [REDACTED] if classified SECRET. Responses must have the actual signature of the authorizing official for your organization.

CUI

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

FOR THE INSPECTOR GENERAL:

A handwritten signature in black ink that reads "Carol N. Gorman". The signature is written in a cursive style with a long horizontal line extending from the end of the name.

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



## **(U) Contents**

---

### **(U) Introduction**

(U) Objective .....	1
(U) Background .....	1
(U) Review of Internal Controls .....	7

### **(U) Findings**

(U) Finding A. DoD Components Did Not Consistently Comply with DoD Authorization Requirements Before Deploying Collaboration Tools .....	9
(U) DoD Components Did Not Consistently Complete the Required Cybersecurity Reciprocity Steps .....	10
(U) DoD Components’ Deployment of Unauthorized Collaboration Tools Could Increase the Risk of Cyber Attacks .....	12
(U) Recommendations, Management Comments, and Our Response .....	13
(U) Finding B. DoD Components Did Not Ensure That All Critical Configuration Settings Were Implemented .....	17
(U) Configuration Settings Assessed .....	18
(U) DoD Components Did Not Consistently Implement Configuration Settings to Protect Collaboration Tools .....	19
(U) DoD Information Shared While Using Collaboration Tools Could Be Compromised by Cyber Attacks .....	24
(U) Recommendations, Management Comments, and Our Response .....	24
(U) Finding C. DoD Components Generally Implemented Cybersecurity Controls to Protect DoD Networks and Systems .....	27
(U) Cybersecurity Controls Assessed .....	27
(U) Unmitigated Vulnerabilities Could Increase the Risk of Cyber Attacks .....	30
(U) Recommendation, Management Comments, and Our Response .....	30

### **(U) Appendixes**

(U) Appendix A. Scope and Methodology .....	32
(U) Internal Control Assessment and Compliance .....	34
(U) Use of Computer-Processed Data .....	34
(U) Use of Technical Assistance .....	34
(U) Prior Coverage .....	34

## **(U) Contents (cont'd)**

---

(U) Appendix B. Sampling Approach.....	36
(U) Appendix C. House of Representatives, Committee on Oversight and Reform, Congressional Request Letter.....	37
(U) Appendix D. Enterprise and Alternative Collaboration Tools.....	41
<b>(U) Management Comments</b>	
(U) DoD Chief Information Officer.....	42
(U) Defense Finance and Accounting Service.....	43
(U) Defense Logistics Agency.....	45
(U) Defense Threat Reduction Agency.....	47
<b>(U) Acronyms and Abbreviations</b> .....	49
<b>(U) Glossary</b> .....	50

# (U) Introduction

---

## (U) Objective

(U) The objective of this audit was to determine whether the DoD's increased use of collaboration tools to facilitate telework during the coronavirus disease–2019 (COVID-19) pandemic exposed DoD networks and systems to potential malicious activity. We also determined the extent to which the DoD implemented configuration settings and security controls to protect DoD networks when using collaboration tools.

(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 collaboration tools and remote access software during the COVID-19 pandemic.<sup>1</sup> This report focuses on the DoD's use of collaboration tools and we will issue a separate report focusing on the DoD's use of remote access software.<sup>2</sup> See Appendix A for a discussion of the scope and methodology. Appendix B describes our detailed sampling approach for selecting the DoD Components we assessed for this audit. See Appendix C for a copy of the request letter from the House Committee on Oversight and Reform and the Glossary for the definitions of technical terms.

## (U) Background

(U) Collaboration tools include applications that allow employees to conduct meetings and work together virtually to perform tasks regardless of their physical location. Organizations use collaboration tools to boost productivity and connect users in different geographic locations. Examples of collaboration tool capabilities include the following.

- (U) Video conferencing, such as Zoom for Government, allows users in different locations to hold face-to-face meetings without gathering in person at a single location.
- (U) Instant messaging, such as Cisco Jabber, provides text-based communications that connect users in real-time conversation.
- (U) Online whiteboards, such as Microsoft Whiteboard, are web-based tools that act as an actual whiteboard that allows users to share text, graphs, and drawings.

---

<sup>1</sup> (U) On January 9, 2023, as part of the 118th Congress, the House Committee on Oversight and Reform was renamed to the House Committee on Oversight and Accountability.

<sup>2</sup> (U) DoD OIG Report No. DODIG-2023-057, "Audit of DoD Actions Taken to Implement Cybersecurity Protections Over Remote Access Software in the Coronavirus Disease–2019 Telework Environment," March 24, 2023.

- (U) Real-time information sharing, such as Microsoft Teams, allows users to review and edit documents simultaneously.

(U) DoD Components deploy collaboration tools directly on their network as an application or access the tools in a cloud-based environment. When a collaboration tool resides in a cloud-based environment, the users access the collaboration tool through the Internet while connected to the DoD Component's network. The DoD Component or an external vendor can own the cloud-based environment.<sup>3</sup> If an external vendor owns the cloud-based environment, the vendor is responsible for managing some security controls, such as data encryption and vulnerability management, although the DoD Component can maintain responsibility for other security controls, such as granting user access to the collaboration tool.

### ***(U) Collaboration Tools Approved for DoD Use***

(U) In April 2020, to support the increase in telework during the COVID-19 pandemic, the DoD Chief Information Officer (CIO) issued a memorandum directing DoD Components to use Defense Information Systems Agency (DISA)-provided enterprise collaboration tools, which included Commercial Virtual Remote, Defense Collaboration Services–Unclassified, and DoD Enterprise Portal Services.<sup>4</sup> The DoD CIO also authorized DoD Components to approve the use of 13 alternative collaboration tools if the enterprise tools did not fully meet the needs of DoD Components. See Appendix D for a list of the 13 alternative collaboration tools approved for use by the DoD CIO.

(U) The DoD CIO also acknowledged in his April 2020 memorandum that DoD Components might need capabilities not provided by the enterprise and 13 alternative collaboration tools and, as a result, established a process for DoD Components to submit other collaboration tools to the DoD CIO and U.S. Cyber Command for approval. In June 2021, DISA decommissioned Commercial Virtual Remote and Defense Collaboration Services–Unclassified but approved and encouraged the use of two other enterprise collaboration tools, Microsoft Teams and Cisco Jabber.

### ***(U) DoD Component Deployment of Collaboration Tools***

(U) DoD Components must conduct a risk assessment before deploying collaboration tools on their networks or in a vendor cloud-based environment. If risks are identified, the DoD Component must take steps to reduce those risks to an acceptable level. When a DoD Component deploys one of the DoD's enterprise collaboration tools, such as Microsoft Teams or Cisco Jabber, the DoD Component

<sup>3</sup> (U) For the purposes of this report, vendors are the cloud service providers who own their cloud-based environment.

<sup>4</sup> (U) DoD CIO memorandum, "Authorized Telework Capabilities and Guidance," April 13, 2020.

(U) is not required to conduct a separate risk assessment because DISA is responsible for assessing and mitigating the cybersecurity risks associated with using the enterprise tools.

(U) For the 13 alternative collaboration tools, DISA granted a provisional authorization to operate, meaning that the collaboration tools were assessed under the Federal Risk and Authorization Management Program (FedRAMP) and passed a security and compliance review based on National Institute of Standards and Technology (NIST) requirements.<sup>5</sup> During the security review, DISA assessed compliance with 17 NIST Special Publication (SP) 800-53 control families that include over 400 security controls related to, among other controls, access control, configuration management, vulnerability management, and incident response.<sup>6</sup>

(U) Because DISA only granted a provisional authorization to operate for the 13 alternative collaboration tools, the authorizing official (AO) for each DoD Component must still assess and authorize the use of the collaboration tool on their respective network before the DoD Component can deploy the tool. To reduce the time and resources necessary to assess and authorize collaboration tools that already have a provisional authorization to operate, DoD Components can accept and reuse another organization's (internal or external) security assessments to authorize information technology systems to operate on the DoD Information Network. DoD Instruction 8510.01 defines this process as cybersecurity reciprocity and it contains six steps that DoD Component AOs must follow.<sup>7</sup>

1. (U) Review the collaboration tool's security authorization package.
2. (U) Determine the security impact of allowing access to the collaboration tool through the Component's network.
3. (U) Determine the risk of using the collaboration tool within the network.
4. (U) Execute a documented agreement, such as a memorandum of understanding or service-level agreement with the vendor of the collaboration tool, for the maintenance and monitoring of the security posture of the system.
5. (U) Document the acceptance of any residual risk identified in Step 3.
6. (U) Include the collaboration tool in the DoD Component's authorization documentation.

<sup>5</sup> (U) FedRAMP provides a standardized approach to security authorizations for Cloud Service Offerings.

<sup>6</sup> (U) NIST SP 800-53, "Security and Privacy Controls For Federal Information Systems and Organizations," Revision 4, Updated January 22, 2015. NIST SP 800-53 was re-issued on December 10, 2020, however, FedRAMP uses the prior version for its moderate baseline.

<sup>7</sup> (U) DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology (IT)," March 12, 2014 (Incorporating Change 3, December 29, 2020). DoD Instruction 8510.01 was re-issued on July 19, 2022; however, we used the prior version that was in place during the audit.

(U) For collaboration tools that are neither enterprise tools nor one of the 13 alternative tools, the DoD Cloud Computing Security Requirements Guide (SRG) requires DoD Components to request that DISA assess the security of the tools before DoD Components can approve cloud-based tools. For noncloud-based tools, the DoD Component must follow DoD Instruction 8510.01 requirements to assess and authorize the collaboration tool to operate on DoD networks.<sup>8</sup>

(U) For cloud-based and noncloud-based collaboration tools purchased by members of the Intelligence Community (IC), Intelligence Community Directive (ICD) 503 directs members to use Committee on National Security Systems Instruction (CNSSI) 1253 requirements to assess and authorize collaboration tools, instead of following the DoD Instruction 8510.01 reciprocity steps.<sup>9</sup> Before deploying a collaboration tool on the IC network, ICD 503 requires IC members to conduct a security assessment of the tool and then authorize the tool to operate on its network.<sup>10</sup>

(U) For an overview of the DoD Component process for approving and using collaboration tools, see the following figure.

