Report No. DODIG-2023-062

~~CUI~~

INSPECTOR GENERAL

U.S. Department of Defense

MARCH 31, 2023

(U) Management Advisory: The U.S. Transportation Command's Compliance with the Federal Information Security Modernization Act of 2014

~~Controlled by: DoD OIG~~
~~Controlled by: Audit/Cyberspace Operations~~
~~CUI Category: OPSEC/ISVI~~
~~Distribution/Dissemination Control: FEDCON~~
~~POC: Assistant Inspector General For Audit, Cyberspace Operations & Acquisition, Contracting, And Sustainment,~~ [redacted]

INTEGRITY ★ INDEPENDENCE★ EXCELLENCE

~~CUI~~


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

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

March 31, 2023

MEMORANDUM FOR UNITED STATES TRANSPORTATION COMMAND CHIEF INFORMATION OFFICER
UNITED STATES TRANSPORTATION COMMAND SENIOR PRIVACY OFFICER
INSPECTOR GENERAL, UNITED STATES TRANSPORTATION COMMAND

SUBJECT: (U) Management Advisory: The United States Transportation Command's Compliance with the Federal Information Security Modernization Act of 2014 (Report No. DODIG-2023-062)

(U) The purpose of this management advisory is to provide U.S. Transportation Command (USTRANSCOM) leadership with the DoD Office of Inspector General (DoD OIG) findings and recommendations specific to USTRANSCOM's compliance with the Federal Information Security Modernization Act of 2014 (FISMA). We identified these findings during our FY 2021 review of the DoD's compliance with FISMA, which was announced on November 18, 2020 (Project No. D2021-D000CP-0034.000). We conducted the work on this project with integrity, objectivity, and independence, as required by the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Federal Offices of Inspector General.

(U) FISMA requires Federal agencies to develop, document, and implement an agencywide program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources. FISMA also requires Federal agency Inspectors General (IGs), or an independent external auditor designated by an IG, to conduct an annual independent review on the effectiveness of the agency's information security program and practices. IGs must submit their annual results to the Office of Management and Budget and the Department of Homeland Security.

(U) As part of our FY 2021 independent review, we assessed selected portions of USTRANSCOM's information security program and practices. We submitted the results of the overall effectiveness of the DoD's information security program and practices to the Office of Management and Budget and Department of Homeland Security on October 28, 2021. We are issuing this advisory to report the results specific to USTRANSCOM and to issue recommendations for corrective action.

(U) We provided a draft copy of this management advisory to DoD management and requested written comments on the findings and recommendations. We considered management's comments on the draft and included comments in the final advisory.

(U) This management advisory contains six recommendations. We consider two recommendations unresolved, three recommendations resolved but open, and one recommendation closed. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section, the unresolved recommendations will remain unresolved until an agreement is reached on the actions to be taken to address the recommendations. Once an agreement is reached, the recommendations will be considered resolved but will remain open until documentation is submitted showing that the agreed-upon actions are complete. The three resolved recommendations will remain open until documentation is submitted showing that the agreed-upon actions are complete. Once we verify that the actions are complete, we will close the recommendations.

(U) DoD Instruction 7650.03 requires that recommendations be resolved promptly. For the unresolved recommendations, within 30 days please provide us your comments concerning specific actions in process or alternative corrective actions proposed on the recommendations. For the resolved recommendations, please provide us documentation within 90 days showing you have completed the agreed-upon actions. You should send your response as a PDF file to either followup@dodig.mil if unclassified or rfunet@dodig.smil.mil if classified SECRET. Responses must have the actual signature of the authorizing official for your organization.

(U) We appreciate the cooperation and assistance received during the review. If you have questions, please contact me [redacted]

FOR THE INSPECTOR GENERAL:

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

(U) Background

(U) On December 17, 2002, the President signed the "Federal Information Security Management Act" into law as part of the E-Government Act of 2002 (Public Law 107-347, Title III). The law provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets and provides a mechanism for improved oversight of Federal agency information security programs. Congress amended the law on December 18, 2014, (Public Law 113-283) and renamed it the "Federal Information Security Modernization Act of 2014" (FISMA). The amendment also establishes the Director of the Office of Management and Budget's (OMB) authority to oversee information security policies and practices for Federal agencies and the Secretary of the Department of Homeland Security's authority to manage the information security policies and practices across the Government. FISMA requires that senior agency officials provide security for the information and information systems (information security program) that support the operations and assets under their control, including assessing the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems. Federal agencies' information security programs are supported by security policy issued through the OMB, Department of Homeland Security, and risk-based standards and guidelines published by the National Institute of Standards and Technology (NIST).

