Report No. DODIG-2022-041

~~CUI~~

INSPECTOR GENERAL

U.S. Department of Defense

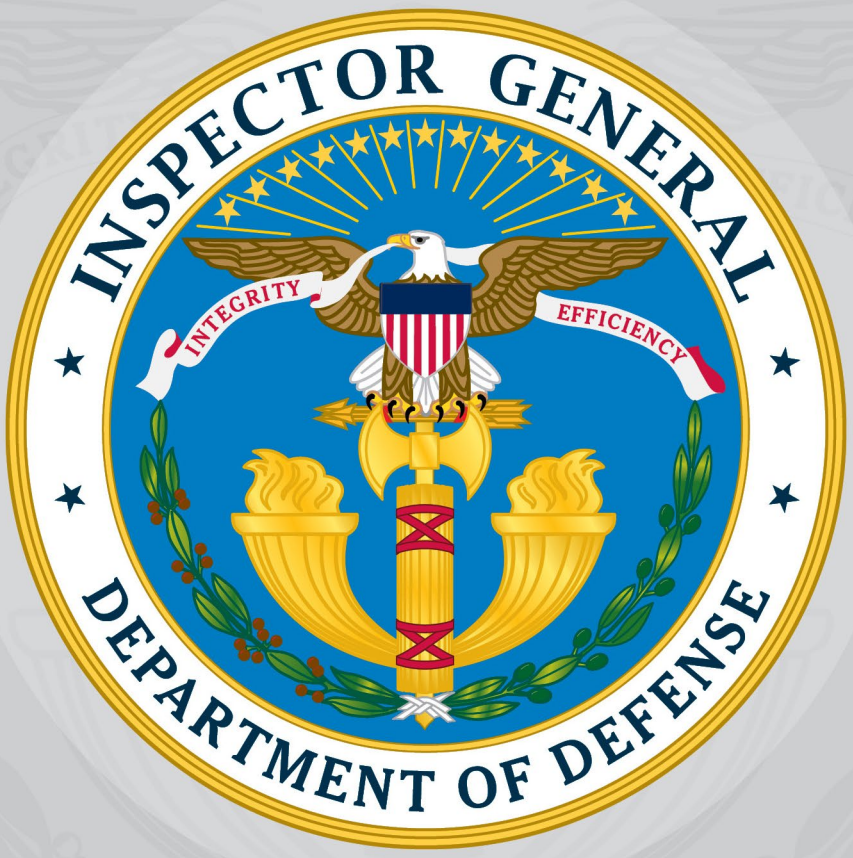
DECEMBER 3, 2021

(U) Audit of the DoD's Use of Cybersecurity Reciprocity Within the Risk Management Framework Process

~~Controlled by: DoD OIG~~
~~Controlled by: Audit/Cyberspace Operations~~
~~CUI Category: BUDG; STAT~~
~~LDC: FED ONLY, DL (SASC, HASC, SAC-D, HAC-D, HSGAC, HCOR, SSCI, HPSCI)~~
POC: [redacted]

INTEGRITY ★ INDEPENDENCE★ EXCELLENCE

~~CUI~~


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

(U) Results in Brief

(U) Audit of the DoD's Use of Cybersecurity Reciprocity Within the Risk Management Framework Process

December 3, 2021

(U) Objective

(U) The objective of this audit was to determine whether DoD Components leveraged cybersecurity reciprocity to reduce redundant test and assessment efforts when authorizing information technology through the Risk Management Framework (RMF) process. This audit was conducted concurrently with audits conducted by the Military Department audit agencies: U.S. Army Audit Agency (AAA), Naval Audit Service (NAS), and Air Force Audit Agency (AFAA).

(U) The AAA, NAS, and AFAA audits focused on the use of reciprocity within their respective Military Departments, whereas our audit focused on the use of reciprocity by a combatant command (U.S. Transportation Command), two Defense agencies (Defense Health Agency, and Defense Logistics Agency), and a DoD field activity (Defense Human Resources Activity). Each audit agency conducted their audits and issued their reports and recommendations separately. The results of the Military Department audit agencies are summarized in Appendix B.

(U) Background

(U) In March 2014, the DoD began transitioning to a new approach for authorizing the operations of its information systems known as the RMF process. The RMF process is a disciplined and structured process that combines system security and risk management activities into the system development lifecycle. One benefit of the

(U) Background (cont'd)

(U) RMF process is the ability to leverage reciprocity, which reduces time and work resources spent on redundant tests, assessments, and documentation efforts.

(U) Reciprocity is an agreement to accept and reuse another organization's (internal or external to the DoD) security assessments to share information and thereby reduce associated costs in time and resources for authorizing information technology systems to operate on the DoD Information Network. The DoD Chief Information Officer (CIO) requires DoD Components to leverage reciprocity when authorizing systems through the RMF process. Leveraging reciprocity enables the DoD to more rapidly deliver secure systems to DoD Components, while reducing process inefficiencies and system authorization costs. For this report, we determined whether DoD Components leveraged reciprocity by reviewing their actions for:

- (U) making systems and authorization documentation available to other DoD Components in the DoD's RMF compliance tool (Enterprise Mission Assurance Support Service);
- (U) appointing reciprocity users that can review existing system authorization documentation across all DoD versions of the Enterprise Mission Assurance Support Service (eMASS); and
- (U) identifying and authorizing common controls to be used by all systems within the component.

(U) Finding

(U) The U.S. Transportation Command and the Defense Health Agency (DHA) leveraged reciprocity while authorizing their systems through the RMF process; however, the Defense Logistics Agency (DLA) and Defense Human Resources Activity (DHRA) did not. Specifically:

- (U) DLA cybersecurity officials did not make their systems and authorization documentation available in eMASS for reciprocity across the DoD. In addition,

(U) Results in Brief

(U) Audit of the DoD's Use of Cybersecurity Reciprocity Within the Risk Management Framework Process

(U) Finding (cont'd)

(U) DLA cybersecurity officials did not appoint eMASS reciprocity users to obtain and review existing systems and authorization documentation. This occurred because they concluded that their systems had unique missions, and were relevant only to DLA personnel. Therefore, DLA cybersecurity officials incorrectly determined their systems were not subject to DoD reciprocity requirements.

- (U) DLA cybersecurity officials did not authorize all Tier 2 common controls to be used by DLA systems because they did not consider the DoD's RMF and reciprocity policy and implementation guidance to be a priority.
- (U) DHRA cybersecurity officials also did not appoint reciprocity users to obtain and review existing systems and authorization documentation, and identify and authorize all Tier 2 common controls to be used by DHRA systems. This occurred because the DHRA was undergoing a reorganization, and the DHRA Director had yet to assign and document cybersecurity roles and responsibilities for implementing RMF and reciprocity requirements.

(U) In addition, the DoD CIO did not implement processes necessary to oversee DoD Components' compliance with DoD reciprocity guidance. Instead, the DoD CIO relied on DoD Components to manage the system authorization process and use reciprocity to maximize the reuse of testing and assessments results developed during prior system authorizations.

~~(CUI)~~ The DoD's requirement to leverage reciprocity enables the DoD to rapidly deliver secure systems to DoD Components while reducing process inefficiencies and system authorization costs. Unless DoD Components fully leverage RMF reciprocity, the associated benefits may not be fully realized, including cost savings. [redacted]

~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted] The DoD could achieve even greater cost savings and efficiencies if all DoD Components maximized the use of reciprocity when authorizing their systems through RMF. DoD Components can increase reciprocity by making systems and authorization documentation available to other DoD Components in eMASS, appointing eMASS reciprocity users, and identifying and authorizing common controls.