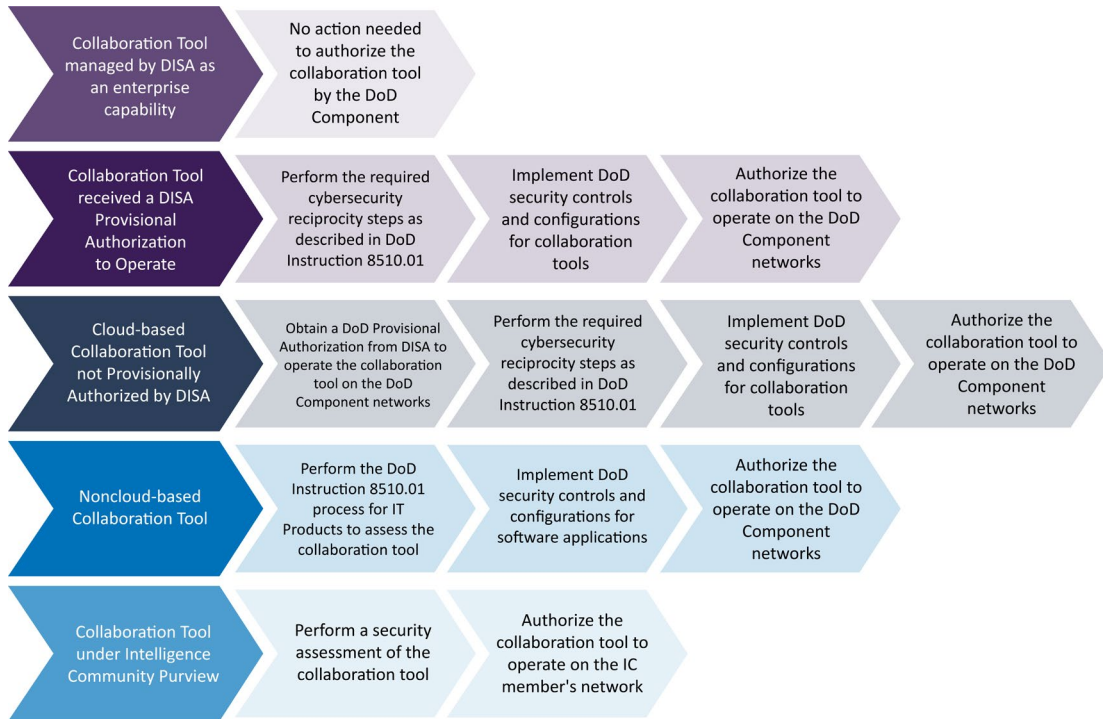
<sup>8</sup> (U) For noncloud-based tools, the DoD Component has direct control over the application and is within the organization's authorization boundary, which meets the definition of an IT product instead of an IT service. An IT product is individual hardware or software which can be commercial or government provided and include operating systems, office productivity software, firewalls, and routers.

<sup>9</sup> (U) Intelligence Community Directive 503 Technical Amendment, "Intelligence Community Information Technology Systems Security Risk Management, Certification, and Accreditation," July 21, 2015.

(U) Committee on National Security Systems Instruction 1253, "Security Categorization and Control Selection and Control Selection for National Security Systems," March 27, 2014.

<sup>10</sup> (U) As part of our audit, we included two IC members (National Security Agency and the National Geospatial-Intelligence Agency) in our assessment of cybersecurity controls and configuration settings.

(U) Figure. DoD Component Process for Approving and Using Collaboration Tools



(U) Source: The DoD OIG.

### (U) Requirements for Configuring Collaboration Tools

(U) Collaboration tools need additional protections because they often rely on networks and systems outside of the DoD’s control. Configuration management, a subset of cybersecurity controls, is the process of maintaining compliance with cybersecurity requirements on Information Technology (IT) hardware and software by implementing, 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 to affect the security posture and functionality of hardware and software. For example, system administrators can configure collaboration tools to enforce multifactor authentication for users accessing the collaboration tool.<sup>11</sup>

(U) Configuration requirements for collaboration tools vary, depending on which organization manages the tool and the sensitivity of the information shared using the tool. For cloud-based collaboration tools, DoD Components are responsible for working with the vendor to ensure that the collaboration tool is configured to meet DoD requirements. When sharing only unclassified, publicly releasable information on a cloud-based collaboration tool, the DoD Cloud Computing SRG requires

<sup>11</sup> (U) Multifactor authentication requires using something in a user’s possession, such as a token, in combination with something known only to the user, such as a personal identification number to access an information system or application.

(U) DoD Components work with the vendor to implement the FedRAMP Moderate Baseline as the minimum configuration requirement. The FedRAMP Moderate Baseline includes more than 300 controls and configuration settings based on NIST SP 800-53 controls, including multifactor authentication for privileged users, minimum password lengths, and limiting unsuccessful logon attempts.

(U) For cloud-based collaboration tools authorized to share sensitive information, such as controlled unclassified information, the DoD Cloud Computing SRG requires DoD Components to work with the vendor to implement up to 47 additional NIST SP 800-53 controls. The additional controls are referred to as FedRAMP Plus, and include additional monitoring of privileged users' activity and automated mechanisms to alert security personnel of inappropriate or unusual activities, to protect the information shared using the collaboration tool.

(U) For noncloud-based collaboration tools, DoD Components are responsible for configuring the tool regardless of the sensitivity of the information. DoD Instruction 8500.01, "Cybersecurity," directs Components to configure the tools in accordance with the DISA Application Security and Development Security Technical Implementation Guide (STIG).<sup>12</sup> Furthermore, for cloud-based or noncloud-based collaboration tools authorized by DoD Components that are members of the IC, ICD 503 requires Components to apply configuration settings from the Committee on National Security Systems, such as CNSSI 1253.

(U) Table 1 lists the different collaboration tool deployment methods and the respective configuration requirements.

(U) Table 1. Collaboration Tool Deployment Method and Configuration Requirement

(U) Collaboration Tool Deployment Method	Sensitivity of Information Shared	Configuration Requirement
Cloud-based	Publicly Releasable	FedRAMP Moderate Baseline
Cloud-based	Controlled Unclassified Information	FedRAMP Plus
Noncloud-based	Publicly Releasable or Controlled Unclassified Information	DISA Application Security and Development STIG
Collaboration tools deployed by a member of the IC	Publicly Releasable or Controlled Unclassified Information	CNSSI 1253

(U) Source: The DoD OIG.

<sup>12</sup> (U) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014 (Incorporating Change 1, October 7, 2019).



**(U) DoD Components and Collaboration Tools Assessed**

(U) We assessed nine DoD Components that used collaboration tools to determine whether the DoD’s use of collaboration tools increased the risk of exposure of DoD networks and systems to potential malicious activity. Additionally, we assessed whether the DoD Components implemented the cybersecurity controls and configuration settings required to mitigate the risks associated with using collaboration tools on DoD networks. Table 2 lists the nine DoD Components and corresponding collaboration tools we assessed.

*(U) Table 2. DoD Components Visited and the Collaboration Tools Assessed*

<b>(U)</b> DoD Component	Collaboration Tool Used	Deployment Method
DISA	Microsoft Teams	Cloud
DISA	Cisco Jabber	Noncloud
Defense Advanced Research Projects Agency	Zoom for Government	Cloud
Defense Finance and Accounting Service	Adobe Connect	Cloud
Defense Threat Reduction Agency	Zoom for Government	Cloud
Defense Counterintelligence and Security Agency	Cisco Webex	Cloud
Defense Logistics Agency	Zoom for Government	Cloud
U.S. Army Cyber Command	Zoom for Government	Cloud
National Geospatial-Intelligence Agency	Rocket Chat Unclassified Cloud	Cloud
National Security Agency	Collaboration Development Environment	Cloud <b>(U)</b>

(U) Source: The DoD OIG.

**(U) Review of Internal Controls**

(U) DoD Instruction 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. We identified internal control weaknesses related to the authorization of collaboration tools for use on DoD networks and the implementation of cybersecurity controls to protect DoD networks and systems from malicious

(U) activity when using collaboration tools. We will provide a copy of the final report to the senior official responsible for internal controls in the DoD Office of the CIO, U.S. Army Cyber Command (ARCYBER), Defense Finance and Accounting Service (DFAS), Defense Logistics Agency (DLA), Defense Threat Reduction Agency (DTRA), and National Geospatial-Intelligence Agency (NGA).

## (U) Finding A

### (U) DoD Components Did Not Consistently Comply with DoD Authorization Requirements Before Deploying Collaboration Tools

(U) DoD Components did not consistently comply with DoD requirements before deploying collaboration tools on their networks. Of the nine DoD Components that we reviewed, AOs at four DoD Components (ARCYBER, DFAS, DLA, and DTRA) did not complete all six required reciprocity steps outlined in DoD Instruction 8510.01 before deploying one of the 13 alternate collaboration tools on their networks. Specifically, for the one tool assessed at each DoD Component, the AOs at:

- (U) ARCYBER and DFAS did not review security authorization packages for their collaboration tools (Step 1);
- (U) ARCYBER, DFAS, and DLA did not identify the security impacts of using their collaboration tools (Step 2);
- (U) ARCYBER, DFAS, and DLA did not identify the risks associated with using their collaboration tools (Step 3);
- (U) ARCYBER, DFAS, DLA, and DTRA did not document the acceptance of the security impacts and risks (Step 5); and
- (U) ARCYBER, DFAS, DLA, and DTRA did not update the Component's authorization documentation to include their collaboration tools (Step 6).<sup>13</sup>

(U) The DoD Component AOs did not complete some of the required reciprocity steps because they incorrectly believed that, since the collaboration tools were assessed and authorized by FedRAMP and had received a provisional authorization to operate from DISA, they did not need to fully complete the reciprocity steps to authorize the tools for use on their individual networks. However, completing all of the required reciprocity steps demonstrates that a DoD Component exercised due diligence to protect an IT system from incidents such as cyber attacks, security breaches, malware, and phishing attempts. By not completing all of the required reciprocity steps for properly authorizing collaboration tools, DoD Components unnecessarily increased the risk that malicious cyber actors could exploit undetected security weaknesses to gain unauthorized access to DoD networks and systems that are critical to national security.

<sup>13</sup> (U) We did not identify any issues with DoD Components executing documented agreements with the vendors for the maintenance and monitoring of the collaboration tool (Step 4).