(U) FISMA requires that senior agency officials provide security for the information and information systems (information security program) that support the operations and assets under their control.

(U) FISMA also requires that Federal agencies conduct an annual, independent review of the effectiveness of their information security program and practices. For a Federal agency with an IG appointed under the IG Act of 1978, that IG, or an independent external auditor designated by that IG, must conduct the review and submit the results to the OMB and Department of Homeland Security. Each year, the OMB issues guidance that requires the IGs to assess the effectiveness their agencies' information security program using annual IG FISMA reporting metrics.[1] The OMB, Department of Homeland Security, and Council of the Inspectors General on Integrity and Efficiency develop the IG FISMA reporting metrics, in consultation with the Federal Chief Information Officer Council.

[1] (U) OMB Memorandum M-21-02, "Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements," November 9, 2020.

(U) FISMA Reporting Metrics

(U) The FY 2021 OMB guidance included 66 IG FISMA reporting metrics.[2] The metrics were grouped into nine domains aligned under the five information security functions established by the NIST Cybersecurity Framework—Identify, Protect, Detect, Respond, and Recover.[3]

(U) The NIST Cybersecurity Framework provides Federal agencies with a common structure for identifying and managing cybersecurity risk across their information technology enterprise.

(U) The NIST Cybersecurity Framework provides Federal agencies with a common structure for identifying and managing cybersecurity risk across their information technology enterprise.[4] Table 1 lists the nine domains by function.

(U) Table 1. Descriptions of NIST Cybersecurity Framework Functions and FISMA Domains

(U) Function	Domain	Description
Identify	Risk Management	Risk management is the program and processes for managing information security risks to organizational operations (including mission, functions, image, and reputation), organizational assets, staff, and other organizations.
	Supply Chain Risk Management	Supply chain risk management is the process of ensuring that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity requirements.
Protect	Configuration Management	Configuration management consists of a collection of activities focused on establishing and maintaining the integrity of information technology products and information systems.
	Identity and Access Management	Identity and access management consists of the controls and processes for identifying users, using credentials, and managing user access to network resources.
	Data Protection and Privacy	Data protection and privacy consists of the controls and processes for protecting systems and information (data) and ensuring that management of those systems and data are consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
	Security Training	Security training consists of an established program that ensures all users complete the necessary mandatory cybersecurity training requirements before they receive access to organizational information technology resources, including specialized training for individuals requiring privileged access.
Detect	Information Security Continuous Monitoring	Information security continuous monitoring is the process for maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
Respond	Incident Response	Incident response is a formal, focused, and coordinated approach to responding to cybersecurity incidents.
Recover	Contingency Planning	Contingency planning is a coordinated strategy involving plans, procedures, and technical measures that will enable the recovery of information systems, operations, and data after a disruption. **(U)**

(U) Source: The DoD OIG.