(U) Management Actions Taken

~~(CUI)~~ During the audit, DLA and DHRA cybersecurity officials took corrective actions to leverage reciprocity when authorizing systems through the RMF process. On April 14, 2021, DLA cybersecurity officials [redacted] and authorization documentation available in eMASS. In addition, on April 21, 2020, DLA cybersecurity officials issued a reciprocity memorandum appointing three reciprocity users, and on January 8, 2021, the DLA Authorizing Official granted an authorization to operate for the DLA Tier 2 common controls package.

(U) Results in Brief

(U) Audit of the DoD's Use of Cybersecurity Reciprocity Within the Risk Management Framework Process

(U) Actions Taken (cont'd)

(U) On September 14, 2020, a DHRA cybersecurity official issued a reciprocity memorandum appointing eight reciprocity users. Additionally, on May 14, 2021, the DHRA Authorizing Official granted an authorization to operate for the DHRA Tier 2 common controls package. Furthermore, DHRA cybersecurity officials developed six standard operating procedures defining roles and responsibilities, and steps necessary to authorize the DHRA systems through the RMF process.

(U) We consider the actions taken by DLA and DHRA cybersecurity officials to have addressed the issues identified during this audit. Therefore, this report does not include recommendations for the DLA and DHRA.

(U) Recommendations

(U) We recommend that the DoD CIO:

- (U) update the eMASS system registration process, in coordination with the eMASS Program Manager, to require DoD Component system program managers to select a valid justification for exemption when a system is not made available for reciprocity use;
- (U) revise existing guidance or issue new guidance that requires system program managers to certify that reciprocity was considered before authorizing and reauthorizing systems; and
- (U) review the AAA, NAS, and AFAA reports on reciprocity, and discuss findings and actions taken by each Military Service at an RMF Technical Advisory Group meeting.

(U) Management Comments and Our Response

(U) The Principal Director to the Deputy CIO for Resources and Analysis, Performing the Duties of the DoD CIO, agreed with the recommendations. We will close the recommendations once we verify that the agreed upon actions are complete. Please see the Recommendations Table on the next page for the status of recommendations.

(U) Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
(U) DoD Chief Information Officer	None	1, 2, 3	None

Please provide Management Comments by March 3, 2022.

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

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

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

December 3, 2021

(U) MEMORANDUM FOR CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
AUDITOR GENERAL, DEPARTMENT OF THE NAVY
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

(U) SUBJECT: Audit of the DoD's Use of Cybersecurity Reciprocity Within the Risk Management Framework Process (Report No. DODIG-2022-041)

(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. The comments are included in the report.

(U) This report contains three recommendations that are considered resolved. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section of this report, the recommendations will remain open until we verify that the agreed upon actions are complete.

(U) Please provide us within 90 days documentation showing that the agreed-upon actions have been completed or a status of the actions in progress. Send your response to either followup@dodig.mil if unclassified or rfunet@dodig.smil.mil if classified SECRET. We appreciate the cooperation and assistance received during the audit. If you have any questions, please contact me at [redacted]

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

(U) Contents

(U) Introduction

(U) Objective

(U) The objective of this audit was to determine whether DoD Components leveraged cybersecurity reciprocity to reduce redundant test and assessment efforts when authorizing information technology for use on the DoD Information Network (DODIN) through the Risk Management Framework (RMF) process.[1] This audit was conducted concurrently with audits performed by the U.S. Army Audit Agency (AAA), Naval Audit Service (NAS), and Air Force Audit Agency (AFAA). The AAA, NAS, and AFAA audits focused on the use of reciprocity within their respective Military Departments, whereas our audit focused on the use of reciprocity by a combatant command (U.S. Transportation Command), two Defense agencies (Defense Health Agency, and Defense Logistics Agency), and one DoD field activity (Defense Human Resources Activity). See Appendix A for the scope, methodology, and prior audit coverage related to our objective. See the Glossary for definitions of terms used in the report that relate to cybersecurity reciprocity.

(U) The AAA, NAS, and AFAA issued separate audit reports, specific to their Military Departments.[2] This report includes the results of those reports, the status of their recommendations, and our findings and conclusions specific to the use of reciprocity by one combatant command, two Defense agencies, and a DoD field activity. See Appendix B for summaries of final reports issued by the AAA, NAS, and AFAA.

(U) This audit was announced on August 30, 2018; however, due to the coronavirus disease–2019 pandemic, the audit was suspended. We reannounced this audit, with the same audit objectives, on January 21, 2021, to ensure previously collected information was relevant and accurate. Before the audit suspension, we identified several findings and communicated them to the respective DoD Components who took actions to address the findings while the audit was suspended.

[1] (U) For the purpose of this report, the term "cybersecurity reciprocity" is referred to as "reciprocity." Reciprocity is an agreement to accept and reuse another organization's (internal or external) security assessments to share information and reduce associated costs in time and resources for authorizing information technology systems to operate on the DODIN. The DODIN is the set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information to warfighters, policy makers, and support personnel, whether interconnected or stand-alone.

[2] (U) The AAA, NAS, and AFAA had slightly different audit objectives, and their approach to conducting the audits also differed from ours. AAA Report A-2019-0120-AXZ, "Inheriting Common Controls Within the Risk Management Framework," September 30, 2019; NAS Report N2020-0019, "Department of the Navy's Use of Cybersecurity Reciprocity Within the Risk Management Framework Process," April 9, 2020; and AFAA Report F2019-0007-O10000, "Risk Management Framework Tests and Assessments," August 13, 2019.

(U) Background

(U) In March 2014, the DoD began transitioning from the DoD Information Assurance Certification and Accreditation Process to a new approach for authorizing the operations of its information systems known as the RMF process.[3] The RMF provides a disciplined and structured process that combines system security and risk management activities into the system development lifecycle. DoD Instruction 8510.01 requires the DoD to implement the RMF to manage cybersecurity risks to DoD systems throughout the system's lifecycle.[4] One benefit of authorizing systems through the RMF process is the ability to leverage reciprocity, which reduces time and funding spent on conducting tests and assessments, and developing supporting documentation.

(U) RMF Process

(U) The National Institute of Standards and Technology (NIST) developed a seven-step RMF process for authorizing information technology (systems) for use on Federal agency networks.[5] The RMF process described in DoD Instruction 8510.01 is modeled after the NIST. The DoD Chief Information Officer (CIO) requires DoD Components to follow the seven-step process when authorizing information technology for use on the DODIN. The RMF process facilitates the use of reciprocity to reduce duplication of efforts and maximize existing assessments and authorization documentation developed during prior system authorizations. The seven-step RMF process is listed below.

1. **(U) Prepare**. The organization conducts essential preparatory activities to manage its security and privacy risks using the RMF. DoD Components leverage reciprocity of authorization documentation by identifying inheritable common controls satisfied by existing DoD or Component-level policy applicable to multiple systems within an organization.[6]
2. **(U) Categorize**. The organization categorizes the system and information processed, stored, and transmitted based on an impact analysis.

[3] (U) The DoD Information Assurance Certification and Accreditation Process was used to manage the implementation of information assurance capabilities and services, and provide visibility of accreditation decisions regarding the operation of DoD information systems. The DoD initiated the certification and accreditation of systems under the DoD Information Assurance Certification and Accreditation Process in November 2007.