## (U) DoD Components Did Not Consistently Complete the Required Cybersecurity Reciprocity Steps

(U) The AOs for five of the nine DoD Components we assessed (DISA, the Defense Counterintelligence and Security Agency, the Defense Advanced Research Projects Agency, the NGA, and the National Security Agency) completed the assessment and authorization steps required by DoD Instruction 8510.01 or ICD 503 before deploying collaboration tools on their Component networks. However, the AOs for the other four DoD Components (ARCYBER, DFAS, the DLA, and DTRA) did not complete all of the required reciprocity steps outlined in DoD Instruction 8510.01. To determine whether the DoD Components complied with DoD requirements before operating collaboration tools on their networks, we interviewed project managers and IT personnel and analyzed authorization documentation.

### (U) DoD Components Did Not Complete All of the Required Cybersecurity Reciprocity Steps

(U) The AOs for ARCYBER, DFAS, the DLA, and DTRA did not complete the six required cybersecurity reciprocity steps. All four of the DoD Components used cloud-based collaboration tools approved for use in the DoD CIO memorandum and provisionally authorized by DISA and, therefore, should have completed the six required cybersecurity reciprocity steps identified in DoD Instruction 8510.01 before deploying the collaboration tool on their network. Table 3 identifies the steps taken and not taken by DoD Component.

(U) Table 3. Cybersecurity Reciprocity Steps Completed by DoD Components When Assessing and Authorizing Collaboration Tools

(U) DoD Instruction 8510.01 Cybersecurity Reciprocity Steps	ARCYBER	DFAS	DLA	DTRA
Step 1: Review Security Authorization Package	No	No	Yes	Yes
Step 2: Identify Security Impact of Using the Tool	No	No	No	Yes
Step 3: Identify Risk of Using the Tool	No	No	No	Yes
Step 5: AO Acceptance of the Tool	No	No	No	No
Step 6: Update Component Authorization Package	No	No	No	No (U)

(U) Source: The DoD OIG.

(U) The AOs for ARCYBER and DFAS did not review the security authorization package (Step 1) for Zoom for Government or Adobe Connect, respectively. In addition, the AOs for ARCYBER, DFAS, and the DLA did not identify the security impact (Step 2) or risk of using Zoom for Government and Adobe Connect (Step 3). Reviewing the security authorization package is important because it allows DoD Component AOs to understand the security mechanisms in place to protect information shared using the collaboration tool and the risks that the organization will inherit when using the tool. DoD Component AOs are then required to review these risks to identify any security impact or risks to DoD information if the collaboration tool is used and determine whether the risks are acceptable.

(U) Furthermore, the AOs for ARCYBER, DFAS, the DLA, and DTRA did not formally accept the risk of using the tool (Step 5) or update the authorization package (Step 6). If the AO believes the risk is acceptable, the AO should document the acceptance and update the Component authorization package. Completing the required reciprocity steps is important to ensure that collaboration tool security weaknesses are addressed and will not put DoD information at additional risk.

***(U) DoD Components Did Not Believe an Authorization to Operate was Required for Provisionally Authorized Collaboration Tools***

(U) The AOs for ARCYBER, DFAS, the DLA, and DTRA did not complete some of the required reciprocity steps because they incorrectly believed that, since the collaboration tools were assessed and authorized by FedRAMP and had received a provisional authorization to operate from DISA, they did not need to fully complete the reciprocity steps to authorize the tools for use on their individual networks.

For example, the DLA Cybersecurity Operations Engineer stated that they believed that DISA had already performed the required reciprocity steps by issuing the provisional authorization and that they did not need to perform any additional steps. However, the DISA provisional authorization to operate is clear that it does not replace or eliminate the requirement for DoD Components to

*... (U) However, the DISA provisional authorization to operate is clear that it does not replace or eliminate the requirement for DoD Components to separately assess and authorize the tool to operate on their individual networks.*

separately assess and authorize the tool to operate on their individual networks. Therefore, the AO for the DLA should immediately identify the security impact and risks of using Zoom for Government and, if the risk is determined acceptable, formally accept the risk of using the tool and update the authorization package.

(U) In addition, the AOs for ARCYBER and DFAS should immediately review the security authorization package, identify the security impact and risks, and if the risk is determined acceptable, formally accept the risk of using the tool and update the authorization package for Adobe Connect and Zoom for Government, respectively. Furthermore, the AO for DTRA should review the Zoom for Government package and, if the risk is determined acceptable, formally accept the risk of using the tool and update the authorization package.

(U) Since we identified four DoD Components that did not obtain an authority to operate as required by the DoD CIO guidance, we believe this could be a systemic issue for other DoD Components we did not review. Therefore, the DoD CIO should issue clarifying instructions or guidance that states that deploying a collaboration tool with a provisional authorization does not eliminate the need to perform the required cybersecurity reciprocity process. In addition, the DoD CIO should direct DoD Components' AOs to identify collaboration tools in use, verify that the required reciprocity process was completed for each, and, if the process was not completed, direct the Component AOs to complete the process.

### **(U) DoD Components' Deployment of Unauthorized Collaboration Tools Could Increase the Risk of Cyber Attacks**

(U) According to the Cybersecurity and Infrastructure Security Agency, the COVID-19 pandemic has resulted in a significant increase in teleworking since March 2020, which could increase attacks from malicious cyber actors. Deploying unauthorized collaboration tools introduces potential weaknesses that malicious cyber actors could exploit to gain unauthorized access to a network. DoD Components that do not perform the required cybersecurity reciprocity steps before deploying collaboration tools on their networks, increase the risk that security weaknesses within the collaboration tool will not be detected. Finding B details the cybersecurity weaknesses that exist when DoD Components do not perform the required cybersecurity reciprocity steps before deploying collaboration tools on their networks. Undetected security weaknesses on DoD networks could be exploited by malicious cyber actors to threaten DoD information.

## **(U) Recommendations, Management Comments, and Our Response**

### **(U) Recommendation A.1**

**(U) We recommend that the DoD Chief Information Officer:**

- a. **(U) Issue guidance that states that deploying a collaboration tool with a provisional authorization does not eliminate the need to perform the required cybersecurity reciprocity process.**

### ***(U) Department of Defense Chief Information Officer Comments***

(U) The DoD CIO agreed, stating that they will reinforce existing policy to leverage collaboration tools with existing provisional authorizations, as outlined in the “Authorized Telework Capabilities and Guidance” and “Authorizations to Operate Extensions and Cybersecurity Function Prioritization Guidance” memorandums, both issued by the DoD CIO in April 2020.

### ***(U) Our Response***

(U) Comments from the DoD CIO partially addressed the recommendation; therefore, the recommendation is unresolved. Although the DoD CIO stated that they would reinforce the April 2020 memorandums, the DoD CIO did not indicate whether they would issue new guidance or update the April 2020 memorandums to emphasize that deploying a collaboration tool with a provisional authorization does not eliminate the need to perform the required cybersecurity reciprocity process.

(U) Without additional guidance, DoD Components deploying collaboration tools on their networks may not identify security weaknesses associated with the tool, increasing the risk of unauthorized access to DoD networks and information. Therefore, we request that within 30 days the DoD CIO provide additional comments to the final report clarifying whether they will issue new guidance or update the April 2020 memorandums to reinforce the requirement to perform the cybersecurity reciprocity process to authorize collaboration tools.

- b. **(U) Direct DoD Components’ Authorizing Officials to identify collaboration tools in use, verify that the required reciprocity process was completed for each, and, if the process was not completed, direct the DoD Component Authorizing Officials to complete the reciprocity process.**

### ***(U) Department of Defense Chief Information Officer Comments***

(U) The DoD CIO agreed, stating that they will require DoD Components to identify collaboration tools in use and verify that those tools were authorized in accordance with DoD Instruction 8510.01 and the April 13, 2020, memorandum.

### ***(U) Our Response***

(U) Comments from the DoD CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the DoD CIO provides supporting documentation, such as a memorandum showing that the DoD CIO directed DoD Components to identify collaboration tools in use, and verify that the required reciprocity process was completed for each collaboration tool.

### ***(U) Recommendation A.2***

**(U) We recommend that the Authorizing Official for the Defense Finance and Accounting Service review the security authorization package for Adobe Connect, identify the security impact and risks and, if the risk is determined acceptable, formally accept the risk of using the tool, and update the authorization package.**

### ***(U) Defense Finance and Accounting Service Acting Director for Information and Technology Comments***

(U) The DFAS Acting Director for Information and Technology, responding for the DFAS AO, agreed, stating that DFAS completed an authorization package for Adobe Connect on March 27, 2023.

### ***(U) Our Response***

(U) Comments from the Acting Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Acting Director provides the authorization package for Adobe Connect, along with supporting documentation showing that DFAS reviewed the security authorization package, identified the security impact and risks, and if determined acceptable, formally accepted the risk of using Adobe Connect.



### ***(U) Recommendation A.3***

**(U) We recommend that the Authorizing Official for the Defense Logistics Agency identify the security impact and risks of using Zoom for Government and, if the risk is determined acceptable, formally accept the risk of using the tool, and update the authorization package.**

#### ***(U) Defense Logistics Agency Acting Chief Information Officer Comments***

(U) The DLA Acting CIO, responding for the AO, agreed, stating that the DLA authorized Zoom for Government Impact Level 4 to operate until March 2026.<sup>14</sup> The Acting CIO stated that the DLA Security Control Assessor reviewed the Zoom for Government Risk Management Framework request and determined that the security categorization of the tool is Moderate, Moderate, and Low.<sup>15</sup> The Acting CIO also stated that the identified risks presented a very low residual risk to the DLA and the DoD.<sup>16</sup>

#### ***(U) Our Response***

(U) Comments from the Acting CIO addressed the specifics of the recommendation. We reviewed the DLA's authorization documentation and verified that the DLA identified the security impact and risks of using Zoom for Government, authorized the tool for use, and updated the authorization package to document the identified risks. Therefore, the recommendation is closed.

### ***(U) Recommendation A.4***

**(U) We recommend that the Authorizing Official for the Defense Threat Reduction Agency review the Zoom for Government package and, if the risk is determined acceptable, formally accept the risk of using Zoom for Government and update the authorization package.**

<sup>14</sup> (U) Zoom for Government Impact Level 4 accommodates controlled unclassified information, including data used in direct support of military and contingency operations.