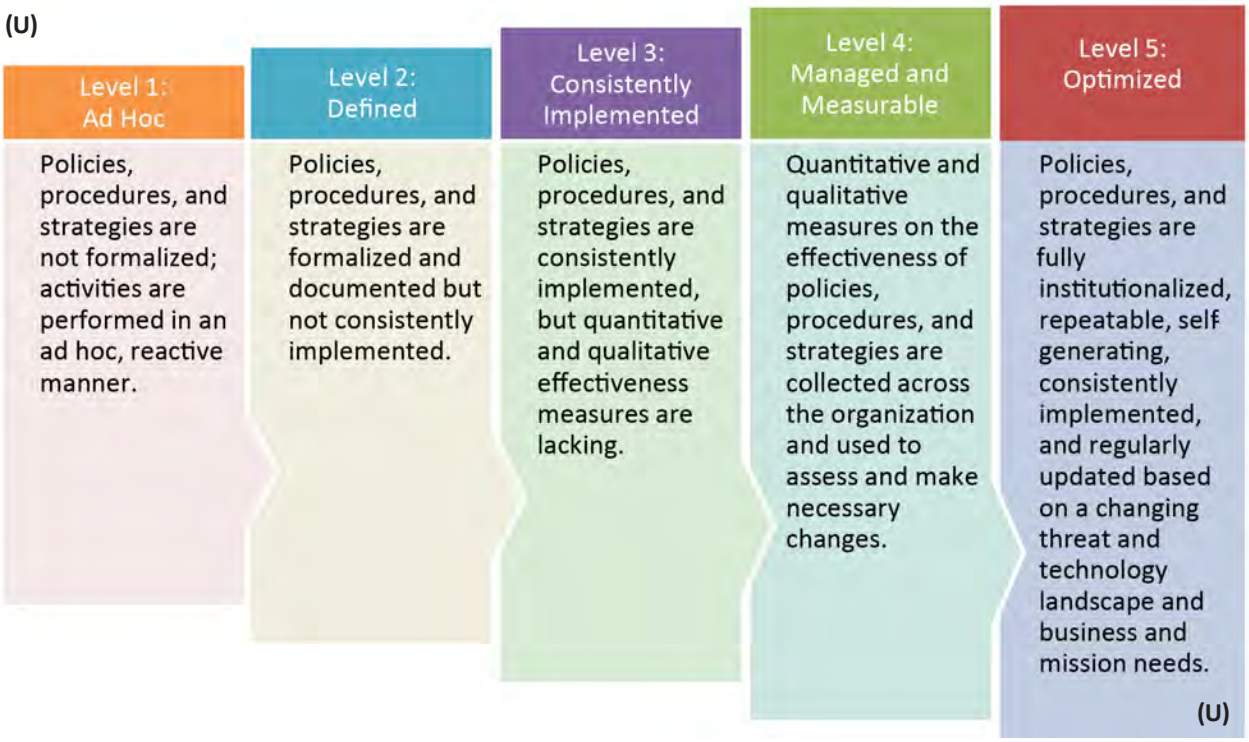
[2] (U) IG FISMA metrics are questions addressing various aspects of an organization's information security program.

[3] (U) "FY 2021 IG FISMA Reporting Metrics," Version 1.1, May 12, 2021. The FY 2021 IG FISMA Reporting Metrics referenced public law, Federal requirements, and NIST guidance as the criteria for measuring an agency's information security program and practices.

[4] (U) "NIST: Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1, April 16, 2018. The NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems.

(U) The IGs assign a maturity level (rating) for each domain by determining whether the agency has issued the required policies and procedures applicable to the domain, and whether the policies and procedures are implemented and effective. Figure 1 shows the five-level IG FISMA maturity model.

(U) Figure 1. IG FISMA Maturity Model



(U) Source: FY 2021 IG FISMA Reporting Metrics.

(U) IGs use a simple majority of the metric ratings to determine the maturity level for each domain and then use the domain ratings to determine the maturity level for each function, which IGs use to determine the overall agency rating. However, the FY 2021 IG FISMA Reporting Metrics allowed IGs to use their discretion when determining the maturity level and to adjust the rating along the scale accordingly. IGs could consider additional factors when determining the maturity levels and the agency's overall effectiveness, such as the maturity levels for the functions and the agency's unique missions, resources, and challenges.

(U) Scope and Methodology

(U) We assessed selected portions of U.S. Transportation Command's (USTRANSCOM) information security program and practices as part of our annual independent review of the DoD's overall information security program and practices. We submitted the results of the overall review to the OMB and Department of Homeland Security on October 28, 2021, and we are issuing this management advisory to report the results specific to USTRANSCOM and to issue recommendations for corrective action.

(U) We are issuing this management advisory to report the results specific to USTRANSCOM and to issue recommendations for corrective action.

(U) We conducted the USTRANSCOM assessment from November 2020 through November 2022. Specifically, we assessed whether USTRANSCOM met the requirements outlined in the FY 2021 IG FISMA Reporting Metrics for 5 of the 66 metrics, which represented four of the nine domains (see the Appendix for a list of the 5 metrics). We selected the five metrics for review using a risk-based approach that considered several factors, such as the DoD's prior FISMA results, the impact level (high, medium, low) of each reporting metric based on related NIST guidance, and whether the DoD Office of the Chief Information Officer (OCIO) tracked related information.[5] For each of the five metrics, we determined whether USTRANSCOM issued policies and procedures related to the metric and whether USTRANSCOM implemented the policies and procedures.