[4] (U) DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology," March 12, 2014, Incorporating Change 3, December 29, 2020.

[5] (U) NIST Special Publication 800-37, "Risk Management Framework for Information Systems and Organizations," Revision 2, December 20, 2018.

[6] (U) Inheritance is a situation where the system receives protection from security controls that are developed, implemented and assessed, authorized, and monitored by an organization (internal or external to DoD) other than those responsible for the system. Common controls are security controls that are inherited by one or more information systems within an organization.

3. **(U) Select**. Based on the system's security categorization, the organization selects applicable security controls, including baseline controls and common controls. Baseline controls, which are established based on a defined impact level to a system, are the minimum security controls that must be implemented by a system owner, and are the starting point for the tailoring process in securing a system.
4. **(U) Implement**. The organization applies the selected security controls to the system and documents how controls are implemented. DoD Components leverage reciprocity during this step by evaluating previously completed system authorization documentation that reduces the need to conduct additional tests or assessments.
5. **(U) Assess**. The organization conducts assessments to determine whether the controls are implemented, operating as intended, and producing the desired outcome. DoD Components leverage reciprocity during this step by accepting test and assessment results of previously authorized systems.
6. **(U) Authorize**. The organization's authorizing official reviews system authorization documentation, analyzes operational risk, and issues the system's authorization to operate (ATO).[7] All DoD Components are required to share their systems and authorization documentation with other DoD Components through the Enterprise Mission Assurance Support Service (eMASS). eMASS is a web based application designed to assist RMF practitioners develop, collect, manage, and share cybersecurity-related data in compliance with RMF requirements.
7. **(U) Monitor**. The organization continuously monitors the system and operational environment for changes at the organization or system level that may adversely affect the previous risk determination. DoD Components are required to update inherited common controls as the DoD or Components issue new guidance.

(U) Leveraging Reciprocity Through the RMF Process

(U) The DoD CIO requires DoD Components to leverage reciprocity when authorizing information technology through the RMF process, and use the RMF Knowledge Service web portal as the authoritative source for RMF procedures and guidance.[8] Nonetheless, in October 2016, the DoD CIO issued a memorandum expressing concern about DoD Components not leveraging reciprocity and

[7] (U) The authorizing official is a senior Federal official or executive with the authority to authorize, and assume responsibility for, the operation of an information system or the use of common controls. An ATO is the official management decision issued by the authorizing official to authorize operation of a system and to explicitly accept the residual risk to agency operations.

[8] (U) The RMF Knowledge Service is an online knowledge base web portal that functions as the authoritative source for DoD RMF procedures and implementation guidance, supporting RMF implementation, planning, and execution.

(U) conducting redundant and unnecessary testing when authorizing information technology. The memorandum emphasized the importance of reciprocity and required authorization documentation to be shared among DoD Components to maximize the reuse of existing testing and assessments.[9]

(U) Leveraging reciprocity allows the DoD to rapidly deliver secure systems to DoD Components, while reducing organizational inefficiencies and system authorization costs. However, not leveraging reciprocity can result in wasted resources and delayed system deployment. For this report, we determined whether DoD Components leveraged reciprocity by reviewing their actions for:

- (U) making systems and authorization documentation available in eMASS for other DoD Components to review and use;
- (U) appointing eMASS reciprocity users to review existing systems and authorization documentation within eMASS, previously completed by other DoD Components; and
- (U) identifying and authorizing common controls to be used by all systems within the component.

(U) Making Systems and Authorization Documentation Available in eMASS

(U) The DoD CIO is responsible for developing the DoD's cybersecurity policy and assigning responsibilities for executing and maintaining the RMF. In October 2014, the DoD CIO established the RMF Technical Advisory Group (TAG) to provide implementation guidance and facilitate the execution of RMF. The RMF TAG guidance is compiled in the RMF Knowledge Service web portal. In addition, the DoD CIO partnered with the Defense Information Systems Agency (DISA) to co-sponsor development of the eMASS repository to facilitate information sharing. In August 2019, the DoD CIO required that DoD Components using commercial solutions to manage their cybersecurity risk to make all cybersecurity authorization documentation available in eMASS for other DoD Components seeking to utilize reciprocity.[10]

(U) To promote information sharing between DoD Components, the eMASS configuration control board proposed changes to the eMASS system registration process in February 2017.[11] As a result, in December 2017, a function was added to the registration process, which automatically designated systems

[9] (U) DoD Chief Information Officer Memorandum, "Cybersecurity Reciprocity," October 18, 2016.

[10] (U) DoD CIO Memorandum, "Component Use of the Enterprise Mission Assurance Support Service," August 12, 2019.

[11] (U) A configuration control board is a group responsible for controlling and approving changes made to a system.

(U) as a "reciprocity system." However, the DoD CIO also identified exemptions allowing DoD Components to de-select the designation as a reciprocity system if the system was classified or was being decommissioned.

(U) Appointing eMASS Reciprocity Users

(U) In 2017, the RMF TAG, through the RMF Knowledge Service web portal, provided DoD Components guidance for appointing eMASS "reciprocity users." RMF TAG guidance states that eMASS reciprocity users may be appointed by DoD Component cybersecurity officials, such as Security Control Assessors, authorizing officials, Chief Information Security Officers, or CIOs. eMASS reciprocity users have read only access to authorization documentation for all DoD systems registered in eMASS and are responsible for searching all systems, previously selected by a Component as reciprocity systems, by name or acronym to identify applicable systems and obtain the associated authorization documentation for review. The eMASS reciprocity user capability enables the identification of reciprocity systems. Once identified, DoD cybersecurity personnel can reuse previously assessed information technology, increasing speed and agility of system deployments, and reducing costs associated with authorization efforts.

(U) Identifying and Authorizing Common Controls

(U) The foundation of the RMF process is the identification, documentation, and authorization of organization-wide common controls that may be used as a form of reciprocity. When applied, common controls eliminate redundant system testing, which allows reusing previously approved authorization documentation for multiple systems within an organization. NIST Special Publication 800-37 requires common controls be authorized based on a determination that the risk to operations and assets, individuals, other organizations, and the Nation is acceptable. Common controls enable deployment of enterprise-wide cybersecurity solutions, which significantly reduce the number of controls that need to be implemented and assessed at the information system level.

(U) Federal and DoD guidance on RMF implementation established a three-tiered approach for DoD Components to manage common controls.[12] The DoD CIO, DoD Component CIOs, and authorizing officials all have responsibilities for identifying common controls.

[12] (U) NIST Special Publication 800-37 and the DoD RMF Knowledge Service web portal.

(U) TIER 1 (Organization)

(U) The DoD CIO identifies common controls addressed by existing DoD policy and guidance, and are applicable throughout the DoD. The DoD CIO identified 27 common controls determined compliant through existing DoD policy. DoD Components assume the risk associated with Tier 1 common controls through their Component's concurrence with DoD policy. For example, the DoD CIO identified the Incident Response Policy and Procedures control (IR-1) as a Tier 1 common control that addresses the establishment of policy and procedures for effective implementation of incidence response controls. DoD Components are automatically compliant with this control because they are covered by existing DoD policies. These 27 common controls are listed in the RMF Knowledge Service web portal.