<sup>15</sup> (U) Security categorization applied to information systems refers to the potential impact values for security objectives: confidentiality, integrity, and availability. For Zoom for Government Impact Level 4, DLA determined that the potential impact was Moderate for confidentiality, Moderate for integrity, and Low for Availability. A moderate potential impact for confidentiality means that the disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A moderate potential impact for integrity means that the unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A low potential impact for availability means that the disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

<sup>16</sup> (U) Residual risk is the portion of risk remaining after security measures have been applied.

### ***(U) Defense Threat Reduction Agency, Authorizing Official Comments***

(U) The DTRA AO agreed, stating that they reviewed the Zoom for Government package, and formally accepted the security impacts and risks of using Zoom for Government. The AO also stated that DTRA updated its unclassified network authorization package to include Zoom for Government.

### ***(U) Our Response***

(U) Comments from the AO addressed the specifics of the recommendation. We reviewed the authorization to operate for the DTRA unclassified networks and verified that the AO accepted the risk of using Zoom for Government, and updated the authorization package. Therefore, the recommendation is closed.

### ***(U) Recommendation A.5***

**(U) We recommend that the Authorizing Official for the U.S. Army Cyber Command review the security authorization package for Zoom for Government, identify the security impact and risks and, if the risk is determined acceptable, formally accept the risk of using the tool, and update the authorization package.**

### ***(U) Management Comments Required***

(U) The ARCYBER AO did not respond to the recommendation and it remains unresolved. Therefore, we request that within 30 days the AO provide comments to the final report.

## (U) Finding B

### (U) DoD Components Did Not Ensure That All Critical Configuration Settings Were Implemented

(U) Network and system administrators did not consistently implement critical collaboration tool configuration settings before deploying collaboration tools. Of the nine DoD Components we assessed, five DoD Components implemented the required configuration settings that we considered critical to protecting collaboration tools from malicious activity and the other four DoD Components did not. Specifically, network and system administrators at:

- (U) the DLA, DFAS, and DTRA did not configure Adobe Connect or Zoom for Government to require privileged users to log on using multifactor authentication or enforce strong passwords for nonprivileged users;
- (U) DFAS and DTRA did not configure Adobe Connect or Zoom for Government, respectively, to lock user accounts after three unsuccessful attempts to log into the collaboration tool; and
- (U) the NGA did not configure Rocket Chat Unclassified Cloud to disable or remove user accounts after 35 days of inactivity.

(U) The configuration settings were not fully implemented because network and system administrators incorrectly believed that, because the collaboration tools were assessed and authorized by FedRAMP and received a DISA provisional authorization, the configuration settings for these tools aligned with the minimum DoD security requirements. In addition, DFAS system administrators did not renegotiate changes with the vendor, as required by DoDI 8510.01, to configure Adobe Connect to meet DoD security requirements because the DFAS Director for IT Enterprise Services believed DISA was responsible for configuring Adobe Connect.

(U) Configuring devices and applications to a security standard is done to reduce unnecessary cyber vulnerabilities. If DoD Components do not consistently configure collaboration tools in accordance with DoD and FedRAMP requirements, malicious cyber actors could exploit vulnerable configuration settings and compromise the confidentiality, integrity, and availability of information shared using collaboration tools.

## (U) Configuration Settings Assessed

(U) To determine whether DoD Components configured collaboration tools to protect DoD networks from potential malicious activities, we assessed selected configuration settings that we considered critical to protecting DoD networks and systems. Table 4 identifies the configuration setting categories we assessed, their importance, and the corresponding configuration setting.

(U) Table 4. Assessed Configuration Settings and Their Importance

(U) Configuration Setting Category	Importance When Configuring Collaboration Tools	Corresponding Configuration Settings
Multifactor Authentication	Authentication mechanisms verify user identities, processes, or devices as a prerequisite to allowing access to collaboration tools. Multifactor authentication requires the use of two or more different factors for the system to allow the user access. 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.	Privileged users must use multifactor authentication to access the application.
Minimum Password Length	Password length is the primary factor in determining password strength. Passwords that are too short are easily guessed by brute-force password attacks or dictionary attacks using words and common passwords.	For cloud-based tools assessed, passwords must be a minimum of 12 characters.  For noncloud-based tools assessed, passwords must be a minimum of 15 characters.
Password Complexity	Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. The use of a complex password helps increase the time and resources required to compromise the password.	Passwords must include 1 numeric, 1 uppercase, 1 lowercase, and 1 special character.
Unsuccessful Logon Attempts	Locking user accounts after consecutive failed logon attempts prevents unauthorized individuals from gaining access to collaboration tools.	User accounts must be locked after 3 consecutive invalid logon attempts during a 15 minute period. (U)

(U) Table 4. Assessed Configuration Settings and Their Importance (cont'd)

(U) Configuration Setting Category	Importance When Configuring Collaboration Tools	Corresponding Configuration Settings
Inactive User Accounts	Disabling inactive user accounts for collaboration tools reduces the risk that accounts will be hijacked. Outdated or unused accounts provide penetration points that may go undetected and be exploited by malicious cyber actors to gain unauthorized access to sensitive DoD information. A malicious cyber actor is an individual that uses technology with the intent to cause harm.	For cloud-based tools assessed, inactive user accounts must be disabled after 90 days of inactivity.  For noncloud-based tools assessed, inactive user accounts must be disabled after 35 days of inactivity.
Inactive User Sessions	Terminating inactive user sessions prevents access to collaboration tools when users stop work and move away from the immediate vicinity of those devices but do not want to log out because of the temporary nature of their absences. If the user session is compromised, DoD information shared within the collaboration tool can be extracted.	User accounts must be terminated after 15 minutes of inactivity.
Encryption	Encryption protects the confidentiality and integrity of DoD data shared using collaboration tools. DoD Components can protect the confidentiality of DoD data in transit by using encryption. Data in transit refers to the state of information when it is in process or in transit between devices such as hard drives and workstations.	Data shared using collaboration tools must be protected by Federal Information Processing Standards-validated encryption.*  <b>(U)</b>

(U) Note: Requirements as stated in the FedRAMP Moderate Baseline, FedRAMP Plus, DISA STIG, and CNSSI 1253 standards.

(U) \* Federal Information Processing Standards (FIPS) is a Federal standard designed to achieve a common level of quality or some level of interoperability in IT, such as encryption devices, used with the Federal Government.

(U) Source: The DoD OIG.

## (U) DoD Components Did Not Consistently Implement Configuration Settings to Protect Collaboration Tools

(U) Network and system administrators did not consistently implement all critical configuration settings before the DoD Components deployed collaboration tools on their networks. Specifically, we identified configuration settings weaknesses at DFAS, the DLA, DTRA, and NGA. We did not identify configuration setting weaknesses at ARCYBER, the Defense Advanced Research Projects Agency, the

(U) Defense Counterintelligence and Security Agency, DISA, or the National Security Agency. To determine whether DoD Components configured collaboration tools to protect DoD networks and systems from potential malicious activity, we assessed DoD Components' configuration settings for compliance with the applicable DoD requirements, IC requirements, and the FedRAMP Moderate Baseline. Table 5 lists the configuration settings that we determined did not meet DoD requirements identified by DoD Component.

(U) Table 5. Configuration Settings Identified at DoD Components that Did Not Meet DoD Requirements

(U) Configuration Setting	DoD Components			
	DFAS	DLA	DTRA	NGA
Enforced Multifactor Authentication for Privileged Users	No	No	No	Yes
Required Minimum Password Length	Yes	No	No	Yes
Limited Unsuccessful Logon Attempts Appropriately	No	Yes	No	Yes
Disabled Inactive User Accounts in a Timely Manner	Yes	Yes	Yes	No (U)

(U) Source: The DoD OIG.

### **(U) DFAS, the DLA, and DTRA Did Not Enforce the Use of Multifactor Authentication or Strong Passwords**

(U) DFAS, the DLA, and DTRA system administrators did not configure Zoom for Government and Adobe Connect to enforce the use of multifactor authentication for privileged users or passwords with a minimum of 12 characters for nonprivileged users.<sup>17</sup> The DoD Cloud Computing SRG directs DoD Components to comply with the FedRAMP Moderate Baseline, which requires DoD Components to enforce multifactor authentication for privileged users and implement a minimum of 12 characters for nonprivileged user passwords. Privileged users are required to use multifactor authentication because they perform security-related functions that nonprivileged users are not authorized to perform. For example, privileged users can create or delete accounts and configure security settings such as password length and complexity.

<sup>17</sup> (U) A privileged user is an individual that is authorized (trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

(U) DFAS system administrators did not configure Adobe Connect to enforce the use of multifactor authentication for privileged users because the DFAS Chief for IT Security Services did not believe that DFAS had privileged users. Instead, the Chief stated that DFAS had two “super users” that performed security-related duties, such as creating accounts and changing password settings for all DFAS users. According to the NIST Glossary, a privileged user is an individual that is authorized (and therefore trusted) to perform security-relevant functions that ordinary users are not authorized to perform. By definition, the DFAS description of “super users” aligns with the duties of a privileged user. DFAS system administrators did not have the ability to directly configure the collaboration tool because the cloud vendor controlled Adobe Connect’s configuration settings. Therefore, the CIO for DFAS should renegotiate changes with the Adobe Connect vendor to configure Adobe Connect to require privileged users to authenticate into the collaboration tool using multifactor authentication.

(U) Although the DLA IT Program Manager recognized the need to implement multifactor authentication for privileged users, he stated during our site visit in April 2022 that DLA was waiting for a software update from Zoom that would enable him to do so. However, according to the March 2022 Zoom for Government System Security Plan, the software update was already available. In August 2022, after our April virtual site visit, we notified the DLA IT Program Manager that the update was available, and the DLA took action to implement multifactor authentication for privileged users that same month. Therefore, we did not include a recommendation to the DLA CIO on implementing multifactor authentication for privileged users in this report.

(U) The DTRA Chief of the Information Management and Technology Directorate did not believe that multifactor authentication for privileged users was a requirement for Zoom for Government if DTRA only shared publicly releasable information using the tool. However, the FedRAMP Moderate Baseline does not limit the need for multifactor authentication based on the sensitivity of the information shared, and states that multifactor authentication is required for sharing any type of information using the tool. Therefore, the CIO for DTRA should configure Zoom for Government to require privileged users to authenticate into the collaboration tool using multifactor authentication.