(U) To accomplish our review, we analyzed USTRANSCOM information technology and cybersecurity policies and procedures relevant to the five metrics and the corresponding NIST Special Publication (SP) 800-53 controls. We reviewed key documents, such as monthly status reports that officials used to track and monitor selected cybersecurity controls, plans for addressing protection of sensitive information, and other management reports supporting USTRANSCOM's efforts to oversee the implementation of selected metric questions. We also interviewed personnel from the USTRANSCOM OCIO and the Privacy and Civil Liberties office who were responsible for overseeing the implementation of cybersecurity and privacy-related policies and procedures.

(U) This report was reviewed by the DoD Component 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. In preparing and marking this report, we considered any comments submitted by the DoD Component about the CUI treatment of its information. If the DoD Component failed to provide any or sufficient comments about the CUI treatment of its information, we marked the report based on our assessment of available information.

[5] (U) Most FISMA metrics align with specific NIST SP 800-53 controls. Although the NIST issued Revision 5 to NIST SP 800-53, "Security and Privacy Controls for Information Systems and Organizations," September 23, 2020, agencies were not required to implement all changes until September 2021. Therefore, the FY 2021 IG FISMA metrics referenced the controls in Revision 4 to NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013.

(U) USTRANSCOM Roles and Responsibilities for Information Security

(U) DoD Instruction 8500.01 requires the DoD Chief Information Officer (CIO) to monitor and evaluate all cybersecurity activities, advise the Secretary of Defense on matters of cybersecurity, and appoint a DoD Senior Information Security Officer to direct and coordinate the DoD cybersecurity program.[6] DoD Instruction 8500.01 also requires that DoD Component CIOs, on behalf of the respective DoD Component heads, develop, implement, maintain, and enforce a DoD Component cybersecurity program that is consistent with the overall DoD cybersecurity program. DoD Instruction 8500.01 also requires CIOs to appoint a DoD Component Senior Information Security Officer to coordinate their DoD Component cybersecurity program. Furthermore, DoD and USTRANSCOM guidance outline the following roles and responsibilities pertaining to USTRANSCOM cybersecurity.

(U) Chief Information Officer. The USTRANSCOM CIO is responsible for developing, implementing, maintaining, and enforcing a cybersecurity program that is consistent with the overall DoD cybersecurity program and monitoring and tracking the overall execution of plans of action and milestones (POA&Ms).

(U) Chief Information Security Officer. The USTRANSCOM Chief Information Security Officer is responsible for directing and coordinating the USTRANSCOM cybersecurity program.

(U) Senior Component Official for Privacy. The USTRANSCOM Senior Component Official for Privacy is responsible for implementing the USTRANSCOM privacy program, providing guidance, and certifying that USTRANSCOM personnel receive appropriate privacy training.

(U) Privacy Act Program Manager. The USTRANSCOM Privacy Act program manager is responsible for ensuring USTRANSCOM is limiting the collection of personally identifiable information (PII) and informing individuals of the purpose and use of information. The Privacy Act program manager is also responsible for training USTRANSCOM personnel on handling PII and reporting privacy breaches.

(U) Authorizing Official. USTRANSCOM Authorizing Officials (AOs) are responsible for granting authorization decisions for USTRANSCOM information technology systems. AOs grant an authorization after determining whether the overall risks of operating a system are at an acceptable level to support mission requirements. In addition, USTRANSCOM AOs are responsible for monitoring the information system vulnerabilities and mitigating identified vulnerabilities using POA&Ms.

(U) Information System Owner. USTRANSCOM information system owners are responsible for the overall procurement, development, integration, modification, operation, and maintenance of USTRANSCOM information technology systems.

[6] (U) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014 (Incorporating Change 1, October 7, 2019).

(U) Program Manager. USTRANSCOM program managers are responsible for enforcing AO authorization decisions for USTRANSCOM information technology systems and appointing an information system security manager for each system. Program managers are also responsible for ensuring the development, tracking, and resolution of POA&Ms for their assigned systems and providing the status to the USTRANSCOM Chief Information Security Officer, AO, and CIO.[7]

(U) Information System Security Manager. USTRANSCOM information system security managers are responsible for maintaining and reporting information systems assessment and authorization status of each system, and they are the primary cybersecurity technical advisors to USTRANSCOM AOs.

(U) USTRANSCOM Information Security Program and Practices

(U) Although USTRANSCOM had policies and procedures in place for the five metrics we reviewed, it did not consistently implement the policies and procedures for three of the five metrics. Specifically, USTRANSCOM officials tracked user completion of annual cybersecurity awareness training (Metric 44) and established a process to ensure that all systems had a valid authorization to operate (ATO) (Metric 49); however, for the remaining three metrics, USTRANSCOM officials did not:

(U) Although USTRANSCOM had policies and procedures in place for the five metrics we reviewed, it did not consistently implement the policies and procedures for three of the five metrics.