(U) TIER 2 (Mission and Business Process)

(U) The DoD Component CIOs identify Component-specific common controls addressed by existing Component policy and guidance. DoD policy requires DoD Components to identify and approve Tier 2 common controls to be used by the DoD Component's systems, when applicable. For example, the Air Force's common controls packages include Access Controls (CA-1) determined to be compliant through existing Air Force policy.[13]

(U) TIER 3 (Information System)

(U) Enclaves or hosting facilities may identify common controls including physical, environmental, and network security protections that are made available to information systems hosted within the enclave or hosted within the data center. For example, systems hosted within a data center will use physical, environmental and network security protections common controls established for that data center, such as door locks, guards, temperature controls, and network boundary security.

(U) For this audit, we focused on the DoD Components' identification and authorization of Tier 2 common controls because these controls apply to all systems authorized within an organization.

[13] (U) CA-1 is a security control within NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," December 10, 2020, that the Air Force determined is automatically compliant through Air Force Instruction 17-101, "Risk Management Framework for Air Force Information Technology," February 6, 2020.

(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.[14] We identified internal control weaknesses related to leveraging reciprocity when authorizing information systems through the RMF process. Specifically, DoD Components did not make system information and authorization documentation available for reciprocity, appoint eMASS reciprocity users, and consistently authorize Tier 2 common controls. We will provide a copy of the report to the senior official at the DoD CIO, U.S. Transportation Command (USTRANSCOM), Defense Health Agency (DHA), Defense Logistics Agency (DLA), and Defense Human Resources Activity (DHRA) who is responsible for internal controls.

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

(U) Finding

(U) The DLA and DHRA Did Not Consistently Leverage Reciprocity

(U) USTRANSCOM and the DHA leveraged reciprocity while authorizing their systems through the RMF process by making their systems and authorization documentation available in eMASS, appointing eMASS reciprocity users, and authorizing Tier 2 common controls in accordance with Federal and DoD guidance; however, the DLA and DHRA did not.[15] Specifically:

- (U) DLA cybersecurity officials did not make their systems and authorization documentation available in eMASS for reciprocity across the DoD. In addition, they did not appoint eMASS reciprocity users to obtain and review existing systems and authorization documentation. This occurred because they believed their systems had unique missions, and were relevant only to DLA personnel. Therefore, DLA cybersecurity officials incorrectly determined their systems were not subject to DoD reciprocity requirements.
- (U) DLA cybersecurity officials did not authorize all Tier 2 common controls to be used by DLA systems because they did not consider the DoD's RMF and reciprocity policy and implementation guidance to be a priority.
- (U) DHRA cybersecurity officials also did not appoint eMASS reciprocity users to obtain and review existing systems and authorization documentation, and identify and authorize all Tier 2 common controls to be used by DHRA systems because the DHRA was undergoing a reorganization, and the DHRA Director had yet to assign and document cybersecurity roles and responsibilities for implementing RMF and reciprocity requirements.

(U) In addition, the DoD CIO did not implement processes necessary to oversee DoD Components' compliance with DoD reciprocity guidance when authorizing systems through the RMF process, as required by DoD guidance. Instead, the DoD CIO relied on DoD Components to manage the system authorization process and use reciprocity to maximize reuse of testing and assessments results developed for prior system authorizations.

[15] (U) NIST Special Publication 800-37 and DoD Instruction 8510.01.

~~(CUI)~~ The DoD's requirement to leverage reciprocity enables the DoD to rapidly deliver secure systems to DoD Components while reducing organizational inefficiencies and system authorization costs. Unless DoD Components fully leverage RMF reciprocity, the associated benefits may not be fully realized, including faster deployment of secure systems and cost savings. [redacted]

~~(CUI)~~ [redacted] The DoD could achieve even greater cost savings and efficiencies if all DoD Components used reciprocity when authorizing their systems through RMF. DoD Components can increase reciprocity by making systems and authorization documentation available to other DoD Components in eMASS, appointing eMASS reciprocity users, and identifying and authorizing common controls.

(U) USTRANSCOM and the DHA Leveraged Reciprocity When Authorizing Their Systems

~~(CUI)~~ USTRANSCOM and the DHA leveraged reciprocity when authorizing [redacted] through the RMF process.[18] Specifically, USTRANSCOM and DHA cybersecurity officials made their systems and authorization documentation available in eMASS, appointed reciprocity users, and authorized Tier 2 common controls to be used by their Component's systems as required by NIST Special Publication 800-37 and DoD Instruction 8510.01.

16 (U) Public Law 116-283, "William M (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021," January 1, 2021, repealed the position of the Chief Management Officer of the Department of Defense.

17 (U) CAPE conducts cost estimates and analysis of acquisition programs for the Secretary of Defense and other senior officials.

18 (U) Number of USTRANSCOM and DHA systems based on systems registered in eMASS with an ATO as of February 9, 2021.

(U) The DLA and DHRA Did Not Consistently Leverage Reciprocity When Authorizing Their Systems

~~(CUI)~~ The DLA and DHRA did not consistently leverage reciprocity when authorizing their systems through the RMF process. Specifically, DLA cybersecurity officials did not make systems and authorization documentation available in eMASS for [redacted] appoint eMASS reciprocity users, and authorize Tier 2 common controls to be used by DLA's systems. Although DHRA cybersecurity officials made systems and authorization documentation available in eMASS for [redacted] DHRA cybersecurity officials did not appoint any eMASS reciprocity users, and did not authorize Tier 2 common controls to be used by the DHRA's systems.[19]

(U) The DLA Did Not Make Its Systems and Documentation Available in eMASS for Reciprocity

~~(CUI)~~ DLA cybersecurity officials did not make their systems and authorization documentation available in eMASS for reciprocity across the DoD for any of [redacted] The DoD CIO guidance requires DoD Components to make their systems and authorization documentation available in eMASS to allow other DoD Components to leverage reciprocity.[20] To identify whether the DLA made its systems and authorization documentation available, we analyzed a list of DoD systems registered in eMASS, provided by the eMASS Program Office, to determine whether DLA systems were marked as reciprocity systems.

~~(CUI)~~ We determined that DLA cybersecurity personnel did not mark any of their systems as reciprocity systems during the eMASS registration process, which prevented other DoD Components' eMASS reciprocity users from viewing the DLA's systems and authorization documentation. According to DLA cybersecurity officials, [redacted] met the DoD CIO exemption criteria and the authorization documentation should have been shared in eMASS.

(U) DLA cybersecurity officials stated that they did not make any systems and authorization documentation available for other DoD Components because the DLA's systems were only relevant for use by DLA personnel and were created for unique missions. Therefore, other DoD Components could not access and review DLA testing and assessments performed for DLA systems. DLA officials took action to address this issue during the audit. See the "Management Actions Taken" section in this report for additional information.

[19] (U) Number of DLA and DHRA systems based on systems registered in eMASS with an ATO as of February 9, 2021.

[20] (U) The RMF implementation guidance includes eMASS system registration business rules that require DoD Components to make their systems and authorization documentation available in eMASS for reciprocity.