(U) DLA and DTRA system administrators improperly retained the eight-character length for passwords that was preset in Zoom for Government instead of requiring the minimum 12-character length. The system administrators stated that they mistakenly assumed that the tool came pre-configured to meet the FedRAMP Moderate Baseline password requirements. However, password lengths shorter than 12 characters make DLA and DTRA’s collaboration tools more susceptible

(U) to password attacks, such as brute-force and dictionary attacks.<sup>18</sup> Therefore, the CIOs for the DLA and DTRA should configure Zoom for Government to require a minimum of 12 characters for password logon for non-privileged users.

(U) According to the Cybersecurity and Infrastructure Security Agency, passwords are one of the most vulnerable cyber defenses, and organizations can improve password security by enforcing longer passwords.<sup>19</sup> NIST SP 800-63B, “Digital Identity Guidelines: Authentication and Lifecycle Management,” explains how passwords that are too short are easily guessed by brute-force password attacks, as well as dictionary attacks using words and common passwords.<sup>20</sup> There are several password-cracking tools that malicious cyber actors can use to guess passwords; choosing strong passwords can make it more difficult to guess a password using this type of software. If a privileged user account is compromised, a malicious cyber actor can impersonate users with administrative privileges to gain unauthorized access, circumvent security controls, and compromise the integrity of the collaboration tool to extract DoD information or perform other malicious activities.

### ***(U) DFAS and DTRA Automatic Account Lock Did Not Meet DoD Requirements***

(U) DFAS and DTRA system administrators did not configure Adobe Connect and Zoom for Government, respectively, to lock user accounts after three unsuccessful logon attempts. The DoD Cloud Computing SRG directs DoD Components to comply with the FedRAMP Moderate Baseline, which requires DoD Components to automatically lock user accounts after three unsuccessful logon attempts in a 15-minute period. Instead, DFAS and DTRA system administrators did not change the default configuration of Adobe Connect and Zoom for Government to automatically lock user accounts after five and six unsuccessful logon attempts, respectively.

(U) DFAS and DTRA system administrators did not renegotiate their contract with the vendor or directly configure their collaboration tools to meet DoD requirements because the system administrators believed that the collaboration tools would be properly configured by the vendor, since DISA issued a provisional authorization for Adobe Connect and Zoom for Government. As a result of this assumption, DFAS and DTRA system administrators did not assess the collaboration tools’ configuration settings or validate that the settings met DoD requirements.

<sup>18</sup> (U) Brute-force password attacks are a method to gain access to a device by attempting multiple combinations of passwords.

<sup>19</sup> (U) Cybersecurity and Infrastructure Security Agency Security Tip ST04-003, “Good Security Habits,” February 1, 2021.

<sup>20</sup> (U) NIST SP 800-63B, “Digital Identity Guidelines: Authentication and Lifecycle Management,” June 2017.



(U) Vendor default configurations generally do not meet DoD requirements, and the collaboration tool should be properly configured before using the tool to process DoD information. DTRA system administrators had the ability to configure Zoom for Government; however, DFAS system administrators did not because the cloud vendor controlled Adobe Connect’s configuration settings.

(U) According to DoD Instruction 8510.01, DoD Components should renegotiate with the vendor to make configuration changes to the collaboration tool settings to meet DoD security requirements. Accepting the default settings without reviewing them increases the risk that malicious cyber actors could exploit weak configuration settings to gain unauthorized access and compromise the integrity of the collaboration tool to extract DoD information. Therefore, the CIO for DFAS should renegotiate changes with the Adobe Connect vendor to configure Adobe Connect to lock user accounts after three unsuccessful logon attempts in a 15-minute period. In addition, the CIO for DTRA should configure Zoom for Government to lock user accounts after three unsuccessful logon attempts in a 15-minute period.

***(U) NGA Did Not Disable User Accounts After 35 Days of Inactivity***

~~(CUI)~~ NGA system administrators did not configure Rocket Chat Unclassified Cloud to disable user accounts after 35 days of inactivity. The NGA Information Assurance Requirements Catalog, which is the NGA’s implementation guide for configurations and controls from CNSSI 1253, requires user accounts be disabled after 35 days of inactivity. According to the NGA Information Systems Security Officer, Rocket Chat Unclassified Cloud does not include a feature that allows the NGA to disable user accounts. To compensate for the absent security feature, the NGA relied on the security controls implemented on its Active Directory, which NGA system administrators configured to disable user accounts across all NGA systems after 60 days of inactivity. [REDACTED]

[REDACTED]

[REDACTED]<sup>21</sup> [REDACTED]

[REDACTED]. Therefore, we did not include a recommendation to the NGA Delegated AO on disabling inactive user accounts in this report.

<sup>21</sup> (U) A delegated AO is an individual who is assigned the functions, responsibilities, and authority of an AO.

## (U) DoD Information Shared While Using Collaboration Tools Could Be Compromised by Cyber Attacks

*(U) DoD Components that do not consistently configure collaboration tools in accordance with SRG, STIG, IC, and FedRAMP requirements increase the risk of unauthorized access to DoD information.*

that do not consistently configure collaboration tools in accordance with SRG, STIG, IC, and FedRAMP requirements increase the risk of unauthorized access to DoD information.

(U) The increased sophistication of malicious cyber actors requires Federal Departments and agencies to maintain and protect the integrity of their IT systems, particularly if they adopt more flexible telework policies after the COVID-19 pandemic subsides. As the DoD workforce continues to use collaboration tools to facilitate telework, DoD Components should implement basic configuration settings required to protect DoD networks and systems from potential malicious activity.

(U) According to Executive Order 14028, “Improving the Nation’s Cybersecurity,” the United States faces persistent and increasingly sophisticated malicious cyber attacks.<sup>22</sup> The use of potentially vulnerable services, such as collaboration tools, amplifies the threat to individuals and organizations in a maximum telework environment. DoD Components

## (U) Recommendations, Management Comments, and Our Response

### (U) Recommendation B.1

**(U) We recommend that the Chief Information Officer for the Defense Finance and Accounting Service renegotiate changes with the Adobe Connect vendor to configure Adobe Connect to:**

- a. **(U) Require privileged users to authenticate into the collaboration tool using multifactor authentication.**
- b. **(U) Lock user accounts after three unsuccessful logon attempts in a 15-minute period.**

<sup>22</sup> (U) Executive Order 14028, “Improving the Nation’s Cybersecurity,” May 12, 2021.

### ***(U) Defense Finance and Accounting Service Acting Director for Information and Technology Comments***

(U) The DFAS Acting Director for Information and Technology, responding for the DFAS CIO, agreed, stating that they plan to use the Global Federated User Domain to implement common access card authentication for privileged users by September 15, 2023.<sup>23</sup> In addition, the Acting Director stated that DFAS is working with the Adobe Connect vendor to configure the tool by April 28, 2023, to lock user accounts after three unsuccessful logon attempts in a 15-minute period.

### ***(U) Our Response***

(U) Comments from the Acting Director addressed the specifics of the recommendations; therefore, the recommendations are resolved but open. We will close the recommendations once the Acting Director provides supporting documentation showing that DFAS implemented multifactor authentication for privileged users and locked user accounts after three unsuccessful logon attempts.

### ***(U) Recommendation B.2***

**(U) We recommend that the Chief Information Officer for the Defense Logistics Agency configure Zoom for Government to require a minimum of 12 characters for password logon for non-privileged users.**

### ***(U) Defense Logistics Agency Acting Chief Information Officer Comments***

(U) The DLA Acting CIO agreed, stating that on March 13, 2023, the DLA configured Zoom for Government to require all passwords be a minimum of 12 characters.

### ***(U) Our Response***

(U) Comments from the Acting CIO addressed the specifics of the recommendation. We verified through screenshots of the Zoom for Government configuration settings, that the DLA configured the tool to require users to enter a minimum of 12 characters for password logon for non-privileged users. Therefore, the recommendation is closed.

---

<sup>23</sup> (U) The Global Federated User Domain is a DISA provided system used to authenticate privileged users to Cloud-based systems and services.

### ***(U) Recommendation B.3***

**(U) We recommend that the Chief Information Officer for the Defense Threat Reduction Agency configure Zoom for Government to:**

- a. **(U) Require privileged users to authenticate into the collaboration tool using multifactor authentication.**
- b. **(U) Require a minimum of 12 characters for password logon for non-privileged users.**

### ***(U) Defense Threat Reduction Agency, Chief Information Officer Comments***

(U) The DTRA CIO agreed, stating that they ensured Zoom for Government was configured to require multifactor authentication for privileged users, and required a minimum of 12 characters for password logon for non-privileged users.

### ***(U) Our Response***

(U) Comments from the CIO addressed the specifics of the recommendations. We verified, through screenshots of the Zoom for Government configuration settings, that DTRA configured the tool to require multifactor authentication for privileged users, and the users must enter a minimum of 12 characters for password logon for non-privileged users. Therefore, the recommendations are closed.

- c. **(U) Lock user accounts after three unsuccessful logon attempts in a 15-minute period.**

### ***(U) Defense Threat Reduction Agency, Chief Information Officer Comments***

(U) The DTRA CIO agreed, stating that DTRA is working with the Zoom for Government vendor to configure the tool to lock user accounts after three unsuccessful logon attempts in a 15-minute period by October 2023.

### ***(U) Our Response***

(U) Comments from the CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the CIO provides documentation such as a screenshot, showing that Zoom for Government was configured to lock user accounts after three unsuccessful logon attempts in a 15-minute period.

## (U) Finding C

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

~~(CUI)~~ Network administrators for the nine DoD Components we assessed generally implemented cybersecurity controls to protect collaboration tools. Specifically, of the nine DoD Components assessed, eight implemented all of the cybersecurity controls that we considered critical to protect collaboration tools used on DoD networks. The remaining DoD Component, the DLA, implemented three of the four controls we assessed. However, DLA network administrators did not mitigate known high vulnerabilities in accordance with DoD vulnerability management requirements or develop plans of action and milestones (POA&Ms) for vulnerabilities that could not be mitigated. According to the DLA IT Program Manager, not including the vulnerability on a POA&M was an oversight and DLA's process for adding vulnerabilities to a POA&M [REDACTED]. High vulnerabilities, if exploited, could result in significant loss of data or downtime and allow a malicious actor to assume elevated privileges.