(U) The DLA and DHRA Did Not Appoint eMASS Reciprocity Users

(U) DLA and DHRA cybersecurity officials did not appoint eMASS reciprocity users to review existing systems and authorization documentation previously completed by other DoD Components as part of the RMF process. The DoD CIO developed the eMASS reciprocity user role in eMASS for DoD Components to maximize the reuse of existing authorization documentation such as system security plans, risk assessments, and testing and assessment results required by the 2016 DoD CIO reciprocity memorandum. eMASS reciprocity users can identify and obtain systems and authorization documentation in eMASS from other DoD Components. To identify whether DLA and DHRA cybersecurity officials appointed eMASS reciprocity users, we analyzed a list of each DoD Component's appointed eMASS reciprocity users, provided by the eMASS Program Office, and requested appointment memorandums supporting those appointments.

(U) We determined that DLA cybersecurity officials did not appoint eMASS reciprocity users because DLA cybersecurity officials considered their systems to have unique missions. Therefore, they believed eMASS reciprocity users were not necessary. We also determined that the DHRA did not appoint any eMASS reciprocity users because the DHRA was undergoing a reorganization, and the DHRA Director had not defined roles and responsibilities for implementing the DoD CIO's RMF and reciprocity requirements.

(U) Without eMASS reciprocity users, DoD Components would not have visibility through eMASS of similar systems previously authorized by another organization. DLA and DHRA officials took action to address this issue during the audit. See the "Management Actions Taken" section in this report for additional information.

(U) The DLA and DHRA Did Not Authorize Tier 2 Common Controls

(U) DLA and DHRA cybersecurity officials did not authorize Tier 2 common controls for use by the DLA and DHRA's respective systems. NIST Special Publication 800-37 and DoD Instruction 8510.01 require all DoD Components to identify and authorize Tier 2 common controls. To determine whether the DLA and DHRA authorized Tier 2 common controls, we interviewed DLA and DHRA cybersecurity personnel to obtain the system name for any common

(U) controls packages used by each DoD Component. In addition, we used eMASS to identify each system using the name provided and analyzed the named systems' security plans, plan of action and milestones, control test results, and other authorization documentation associated with DLA and DHRA Tier 2 common control packages.[21]

(U) We determined that although DLA cybersecurity officials identified Tier 2 common controls for use by DLA systems, those Tier 2 common controls were not authorized through a documented ATO. When asked why the authorization of common controls were not documented in the ATO, DLA officials stated that there was no requirement to authorize their Tier 2 common controls. However, we informed DLA officials that Federal and DoD guidance require DoD Components to authorize Tier 2 common controls as part of the RMF process. DLA officials took action to address this issue during the audit. See the "Management Actions Taken" section of this report for additional information.

(U) We also determined that the Defense Manpower Data Center, a subcomponent of the DHRA, did not identify and authorize Tier 2 common controls applicable to all of its systems because the DHRA was undergoing a reorganization, which started in March 2019, and the DHRA Director had yet to assign and document cybersecurity roles and responsibilities for RMF and reciprocity. DHRA officials took action to address this issue during the audit. See the "Management Actions Taken" section of this report for additional information.

(U) Without identifying Tier 2 common controls, DoD Components could have unnecessarily expended resources when authorizing systems, and delayed system deployment while ensuring compliance with RMF requirements.

(U) The DoD CIO Did Not Ensure DoD Components Consistently Implemented Reciprocity When Authorizing Their Systems

(U) The DoD CIO did not implement processes necessary to oversee DoD Components' compliance with DoD reciprocity guidance when authorizing systems through the RMF process. DoD Instruction 8510.01 requires the DoD CIO to oversee the DoD's implementation of the RMF process, including the use of reciprocity. Although the DoD CIO facilitated periodic meetings with RMF stakeholders and disseminated guidance, the DoD CIO did not verify whether DoD Components made their systems and authorization documentation available for reciprocity in eMASS. In addition, the DoD CIO did not require system program

[21] (U) A plan of action and milestones is a document that identifies tasks and resources required to accomplish the elements of a plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

(U) managers to validate whether they considered reciprocity when authorizing systems. Instead, the DoD CIO relied on DoD Components to manage the system authorization process and use reciprocity to maximize reuse of testing and assessment results developed by prior system authorizations.

~~(CUI)~~ We identified seven DoD Components that did not [redacted] as reciprocity systems in eMASS despite those systems having ATOs. For example, we confirmed that DLA cybersecurity officials unchecked the reciprocity system box in eMASS, which prevented other DoD Components from viewing and obtaining system [redacted] authorized by the DLA although none of those systems met the DoD CIO's exemption criteria.[22] According to the DoD CIO RMF Implementation Chief, DoD Components were responsible for sharing authorization documentation in eMASS, and the Office of the DoD CIO could not efficiently verify compliance with information sharing requirements under the current eMASS configuration. The DoD CIO RMF Implementation Chief stated that he was coordinating updates to eMASS with the eMASS Program Office that would require DoD Component system program managers to select at least one of the approved justifications to exclude a system from reciprocity sharing. When completed, this action should minimize system program managers arbitrarily making their systems unavailable for reciprocity in eMASS.

(U) In addition, the DoD CIO did not require system program managers to validate whether they considered reciprocity when authorizing systems. The DoD CIO RMF Implementation Chief stated that the October 2016 guidance did not require DoD Components to certify whether system program managers considered reciprocity before authorizing systems, but the Chief acknowledged an additional control, to ensure reciprocity was considered, would be a good practice to avoid additional testing and assessments as part of the RMF process.[23]

(U) The reports issued by the AAA, NAS, and AFAA on RMF reciprocity further support the need for the DoD CIO to take action. The AAA report had one finding and six recommendations for the Army that focused on the use of common controls throughout the Army. The NAS report had two findings and five recommendations for the Navy and Marine Corps, one of which focused on aligning Marine Corps guidance with DoD Instruction 8510.01 to include the identification of Tier 2 common controls to be used when authorizing systems across the Marine Corps. The AFAA report did not have findings and recommendations as the AFAA found

[22] (U) DoD Components may de-select the designation as a reciprocity system if a system is classified or is being decommissioned.

[23] (U) DoD Chief Information Officer Memorandum, "Cybersecurity Reciprocity," October 18, 2016.

(U) that Air Force cybersecurity personnel successfully reduced redundant testing and assessment efforts by using five common controls packages when authorizing Air Force systems through the RMF process.

(U) The reports issued by the AAA, NAS, and AFAA provide insight regarding the challenges these Military Services faced when implementing reciprocity, and lessons learned for implementing the other recommendations in this report.

(U) RMF Reciprocity Benefits May Not Be Fully Realized

(U) The DoD's requirement to leverage reciprocity enables the DoD to rapidly deliver secure systems to DoD Components while reducing organizational inefficiencies and system authorization costs. Unless DoD Components fully leverage RMF reciprocity, the associated benefits may not be fully realized, including time, cost savings, and eliminating redundancies.

~~(CUI)~~ [redacted] The DoD could achieve even greater cost savings and efficiencies if all DoD Components used reciprocity when authorizing their systems through the RMF process.[25] DoD Components can increase reciprocity by making systems and authorization documentation available to other DoD Components in eMASS, appointing eMASS reciprocity users, and identifying and authorizing common controls.

(U) Management Actions Taken

~~(CUI)~~ During the audit, DLA and DHRA cybersecurity officials took corrective actions to leverage reciprocity through the RMF process. Specifically, DLA cybersecurity officials made their systems and authorization documentation available in eMASS for other DoD Components to review. We verified that, as of April 8, 2021, systems and authorization documentation for [redacted] was available for other DoD Components to review in eMASS.

[24] (U) The Fourth Estate includes all components in the DoD that are not part of the military or a combatant command.

[25] ~~(CUI)~~ As of August 2021, eMASS contained security assessment information for [redacted]

(U) The DLA also appointed eMASS reciprocity users to review existing systems and authorization documentation, and authorized Tier 2 common controls for use by all DLA systems. We verified that the DLA Security Control Assessor (Cybersecurity Management Services Director) appointed three eMASS reciprocity users in writing on April 21, 2020. We also verified that on January 8, 2021, the DLA Authorizing Official approved the DLA Tier 2 common controls package.

(U) Furthermore, the DHRA appointed eMASS reciprocity users to review existing systems and authorization documentation, and authorized Tier 2 common controls for use by all DHRA systems. We verified that on September 14, 2020, the DHRA Security Control Assessor (Cybersecurity Division Director) appointed eight eMASS reciprocity users in writing. We also verified that on May 14, 2021, the DHRA Authorizing Official approved the DHRA Tier 2 common controls package. Additionally, DHRA cybersecurity officials developed and disseminated six standard operating procedures defining roles and responsibilities, and steps necessary to authorize the DHRA systems through the RMF process.

(U) We consider the actions taken by DLA and DHRA cybersecurity officials sufficient to address these issues identified during this audit. Therefore, we wil not issue recommendations in this report for the DLA or DHRA.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

(U) We recommend that the DoD Chief Information Officer, in coordination with the Enterprise Mission Assurance Support Service Program Manager, update the Enterprise Mission Assurance Support Service system registration process to require DoD Component system program managers to select a valid justification for exemption when a system is not made available for reciprocity use.

(U) Principal Director to the Deputy CIO for Resources and Analysis, Performing the Duties of the DoD CIO Comments

(U) The Principal Director to the Deputy CIO for Resources and Analysis, Performing the Duties of the DoD CIO, agreed, stating that the DoD CIO, in coordination with the eMASS Program Manager, would update the eMASS system registration process to require DoD Component system program managers to select a valid justification when not making a system available for reciprocity use.

(U) The Principal Director also stated that the DoD CIO would ensure DoD Component information outside of eMASS was also made available for reciprocity when DoD Components did not use eMASS. The Principal Director added that the DoD CIO plan to complete the actions by the end of the second quarter of FY 2022.

(U) Our Response

(U) Comments from the Principal Director to the Deputy CIO for Resources and Analysis, Performing the Duties of the DoD CIO, addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once we verify that the eMASS system registration process is updated and that DoD Components not using eMASS have a process in place for sharing their reciprocity information.

(U) Recommendation 2

(U) We recommend that the DoD Chief Information Officer revise existing guidance or issue new guidance that requires system program managers to certify that reciprocity was considered before authorizing and reauthorizing systems.

(U) Principal Director to the Deputy CIO for Resources and Analysis, Performing the Duties of the DoD CIO Comments

(U) The Principal Director to the Deputy CIO for Resources and Analysis, Performing the Duties of the DoD CIO, agreed, stating that the DoD CIO would revise guidance or issue new guidance to require system program managers to certify that reciprocity was considered before authorizing and reauthorizing systems. The Principal Director added that the DoD CIO plans to complete the action by the end of the second quarter of FY 2022.

(U) Our Response

(U) Comments from the Principal Director to the Deputy CIO for Resources and Analysis, Performing the Duties of the DoD CIO, addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once we verify that guidance is issued requiring system program managers to certify that reciprocity was considered before authorizing and reauthorizing systems.

(U) Recommendation 3

(U) We recommend that the DoD Chief Information Officer, Risk Management Framework Implementation Chief, and the Risk Management Framework Technical Advisory Group review the Army Audit Agency, Naval Audit Service, and Air Force Audit Agency reports on reciprocity, and discuss the findings and actions taken by each Military Service at a Risk Management Framework Technical Advisory Group meeting.

(U) Principal Director to the Deputy CIO for Resources and Analysis, Performing the Duties of the DoD CIO Comments

(U) The Principal Director to the Deputy CIO for Resources and Analysis, Performing the Duties of the DoD CIO, agreed, stating that the RMF Implementation Chief and the RMF TAG would review the AAA, NAS, and AFAA reports on reciprocity, and discuss the findings and actions taken by each Military Department at an RMF TAG meeting. The Principal Director added that the DoD CIO plans to complete these actions by the end of the second quarter of FY 2022.

(U) Our Response

(U) Comments from the Principal Director to the Deputy CIO for Resources and Analysis, Performing the Duties of the DoD CIO, addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once we verify that the AAA, NAS, and AFAA reciprocity report findings and Military Department actions taken were discussed at an RMF TAG meeting.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from August 2018 through September 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

(U) Although we initially announced the audit in August 2018, the coronavirus disease-2019 pandemic resulted in suspending the audit. On January 21, 2021, we reannounced this audit, with the same audit objectives.

(U) We reviewed Federal and DoD Component-level guidance to understand requirements for implementing RMF and reciprocity. To understand the process for authorizing systems through RMF and system registration efforts, we met with officials from the following offices and support elements.

- (U) DoD CIO, RMF TAG; Alexandria, Virginia
- (U) Headquarters, DLA; Fort Belvoir, Virginia
- (U) Troop Support, DLA; Philadelphia, Pennsylvania
- (U) Headquarters, DHRA; Alexandria, Virginia
- (U) Headquarters, DHA; Falls Church, Virginia
- (U) DMDC Cybersecurity Division; Seaside, California
- (U) DISA Cybersecurity Division; Letterkenny Army Depot, Pennsylvania
- (U) Headquarters, USTRANSCOM; Scott Air Force Base, Illinois

(U) We interviewed officials from the Offices of the DoD CIO, USTRANSCOM, DHA, DLA, and DHRA responsible for managing information technology portfolios to determine whether DoD Components leveraged cybersecurity reciprocity to reduce redundant testing and assessments when authorizing information technology through the RMF process. We also interviewed officials from the Office of the Secretary of Defense, CAPE to identify cost assessments performed concerning the use of RMF throughout the DoD.

(U) We analyzed system security plans, ATO materials, and other system authorization documentation to determine whether USTRANSCOM, DHA, DLA, and DHRA authorized Tier 2 common controls packages. We also obtained and reviewed eMASS reciprocity user appointment memorandums, and when appointed, interviewed those users to determine their understanding of their roles and responsibilities. Additionally, we accessed eMASS to determine whether USTRANSCOM, the DHA, the DLA, and the DHRA made their systems' authorization documentation available to other DoD Components to support reciprocity requirements. We interviewed cybersecurity officials such as Cybersecurity Divisions Chiefs and Deputy Chiefs, Information Systems Security Managers, and Information Technology Specialists to determine their justifications if their systems were not made available for reciprocity.

(U) This report was reviewed by the DoD Components associated with this oversight project to identify whether any of their reported information, including legacy FOUO information, should be safeguarded and marked in accordance with the DoD CUI Program, established in DoD Instruction 5200.48.[26] In preparing and marking this report, we considered any comments submitted by the DoD Components about the CUI treatment of their information. If the DoD Components failed to provide any or sufficient comments about the CUI treatment of their information, we marked the report based on our assessment of the available information.

(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 internal controls related to DoD Components making system information and authorization documentation available for reciprocity, appointing eMASS reciprocity users, and identifying and authorizing Tier 2 common controls. 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 used computer-processed data from eMASS to identify whether DoD Components made system information and authorization documentation available to other DoD Components to implement reciprocity. Additionally, we used data from eMASS to determine whether DoD Components identified and authorized Tier 2 common controls packages applicable to the selected DoD Components' systems.