### (U) Cybersecurity Controls Assessed

(U) DoD Instruction 8510.01 requires DoD Components to implement cybersecurity controls outlined in NIST SP 800-53. We assessed each DoD Component's implementation of NIST SP 800-53 cybersecurity controls that we considered critical to protect collaboration tools. Table 6 identifies the cybersecurity controls we assessed and their importance.

*(U) Table 6. Assessed Cybersecurity Controls and Their Importance*

<b>(U)</b> Cybersecurity Control Category	Importance of the Cybersecurity Control
Authentication	Authentication mechanisms verify user identities, processes, or devices as a prerequisite to allowing access to the collaboration tool. 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 logon attempts, or automatically end user sessions after a defined period of inactivity.
Access Management	Access management helps organizations limit the risk of unauthorized access to collaboration tools by enabling only authorized users the ability to access the collaboration tool. This includes terminating user sessions or disabling user accounts after a defined period of inactivity.
Vulnerability Identification and Mitigation	Vulnerability identification and mitigation includes scanning collaboration tools to identify potential weaknesses, such as application vulnerabilities, that a malicious actor could exploit as a route to gain access to networks and systems. Identifying and mitigating vulnerabilities reduces a malicious cyber actor's ability to introduce malware on networks and steal critical information that could compromise national security. DoD Components can identify and mitigate vulnerabilities on collaboration tools to prevent malicious cyber actors who target unsecure collaboration tools to steal sensitive information.
Incident Response and System Monitoring	Incident response programs detect, respond to, and mitigate against cyber attacks. Incident response and system activity monitoring includes establishing controls and configurations that allow system administrators to monitor collaboration tools for malicious activities that could result in attacks on DoD networks and systems. <span style="float: right;"><b>(U)</b></span>

(U) Source: The DoD OIG.

### ***(U) The DLA Did Not Mitigate All Vulnerabilities in a Timely Manner***

(U) DLA network administrators did not mitigate all known high vulnerabilities for Zoom for Government on its network in a timely manner. In addition, DLA network administrators did not develop POA&Ms for vulnerabilities they were not able to mitigate. DoD Instruction 8510.01 requires DoD Components to mitigate vulnerabilities or develop a POA&M for vulnerabilities that they cannot mitigate

(U) in a timely manner. To determine whether the DoD Components mitigated vulnerabilities associated with collaboration tools in a timely manner, we compared network scan results from January through July 2022.<sup>24</sup>

~~(CUI)~~ An April 2022 scan revealed that 1 of the 38 vulnerabilities identified in a February 2022 scan remained unmitigated. [REDACTED]  
[REDACTED]. The one vulnerability remained unmitigated because DLA network engineers were unable to upgrade Zoom for Government on specific workstations when users were not connected to the network.<sup>25</sup> In addition, the DLA IT Program Manager stated that the DLA tool that deploys software updates to their workstations experienced a malfunction that prevented workstations from receiving the Zoom for Government software update. After our virtual site visit, the DLA took action to mitigate the vulnerability in May 2022 and therefore, we do not have a recommendation regarding this specific vulnerability.

~~(CUI)~~ Although DLA network administrators mitigated the vulnerability after 84 days, they did not include the vulnerability on a POA&M while they were identifying a solution. According to the IT Program Manager, not including the vulnerability on a POA&M was an oversight and the DLA's process for adding vulnerabilities to a POA&M [REDACTED]  
[REDACTED]. The IT Program Manager acknowledged that DLA should update the POA&M process to [REDACTED]."

(U) Without a POA&M, DLA network administrators may be unable to identify and correct network weaknesses, establish risk mitigation activities, or determine how long a vulnerability remained unmitigated. Consistently mitigating known vulnerabilities is part of basic cyber hygiene. According to the Cybersecurity and Infrastructure Security Agency, malicious cyber actors search for known vulnerabilities they can exploit to gain unauthorized access to networks.<sup>26</sup> If a malicious cyber actor gains unauthorized access to vulnerable enterprise resources and telework devices, the actor can eavesdrop on and extract sensitive communications. Additionally, malicious cyber actors can elevate privileges to launch a denial-of-service attack that can significantly disrupt organizational

<sup>24</sup> (U) A network scan is an automated review performed by a vulnerability scanning tool that determines whether the configuration settings of all systems or a portion of systems meet specific requirements.

<sup>25</sup> (U) When systems are not connected to the network, network engineers should send out a request to connect systems to the network to receive the required updates.

<sup>26</sup> (U) Cybersecurity and Infrastructure Security Agency Binding Operational Directive 19-02 "Vulnerability Remediation Requirements for Internet-Accessible Systems," April 29, 2019.

(U) operations. Therefore, the CIO for DLA should update its POA&M process to ensure a POA&M is developed for all vulnerabilities that cannot be mitigated in a timely manner.

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

(U) According to the Cybersecurity and Infrastructure Security Agency, the COVID-19 pandemic has resulted in a significant increase in teleworking since March 2020, with increased attacks from malicious cyber actors. DoD Components that fully implement NIST cybersecurity controls, such as identifying and mitigating vulnerabilities for their collaboration tools in a timely manner, decrease the risk of exposing DoD networks to potential malicious activity. In addition, implementing cybersecurity controls could prevent malicious cyber actors from exploiting unmitigated collaboration tool vulnerabilities to steal DoD information, which could put the United States at a disadvantage against its adversaries. To maintain the cybersecurity posture of collaboration tools, DoD Components should continue to identify and mitigate vulnerabilities in a timely manner or develop POA&Ms to decrease the risk that malicious actors could exploit known collaboration tool weaknesses. As the DoD workforce continues to use collaboration tools to facilitate telework, DoD Components should remain alert and attentive to known system vulnerabilities and cyber attacks that may threaten DoD information shared using collaboration tools.

## **(U) Recommendation, Management Comments, and Our Response**

### ***(U) Recommendation C.1***

**(U) We recommend that the Chief Information Officer for the Defense Logistics Agency update the Plan of Action and Milestones process to ensure a Plan of Action and Milestones is developed for all vulnerabilities that cannot be mitigated in a timely manner.**



### ***(U) Defense Logistics Agency Acting Chief Information Officer Comments***

(U) The DLA Acting CIO agreed, stating that Zoom for Government is part of the DLA's regular scanning and patch management program. The Acting CIO also stated that Zoom for Government was included in the POA&M process as part of the assessment and authorization efforts by the Program Management Office and the Information System Security Manager.<sup>27</sup>

### ***(U) Our Response***

(U) Comments from the Acting CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Acting CIO provides supporting documentation, such as a policy showing that the DLA updated the POA&M process to include Zoom for Government.

---

<sup>27</sup> (U) Assessment and authorization refers to the two-step authorization process used for cloud-based collaboration tools to assess the tool to determine if it meets security requirements necessary to host DoD information and to accept the risk of hosting DoD information through an authorization to operate.

## (U) Appendix A

---

### (U) Scope and Methodology

(U) We conducted this performance audit from December 2021 through January 2023 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 approve and deploy collaboration tools, and to protect information shared using these tools, we interviewed officials from the following organizations.

- (U) Office of the DoD Chief Information Officer
- (U) Office of the Army Chief Information Officer
- (U) Defense Information Systems Agency
- (U) Joint Forces Headquarters–DoD Information Network
- (U) U.S. Army Cyber Command
- (U) Army Network Enterprise Technology Command
- (U) Naval Fleet Cyber Command
- (U) Naval Network Warfare Command
- (U) Naval Cyber Defense Operations Command

(U) We interviewed project managers and IT 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 and cybersecurity controls.

(U) We selected a nonstatistical sample of 8 of 39 Component-deployed collaboration tools used during the COVID-19 pandemic. For the eight collaboration tools sampled, we selected eight DoD Components to evaluate the security controls and configuration settings they implemented to protect the collaboration tools. In addition, we selected a nonstatistical sample of two of six DoD enterprise collaboration tools available through DISA for use by all DoD users. Table 7 lists the nine DoD Components and the 10 collaboration tools we assessed.

(U) Table 7. DoD Components and Collaboration Tools Reviewed

(U) DoD Component	Collaboration Tool Used
<b>Enterprise Collaboration Tools</b>	
Defense Information Systems Agency	Microsoft Teams
	Cisco Jabber
<b>DoD Component-Deployed Collaboration Tools</b>	
Defense Advanced Research and Projects Agency	Zoom for Government
Defense Finance and Accounting Service	Adobe Connect
Defense Threat Reduction Agency	Zoom for Government
Defense Counterintelligence and Security Agency	Cisco Webex
Defense Logistics Agency	Zoom for Government
U.S. Army Cyber Command	Zoom for Government
National Geospatial-Intelligence Agency	Rocket Chat Unclassified Cloud
National Security Agency	Collaboration Development Environment (U)

(U) Source: The DoD OIG.

(U) To determine whether collaboration tools used to facilitate telework during the COVID 19 pandemic exposed DoD networks and systems to potential malicious activity and whether DoD Components implemented security controls and configuration settings, we:

- (U) virtually observed demonstrations of how users authenticated into collaboration tools;
- (U) virtually observed configuration settings to verify compliance with the FedRAMP Moderate Baseline, DISA Application Security and Development STIG, or CNSSI 1253;
- (U) obtained authorization documentation for collaboration tools to verify that DoD Components assessed and authorized the use of the tools;
- (U) obtained screenshots of configuration settings for collaboration tools;
- (U) obtained and analyzed network vulnerability scan results to verify that DoD Components mitigated vulnerabilities for collaboration tools in a timely manner;
- (U) obtained security incident logs to verify that the logs included the security incident information required by FedRAMP Moderate Baseline, NIST Special Publication 800-53, or CNSSI 1253; 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 the use of collaboration tools.

## **(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 controls environment related to:

- (U) system access and authentication,
- (U) encryption of data stored on systems,
- (U) encryption of data transmitted across the network,
- (U) incident response,
- (U) system monitoring,
- (U) risk assessments, 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 to assess.

## **(U) Prior Coverage**

(U) During the last 5 years, the DoD OIG issued three reports discussing the protection of DoD information while using collaboration tools during the COVID-19 pandemic. Unrestricted DoD OIG reports can be accessed at <http://www.dodig.mil/reports.html/>.

(U) 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’s initial challenges occurred because some DoD Components had not fully tested whether their information systems could support government-wide mandated telework and had not conducted telework exercises with their personnel before March 2020 as required by the DoD Implementation Plan and the DoD Telework Policy. Therefore, some DoD Components were unprepared for the network and communications limitations, as well as equipment and application shortfalls, uncovered by the transition to maximum telework.

(U) 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 implement required cybersecurity controls to protect DoD networks during maximum telework. In addition, the [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED].

~~(CUI)~~ [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

(U) DODIG-2021-050, “Audit of Contracts for DoD Information Technology Products and Services Procured by DoD Components in Response to the Coronavirus Disease–2019 Pandemic,” February 12, 2021

(U) The DoD OIG determined that for the 28 contract actions reviewed, DoD Components did follow the Coronavirus Aid, Relief, and Economic Security Act and other Federal and DoD requirements, and procured IT products and services needed to support operations in response to the COVID-19 pandemic. In addition, the DoD OIG determined that DoD Components assessed whether known cybersecurity risks existed and developed risk mitigation strategies before procuring or using the IT products.

## (U) Appendix B

---

### (U) Sampling Approach

(U) We used a nonstatistical sampling approach to select the DoD Components and collaboration tools to review for this audit. To determine the universe of DoD Components using collaboration tools, we sent a questionnaire requesting that the DoD Components identify the collaboration tools used. We combined the responses to create a consolidated universe of 183 collaboration tools used by DoD Components. We then compiled the initial responses received from DoD Components and judgmentally removed any tools that did not align with our definition of collaboration tools. To eliminate redundancy, we also removed DoD Components that relied on enterprise collaboration tools available through DISA.

(U) The following 19 DoD Components reported using collaboration tools other than those available through DISA.

- (U) Department of the Army
- (U) Department of the Navy
- (U) Department of the Air Force
- (U) Defense Advanced Research Projects Agency
- (U) Defense Contract Management Agency
- (U) Defense Counterintelligence and Security Agency
- (U) Defense Finance and Accounting Service
- (U) Defense Health Agency
- (U) Defense Intelligence Agency
- (U) Defense Logistics Agency
- (U) Defense Security Cooperation Agency
- (U) Defense Technology Security Administration
- (U) Defense Threat Reduction Agency
- (U) Joint Force Headquarters–DoD Information Network
- (U) Missile Defense Agency
- (U) National Geospatial-Intelligence Agency
- (U) National Security Agency
- (U) Space Development Agency
- (U) Uniformed Services University of Health Services

# (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
JAMES COMER, KENTUCKY  
RANKING MINORITY MEMBER

**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>

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.<sup>1</sup> 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.<sup>2</sup> 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.<sup>3</sup>

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.<sup>4</sup> On April 20, 2021, the Cybersecurity and Infrastructure Security Agency

---

<sup>1</sup> Pub. L. No. 113–283 (2014); 44 U.S.C. §3555.

<sup>2</sup> 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](http://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-16.pdf)).

<sup>3</sup> 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/](http://www.dodig.mil/reports.html/Article/2556226/audit-of-maintaining-cybersecurity-in-the-coronavirus-disease-2019-telework-env/)).

<sup>4</sup> 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.<sup>5</sup> *The Washington Post* reported that “Chinese government hackers are believed to have compromised dozens of U.S. government agencies” through the Pulse Connect breach.<sup>6</sup>

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.”<sup>7</sup>

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.<sup>8</sup>

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>).

<sup>5</sup> 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.”).

<sup>6</sup> *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](https://www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac_story.html)).

<sup>7</sup> 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>).

<sup>8</sup> 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

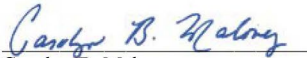
Page 3

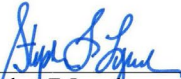
- The acquisition, deployment, management, and security of collaboration platforms such as Microsoft Teams, Zoom, Slack, and Cisco Webex;
- Whether the Department, and all components, has implemented security controls to prevent the unauthorized dissemination of controlled unclassified information, personally 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;<sup>9</sup>
- 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  
 Chairwoman  
 Committee on Oversight and Reform


  
 Stephen F. Lynch  
 Chairman  
 Subcommittee on National Security

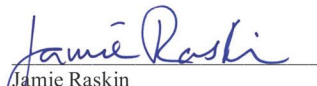
<sup>9</sup> Cybersecurity and Infrastructure Security Agency, *TIC 3.0 Core Guidance Documents* (accessed on Apr. 22, 2021) (online at [www.cisa.gov/publication/tic-30-core-guidance-documents](http://www.cisa.gov/publication/tic-30-core-guidance-documents)).


## (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 Gishnaoorthi  
Chairman  
Subcommittee on Economic and  
Consumer Policy

  
Jamie Raskin  
Chairman  
Subcommittee on Civil Rights and  
Civil Liberties

  
Ro Khanna  
Chairman  
Subcommittee on Environment

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

The Honorable Glenn Grothman, Ranking Member  
Subcommittee on National Security

The Honorable Jody Hice, Ranking Member  
Subcommittee on Government Operations

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

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

The Honorable Ralph Norman, Ranking Member  
Subcommittee on Environment

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

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

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

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

## (U) Appendix D

### (U) Enterprise and Alternative Collaboration Tools

(U) In April 2020, the DoD CIO issued a memorandum directing DoD Components to use the DoD’s enterprise collaboration tools available through DISA. The DoD CIO also approved the use of 13 alternative collaboration tools if the enterprise tools did not fully meet the needs of DoD Components. Table 8 lists the enterprise and alternative collaboration tools approved in the DoD CIO memorandum.

(U) Table 8. Enterprise and Alternative Collaboration Tools

(U) Enterprise Collaboration Tools		
Commercial Virtual Remote	Defense Collaboration Services - Unclassified	DoD Enterprise Portal Service
Alternative Collaboration Tools		
Adobe Connect	Cisco Webex	CoSo Cloud
Google G-Suite	Huddle	Zoom for Government
Collab9	Avaya	Box Enterprise Cloud Content Collaboration Platform
Cisco Hosted Collaboration Solution	Microsoft Office 365 vNext IL5	Microsoft: Dynamics 365 for Government
Cisco Webex Collaboration for U.S. Government		(U)

(U) Source: The DoD OIG.

# (U) Management Comments

## (U) DoD Chief Information Officer



CHIEF INFORMATION OFFICER

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

APR 21 2023

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Review and Comment of DoD Inspector General *"Audit of DoD Actions Taken to Protect DoD Information When Using Collaboration Tools During the Coronavirus Disease-2019 Pandemic"* (D2022-D000CR-0038.00) Draft Report

This is the Department of Defense (DoD) Chief Information Officer (CIO) response to the DoD Inspector General Report, *"Audit of DoD Actions Taken to Protect DoD Information When Using Collaboration Tools During the Coronavirus Disease-2019 Pandemic"* (D2022-D000CR-0038.00)

**DoD IG RECOMMENDATION A.1:** We recommend that the DoD Chief Information Officer:

- a. Issue guidance that states that deploying a collaboration tool with a provisional authorization does not eliminate the need to perform the required cybersecurity reciprocity process.
- b. Direct DoD Components' Authorizing Officials to identify collaboration tools in use, verify that the required reciprocity process was completed foreach, and, if the process was not completed, direct the DoD Component Authorizing Officials to complete the reciprocity process.

**DoD CIO RESPONSE:** DoD CIO agrees with the DoD IG recommendation.

The DoD CIO will reinforce the existing policy to leverage collaboration capabilities with existing provisional authorizations as outlined in the DoD CIO signed memo *"Authorized Telework Capabilities and Guidance"* dated April 13, 2020, and *"Authorizations to Operate Extensions and Cybersecurity Function Prioritization Guidance"* dated April 3, 2020. Both documents can be found on <https://public.cyber.mil> site.

The DoD CIO will require components to identify collaboration tools in use and verify that those capabilities were authorized according to DoDI 8510.01 instructions and the aforementioned memos.

A security review to verify "CONTROLLED UNCLASSIFIED INFORMAITON" (CUI) markings in the report has been completed and there are no additional recommendations.

The point of contact for this matter is [REDACTED]. He can be reached at [REDACTED] or [REDACTED].

John B. Sherman

## (U) Defense Finance and Accounting Service



### DEFENSE FINANCE AND ACCOUNTING SERVICE

8899 EAST 56<sup>TH</sup> STREET  
INDIANAPOLIS, IN 46249-0201

DFAS-IN/ZT

April 21, 2023

MEMORANDUM FOR DEPARTMENT OF DEFENSE (DoD) OFFICE OF INSPECTOR  
GENERAL (OIG)

SUBJECT: DoD OIG Draft Report, Audit of DoD Actions Taken to Protect DoD Information  
When Using Collaboration Tools During the Coronavirus Disease – 2019 Pandemic,  
Project No. D2022-D000CR-0038.000

In accordance with the subject draft report, Defense Finance and Accounting Service (DFAS) concurs with recommendations A.2, B.1.a, and B.1.b. Management comments are included at TAB A.

DFAS has reviewed the draft report and has no changes to the DoD OIG classification or markings. The completed DoD OIG Request for Security Markings Review is included at TAB B.

DFAS acknowledges that our Component's Controlled Unclassified Information will be released to Congress.

My point of contact is [REDACTED].

PERSSON.MATS

A [REDACTED]

Mats A. Persson

Acting Director, Information & Technology

Proudly Serving America's Heroes

[www.dfas.mil](http://www.dfas.mil)

## (U) Defense Finance and Accounting Service (cont'd)

~~CUI~~

(U) Department of Defense (DoD) Office of Inspector General (OIG) Draft Report, Audit of DoD Actions Taken to Protect DoD Information When Using Collaboration Tools During the Coronavirus Disease – 2019 Pandemic, Project No. D2022-D000CR-0038.000

### (U) Defense Finance and Accounting Service (DFAS) Management Comments to Subject Draft Report

#### (U) Recommendation A.2

(U) We recommend that the Authorizing Official for DFAS review the security authorization package for Adobe Connect, identify the security impact and risks and, if the risks are determined acceptable, formally accept the risk of using the tool and update the authorization package.