[26] (U) DoD Instruction 52000.48, "Controlled Unclassified Information," March 6, 2020.

(U) We also obtained a list of all systems registered in eMASS, as of February 9, 2021, from DISA. We used this list to identify the number of systems the selected DoD.

(U) Components registered in eMASS with ATOs. We assessed the reliability of the data through discussions with DoD Components' cybersecurity personnel, and cross-referencing information in the list with documentation received from other audited entities. We determined that the data were reliable to verify that system and authorization documentation was available in eMASS and DoD Components identified and authorized Tier 2 common controls.

(U) Prior Coverage

(U) During the last 5 years, the DoD Office of Inspector General (OIG), AAA, and AFAA issued four reports discussing the implementation of RMF for systems; the categorization of systems and selection of security controls to implement the RMF; and the use of DoD Information Technology System Repositories. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/reports.html/. Unrestricted AAA reports can be accessed at http://www.aaa.army.mil. Unrestricted AFAA reports can be accessed from https://www.afaa.af.mil/ by clicking on Freedom of Information Act Reading Room and then selecting audit reports.

(U) DoD OIG

(U) Report No. DODIG-2018-154, "DoD Information Technology System Repositories," September 24, 2018

> (U) The DoD OIG determined that the DoD did not accurately report or complete system information in the SECRET Internet Protocol Router Network Information Technology Registry. In addition, the DoD OIG determined that the DoD maintained similar information technology data in multiple repositories including the eMASS, Xacta, and Archer.

(U) AAA

(U) Report No. A-2019-0013-IET, "Risk Management Framework for Systems with Authorization Termination Dates," November 8, 2018

(U) The AAA determined that the Army did not have sufficient processes to successfully implement the RMF. Furthermore, not all systems reviewed had evidence of information mapping or acceptable continuous monitoring strategies. The audit also determined that the Army did not have evidence of approved security plans to provide assurance for the Army that inherited common controls were developed to avoid testing and evaluating more security controls than required.

(U) AFAA

(U) Report No. F2017-0009-O10000, "Financial Systems Authority to Operate," September 20, 2017

(U) The AFAA determined that Air Force personnel did not manage the ATO process as required for the financial and financial feeder systems material to the Air Force's financial statements. Specifically, the Air Force's authorizing officials allowed 21 percent of their financial and financial feeder systems to operate on the Air Force networks without current ATOs. On average, those systems were connected to the network for over 110 days.

(U) Report No. F2017-0004-O10000, "Risk Management Framework Implementation – Financial Systems," May 15, 2017

(U) The AFAA determined that the Secretary of the Air Force/CIO A6 personnel did not implement the RMF on financial systems critical to implement the Financial Improvement and Audit Readiness initiative. Specifically, Air Force information system owners did not properly categorize and select security controls for their financial systems.

(U) Appendix B

(U) Army, Navy, and Air Force Audit Agencies Reports on Reciprocity

(U) The AAA, NAS, and AFAA issued reports discussing the implementation of reciprocity to reduce redundant test and assessment efforts while authorizing systems through the RMF process. The following are summaries of AAA, NAS, and AFAA reports concerning the use of reciprocity within their respective Military Departments. The summaries describe the report findings, recommendations, and the status of the recommendations.

(U) AAA

(U) Report No. A-2019-0120-AXZ, "Inheriting Common Controls Within the Risk Management Framework," September 30, 2019

~~(CUI)~~ [redacted]

(U) The AAA reported that the Army did not fully leverage common controls because Army guidance did not clearly address the requirement to use inheritance. Furthermore, the Army did not have readily available inheritance implementation processes and procedures in RMF training, or incorporate a user's guide to help activities with inheritance efforts. In addition, the Army did not develop and implement a standardized format for naming and structuring critical artifacts to maximize use of common controls and allow auditability in eMASS.

[27] ~~(CUI)~~ As of October 24, 2018, the Army [redacted] registered in eMASS with an ATO.

(U) To address the weaknesses identified during the audit, AAA issued five recommendations to the Army CIO. The AAA closed all of the recommendations made to the Army. The following are the issues identified and the Army CIO's actions taken:

- (U) Develop Army guidance that requires establishing and using common controls packages under RMF. In response, the Army CIO reviewed guidance and implemented Tier 2 common controls packages.
- (U) Update Army guidance to align the different tier-level controls with DoD guidance. In response, the Army CIO updated Army regulation to align with DoD guidance and published the revised regulation in the first quarter of FY 2020.
- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted]

(U) NAS

(U) Report No. N2020-0019, "Department of the Navy's Use of Cybersecurity Reciprocity Within the Risk Management Framework Process," April 9, 2020

(U) The NAS determined whether Navy commands leveraged reciprocity to reduce redundant testing and assessment efforts for information technology authorized within the RMF process. In addition, the NAS determined whether the Navy and Marine Corps established common controls packages and used them to authorize systems through RMF. The NAS identified that Department of Navy activities leveraged reciprocity to reduce redundant testing and assessment efforts, but lacked assurance that four systems authorized using reciprocity were operating with the appropriate level of security. The NAS reported that the Navy and Marine Corps lacked assurance regarding the

(U) four systems because Navy and Marine Corps personnel accepted these systems without establishing a documented agreement assigning roles and responsibilities for maintenance and monitoring the systems' security posture.

(U) In addition, the NAS determined that the Marine Corps had diminished capability to support reciprocity because it did not align RMF activities with DoD Instruction 8510.01, and did not require RMF practitioners to identify Tier 2 common controls. Furthermore, the NAS determined that the Marine Corps used the Marine Corps Compliance and Authorization Support Tool to implement common controls instead of eMASS. The NAS reported that although the Marine Corps Compliance and Authorization Support Tool can be used to track RMF compliance within the Marine Corps, it may hinder reciprocity because other DoD Components did not have access to that information.

(U) To address the weaknesses identified in the audit, NAS issued five recommendations to the Naval Information Warfare Systems Command Commander and the Commandant of the Marine Corps. The NAS closed all recommendations to the Naval Information Warfare Systems Command Commander; however, recommendations to the Commandant of the Marine Corps remain open while awaiting completion of agreed upon actions. The following are the weaknesses identified and the recommendations to the Naval Information Warfare Systems Command Commander and the Commandant of the Marine Corps:

(U) Naval Information Warfare Systems Command Commander

- (U) Develop and implement a documented agreement with the Marine Corps for maintaining and monitoring systems authorized using reciprocity, and establish internal controls to ensure that an agreement between receiving and deploying agencies exists for assigning roles and responsibilities to maintain and monitor the security posture of the systems. In response, the Naval Information Warfare Systems Command Commander developed an agreement with the Marine Corps for maintaining and monitoring the security posture of systems authorized through reciprocity and developed a template to guide future agreements between the Navy and other Components authorizing systems using reciprocity.

(U) Commandant of the Marine Corps

- (U) Develop and implement a documented agreement with the Naval Information Warfare Systems Command for maintaining and monitoring systems authorized using reciprocity. In response, the Commandant of the Marine Corps agreed to update a memorandum of understanding to reflect the current system operating environment and assign personnel responsibility for maintaining and monitoring systems authorized using reciprocity as well as Marine Corps guidance to require written agreements between authorizing officials when authorizing systems using reciprocity.
- (U) Revise Marine Corps Enterprise Cybersecurity Manual 018 to align with DoD Instruction 8510.01 requirements for categorizing systems by information types, identifying Tier 2 common controls, and developing and implementing documented agreement between the Marine Corps and agencies authorizing systems through reciprocity. In response, the Commandant of the Marine Corps agreed to update Marine Corps Enterprise Cybersecurity Manual 018 to address the issues identified.