#### (U) Management Response:

(U) DFAS concurs with recommendation A.2 and completed an authorization package for Adobe Connect on March 27, 2023.

(U) Estimated Completion Date (ECD): COMPLETE

#### (U) Recommendation B.1

(U) We recommend that the Chief Information Officer for DFAS renegotiate changes with the Adobe Connect vendor to configure Adobe Connect to:

- a. (U) Require privileged users to authenticate into the collaboration tool using multifactor authentication.

#### (U) Management Response:

(U) DFAS concurs with recommendation B.1.a and plans to use the Global Federated User Domain (GFUD) to implement common access card authentication (CAC) for privileged users, satisfying the requirement to implement multifactor authentication in Adobe Connect. The Plan of Action and Milestones is in place with a completion date of September 15, 2023.

(U) Estimated Completion Date (ECD): September 15, 2023

- b. (U) Lock user accounts after three unsuccessful logon attempts in a 15-minute period.

#### (U) Management Response:

(U) DFAS concurs with recommendation B.1.b and is working with the contractor to implement locking accounts after three unsuccessful logon attempts in a 15-minute period. The Plan of Action and Milestones is in place with a completion date of April 28, 2023.

(U) Estimated Completion Date (ECD): April 28, 2023.

~~CUI~~

# (U) Defense Logistics Agency



**DEFENSE LOGISTICS AGENCY**  
HEADQUARTERS  
8725 JOHN J. KINGMAN ROAD  
FORT BELVOIR, VIRGINIA 22060-6221

April 25, 2023

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL, PROGRAM DIRECTOR FOR AUDIT, CYBERSPACE OPERATIONS DIRECTORATE

SUBJECT: Response to Office of Inspector General Draft Report: “Audit of DoD Actions Taken to Protect DoD Information When Using Collaboration Tools During the Coronavirus Disease-2019 Pandemic” (Project No. D2022-D000CR-0038.000)

DLA appreciates the opportunity to review and comment on this draft audit report, dated March 24, 2023. DLA agrees with the findings and recommendations as presented and has completed corrective actions. A copy of the agency’s specific response to each of the recommendations is attached.

The point of contact for this audit is [REDACTED]

RUNSTROM.KAR [REDACTED]  
YN.A [REDACTED]

KARYN A. RUNSTROM  
Acting Chief Information Officer  
DLA Information Operations

Attachment  
Individual responses to each of the report recommendations

## (U) Defense Logistics Agency (cont'd)

**DOD OIG DRAFT REPORT DATED MARCH 24, 2023, “Audit of DoD Actions Taken to Protect DoD Information When Using Collaboration Tools During the Coronavirus Disease-2019 Pandemic” (Project No. D2022-D000CR-0038.000)**

**DEFENSE LOGISTICS AGENCY’S RESPONSE TO THE DOD OIG RECOMMENDATIONS**

**RECOMMENDATION A.3.:** DoD OIG recommends that the Authorizing Official for the Defense Logistics Agency identify the security impact and risks of using Zoom for Government and, if the risk is determined acceptable, formally accept the risk of using the tool, and update the authorization package.

**DLA RESPONSE:** Agree. This recommendation has been fully implemented by DLA via authorizing this system under a full Assess & Authorize package. Package currently has an ATO and is due for re-Authorization in March 2026. The DLA Security Control Assessor (SCA) recently completed the SCA review of the Zoom for Government IL4 (Z4G) Risk Management Framework request in eMASS. The security categorization of Moderate, Moderate, Low and with the identified risks, the RMF request submitted in eMASS presents Very Low residual risk to DLA and the DoD. DLA requests closure of this recommendation.

**RECOMMENDATION B.2.:** DoD OIG recommends that the Chief Information Officer for the Defense Logistics Agency configure Zoom for Government to require a minimum of 12 characters for password logon for non-privileged users.

**DLA RESPONSE:** Agree. DLA has implemented this requirement via DLA Zoom for Government IL4 instance. All passwords are required to be 12-character minimum length. Enforcement started on 3/13/2023. DLA requests closure of this recommendation.

**RECOMMENDATION C.1.:** DoD OIG recommends that the Chief Information Officer for the Defense Logistics Agency update the Plan of Action and Milestones process to ensure a Plan of Action and Milestones is developed for all vulnerabilities that cannot be mitigated in a timely manner.

**DLA RESPONSE:** Agree. DLA has implemented this recommendation for the DLA Zoom for Government IL4 instance. The system is part of the regular scanning and patch management program. In addition, DLA Zoom for Government IL4 program has been implemented into the POAM process as part of Assess & Authorize efforts by the PMO and ISSMs. DLA requests closure of this recommendation.



## (U) Defense Threat Reduction Agency

~~CUI~~



**DEFENSE THREAT REDUCTION AGENCY**  
8725 JOHN J. KINGMAN ROAD, STOP 6201  
FORT BELVOIR, VA 22060-6201

April 28, 2023

MEMORANDUM FOR DOD IG ATTN: [REDACTED]

SUBJECT: ~~CUI~~ Defense Threat Reduction Agency (DTRA) response to “Audit of DoD Actions Taken to Protect DoD Information When Using Collaboration Tools During the COVID-19 Pandemic” report. (Project No. D2022-D000CR-0038.000)

References: ~~CUI~~ “Audit of DoD Actions Taken to Protect DoD Information When Using Collaboration Tools During the COVID-19 Pandemic” Report (Project No. D2022-D000CR-0038.000)

(U) DTRA agrees with the recommendations provided in the “Audit of DoD Actions Taken to Protect DoD Information When Using Collaboration Tools During the COVID-19 Pandemic” report.

(U) Action to Recommendation A.4: DTRA Authorizing Official reviewed the Zoom for Government package, formally accepted the security impacts and the risk of using Zoom for Government. The authorization package/Authorization to Operate (ATO) memo for Defense Threat Reduction Agency Network – Unclassified (DTRANET-U) was updated to include Zoom for Government. The updated DTRANET-U ATO memo (Appendix A) has been provided as a supporting document.

(U) Action to Recommendation B.3.a & B.3.b: DTRA Chief Information Officer ensured that Zoom for Government is configured to:

- a. (U) Require privileged users to authenticate into the collaboration tool using multifactor authentication. The screenshot capturing the updated configuration has been provided as a supporting document.
- b. (U) Require a minimum of 12 characters for password logon for non-privileged users. The screenshot capturing the updated configuration has been provided as a supporting document.

(U) Action to Recommendation B.3.c: DTRA Chief Information Officer will ensure that Zoom for Government is configured to:

- c. (U) Lock user accounts after three unsuccessful logon attempts in a 15-minute period. DTRA is currently working with the vendor and will require a six-month (24 OCT 2023) Plan of Action & Milestone (POA&M) to close this recommendation/finding.

~~CUI~~

## (U) Defense Threat Reduction Agency (cont'd)

~~CUI~~

SUBJECT: ~~CUI~~ Defense Threat Reduction Agency (DTRA) response to “Audit of DoD Actions Taken to Protect DoD Information When Using Collaboration Tools During the COVID-19 Pandemic” report. (Project No. D2022-D000CR-0038.000)

X ROTH.MICHAEL [REDACTED]  
J [REDACTED]

Michael J. Roth  
Authorizing Official and DTRA Chief Information Security Officer

X TURK.ROBERT.WA [REDACTED]  
YNE [REDACTED]

Robert Wayne Turk  
Acting Director, Information Management & Technology and Chief Information Officer

~~CUI~~

## (U) Acronyms and Abbreviations

---

(U) AO	Authorizing Official
(U) ARCYBER	U.S. Army Cyber Command
(U) CIO	Chief Information Officer
(U) CNSSI	Committee on National Security Systems Instruction
(U) COVID-19	Coronavirus disease–2019
(U) CUI	Controlled Unclassified Information
(U) DFAS	Defense Finance Accounting Service
(U) DISA	Defense Information Systems Agency
(U) DLA	Defense Logistics Agency
(U) DTRA	Defense Threat Reduction Agency
(U) FedRAMP	Federal Risk and Authorization Management Program
(U) IC	Intelligence Community
(U) ICD	Intelligence Community Directive
(U) IT	Information Technology
(U) NGA	National Geospatial-Intelligence Agency
(U) NIST	National Institute of Standards and Technology
(U) POA&M	Plan of Action and Milestones
(U) SP	Special Publication
(U) SRG	Security Requirements Guide
(U) STIG	Security Technical Implementation Guide

## (U) Glossary

---

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

**(U) Authorization-to-Operate.** The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

**(U) Brute-Force Password Attacks.** Method of accessing a device by attempting multiple combinations of passwords.

**(U) Cloud Service.** Information technology services provided by a cloud service provider.

**(U) Collaboration Tool.** Hardware and software that allows personnel in geographically dispersed locations to perform tasks and work on projects collaboratively.

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

**(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) High Vulnerabilities.** A weakness in a system, application, or network that if exploited, could result in obtaining unauthorized elevated privileges, significant data loss, and network downtime.

**(U) Multifactor Authentication.** Authentication using two or more different factors to achieve authentication. Factors include something known to the user (for example, a personal identification number or password), something in the user's possession (for example, a cryptographic identification device or token), or a physical aspect of the user (such as biometric information).

**(U) Plan of Action and Milestones.** 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) Privileged User.** A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

**(U) Security Requirements Guide.** Collection of requirements that mitigate sources of vulnerabilities found across IT systems and applications.

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

**(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) Vulnerability.** A weakness in a system, application, or network that a threat could exploit.



## **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/Whistleblower-Reprisal/> or contact the Whistleblower Protection Coordinator at [Whistleblowerprotectioncoordinator@dodig.mil](mailto: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](mailto:public.affairs@dodig.mil); 703.604.8324

### **DoD OIG Mailing Lists**

[www.dodig.mil/Mailing-Lists/](http://www.dodig.mil/Mailing-Lists/)

### **Twitter**

[www.twitter.com/DoD\\_IG](http://www.twitter.com/DoD_IG)

### **DoD Hotline**

[www.dodig.mil/hotline](http://www.dodig.mil/hotline)

**CUI**



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive  
Alexandria, Virginia 22350-1500  
[www.dodig.mil](http://www.dodig.mil)  
DoD Hotline 1.800.424.9098

**CUI**