(U) AFAA

(U) Report No. F2019-0007-O10000, "Risk Management Framework Tests and Assessments," August 13, 2019

~~(CUI)~~ The AFAA determined whether the Air Force reduced cybersecurity testing and assessment efforts through the RMF process. The AFAA [redacted] ATOs, registered in eMASS as of April 1, 2019. The AFAA determined whether the Air Force established common controls packages and used them to authorize its systems through RMF. The AFAA determined that Air Force personnel used the RMF process and inheritance to reduce cybersecurity testing and assessments. Specifically, the AFAA reported that Air Force systems inherited 21,936 [redacted] reviewed. AFAA reported that the Air Force reviewed, assessed, and created five common controls packages to allow inheritance of Air Force and DoD policies in eMASS, and continuously monitored the common controls packages for updates, testing results, and policy changes. For example, personnel included and updated testing and assessment results for each of the 21,936 common controls in eMASS. According to AFAA, using the RMF process and inheritance saved Air Force personnel more than 10,000 hours during system authorizations by inheriting 21,936 common controls. The AFAA did not identify issues requiring corrective action and, therefore, did not issue any recommendations.

(U) Management Comments

(U) Office of the DoD Chief Information Officer

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

OCT - 5 2021

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Review and Comment of DoD Inspector General "DoD's Use of Cybersecurity Reciprocity within the Risk Management Framework Process" (D2018-D000CS-0199.000) Draft Report

This is the Department of Defense (DoD) Chief Information Officer (CIO) response to the DoD Inspector General Report, Audit of "DoD's Use of Cybersecurity Reciprocity within the Risk Management Framework Process" (D2018- D000CS-0199.000).

DoD IG RECOMMENDATION 1: We recommend that the Department of Defense Chief Information Officer (DoD CIO), in coordination with the Enterprise Mission Assurance Support Service (eMASS) Program Manager (PM), update the eMASS system registration process to require DoD Component system PMs to select a valid justification for exemption when a system is not made available for reciprocity use.

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

The DoD CIO, in coordination with the eMASS PM, will update the eMASS system registration process to require DoD Component system PMs to select a valid justification for exemption when a system is not made available for reciprocity use. As not all DoD Components use eMASS, DoD CIO will ensure Component information outside of eMASS is available for reciprocity search as well. EDC end of Q2FY22.

DoD IG RECOMMENDATION 2: We recommend that the Department of Defense Chief Information Officer (DoD CIO) revise existing guidance or issue new guidance that requires system PMs to certify that reciprocity was considered before authorizing and reauthorizing systems.

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

The DoD CIO will revise existing guidance or issue new guidance that requires system PMs to certify that reciprocity was considered before authorizing and reauthorizing systems. EDC end of Q2FY22.

DoD IG RECOMMENDATION 3: We recommend that the Department of Defense Chief Information Officer (DoD CIO), Risk Management Framework Implementation Chief, and the Risk Management Framework Technical Advisory Group review the Army Audit Agency, Naval Audit Service, and Air Force Audit Agency reports on reciprocity, and discuss the findings and actions taken by each Military Service at a Risk Management Framework Technical Advisory Group meeting.

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

(U) Office of the DoD Chief Information Officer (cont'd)

The DoD CIO, Risk Management Framework Implementation Chief, and the Risk Management Framework Technical Advisory Group will review the Army Audit Agency, Naval Audit Service, and Air Force Audit Agency reports on reciprocity, and discuss the findings and actions taken by each Military Department at a Risk Management Framework Technical Advisory Group meeting. EDC end of Q2FY22.

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

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

Dr. Kelly E. Fletcher
Performing the Duties of the Chief Information Officer
of the Department of Defense

2

(U) Acronyms and Abbreviations

AAA	U.S. Army Audit Agency
AFAA	Air Force Audit Agency
ATO	Authorization to Operate
CAPE	Cost Assessment and Program Evaluation
CIO	Chief Information Officer
DHA	Defense Health Agency
DHRA	Defense Human Resources Activity
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DODIN	DoD Information Network
eMASS	Enterprise Mission Assurance Support Service
NAS	Naval Audit Service
NIST	National Institute of Standards and Technology
RMF	Risk Management Framework
RMF TAG	Risk Management Framework Technical Advisory Group
USTRANSCOM	U.S. Transportation Command

(U) Glossary

(U) Authorization to Operate (ATO). 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) Baseline Controls. Minimum security controls that are defined for a low-impact, moderate-impact, or high-impact categorized information system. These controls provide a starting point for the tailoring process.

(U) Common Controls. Security controls that can be inherited by one or more organizational information systems.

(U) Enterprise Mission Assurance Support Service (eMASS). A web-based application that supports cybersecurity program management. eMASS allows users to track system authorizations, associated documentation, compliance status for security controls, and assessment procedures.

(U) eMASS Reciprocity User. eMASS users with "view only" access to system information, security control assessments, plan of actions and milestones, implementation plans, risk assessment reports, and artifacts for all systems identified as reciprocity systems in eMASS.

(U) Inheritance. A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides.

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

(U) Reciprocity. Mutual agreement among participating enterprises to accept each other's security assessments to reuse information system resources and accept each other's assessed security posture to share information.

(U) Risk Management Framework (RMF). Provides a disciplined and structured process that combines information system security and risk management activities into the system development lifecycle. The process consists of seven steps: prepare for RMF activities, categorize system; select security controls; implement security controls; assess security controls; authorize system, and monitor security controls. The RMF applies to all DoD information technology that receives, processes, stores, displays, or transmits DoD information.

(U) Risk Management Framework (RMF) Technical Advisory Group (TAG). Provides implementation guidance for the RMF by collaborating with the DoD components cybersecurity programs, cybersecurity communities of interest, and other entities to address issues that are common across all entities. The RMF TAG makes its detailed analysis and RMF implementation guidance available through the RMF Knowledge Service web portal.

(U) Tier 1 Common Controls. Security controls identified by the DoD CIO and addressed based on existing DoD policy and guidance and applicable throughout the DoD. For example, the DoD CIO identified the Incident Response Policy and Procedures control (IR-1) as a Tier 1 common control that addresses the establishment of policy and procedures for effective implementation of incidence response controls. DoD Components are automatically compliant with this control because they are covered by existing DoD policies.

(U) Tier 2 Common Controls. Security controls identified by the DoD Component CIO as component-specific security controls, addressed by existing component policy and guidance, and applicable throughout the Component. For example, the Air Force's common controls packages include Access Controls (CA-1) determined to be compliant through existing Air Force policy.

(U) Tier 3 Common Controls. Security controls that are specific to enclaves on the DoD Information Network with a current ATO. These common controls are available to systems or major applications hosted within the enclave. Enclaves could include local area networks and the applications they host, backbone networks, and data processing centers. For example, systems hosted within a data center will use physical, environmental, and network security protections common controls established for that data center, such as door locks, guards, temperature controls, and network boundary security.

Whistleblower Protection
U.S. Department of Defense

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

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

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

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

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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