- (U) track and monitor the mitigation of system security weaknesses identified in POA&Ms within established timeframes (Metric 8);[8]
- (U) report all required privacy-related breaches (Metric 38); or
- (U) require that personnel take privacy awareness training annually, including role-based training (Metric 39).

(U) Consistent implementation of cybersecurity policies and procedures is critical for an effective cybersecurity program and reduces the risk of successful cyber attacks, data breaches, data loss, data manipulation, and unauthorized disclosures of mission-essential or sensitive information by malicious actors. Therefore, USTRANSCOM should take action to address the recommendations in this management advisory, which will result in more consistent implementation of the policies and procedures and reduce the risk associated with the three metrics we reviewed.

[7] (U) A POA&M is a document used to record the known weaknesses (risks) in a system or network, the actions and resources needed to mitigate those weaknesses, and the expected milestones and completion dates for mitigating the weaknesses.

[8] (U) FISMA, NIST, and USTRANSCOM sometimes use the terms weakness and vulnerability interchangeably, but we use the term weakness for purposes of this advisory.

(U) Identify Function/Risk Management Domain

(U) For the Identify Function/Risk Management Domain, we assessed FY 2021 IG FISMA Reporting Metric 8, which asks, *"To what extent has the organization ensured that POA&Ms are utilized for effectively mitigating security weaknesses?"*

(U) USTRANSCOM program managers were not always monitoring and tracking the POA&Ms to ensure that the weaknesses were mitigated in accordance with USTRANSCOM policies and procedures.

(U) USTRANSCOM policies and procedures require officials to develop and use POA&Ms for mitigating security weaknesses. However, USTRANSCOM program managers were not always monitoring and tracking the POA&Ms to ensure that the weaknesses were mitigated in accordance with USTRANSCOM policies and procedures. NIST SP 800-53 requires that organizations prepare POA&Ms to document planned mitigation or remediation steps to correct weaknesses identified and to reduce or eliminate known weaknesses. DoD Instruction 8510.01 aligns with NIST SP 800-53. DoD Instruction 8510.01 requires that program managers prepare POA&Ms when system weaknesses are identified and document the progress in mitigating the weaknesses in the POA&M.[9]

(U) The USTRANSCOM POA&M Guidebook, March 2020, was USTRANSCOM's implementation guidance for managing information system weaknesses in FY 2021 and stated that program managers or information system security managers are responsible for implementing the corrective actions identified in POA&Ms. The Guidebook also stated that the USTRANSCOM CIO is responsible for monitoring and tracking the overall execution of system-level POA&Ms, while the AO is responsible for monitoring weaknesses and actions taken to mitigate system-level POA&Ms. The Guidebook required correction of all very high and high weaknesses within 30 days and mitigation of all moderate weaknesses within 90 days. A very high weakness is an exposed and exploitable weakness, and its exploitation could result in severe operational impact; relevant security controls to address the weakness are not planned or identified. A high weakness is based on exposure of the weakness, ease of exploitation, and the severity of impact; relevant security controls are planned but not implemented or compensating controls are in place and minimally effective. A moderate weakness is based on exposure of the weakness, ease of exploitation, and severity of impact; relevant security controls to address the weakness are planned, partially implemented, and somewhat effective. However, in September 2021, USTRANSCOM issued the POA&M Standard Operating Procedure and removed the 30- and 90-day requirements for timely mitigation of high and moderate weaknesses required by the previous guidance. The September 2021 POA&M Standard Operating Procedure requires that officials mitigate weaknesses within the established POA&M completion date.

[9] (U) DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022. Although the Instruction was updated in July 2022, the requirement for program managers to oversee POA&M development, monitoring, and resolution is similar to previous versions.

~~(CUI)~~ Although USTRANSCOM program managers were preparing POA&Ms to address known weaknesses in the systems, USTRANSCOM OCIO officials were not consistently monitoring and tracking the status of the very high, high, and moderate weaknesses to ensure that program managers mitigated identified weaknesses within established timeframes. USTRANSCOM tracks its POA&Ms in the Enterprise Mission Assurance Support Service (eMASS). eMASS is a web-based tool used to capture key system information such as system security plans, security control test results, POA&Ms, and authorization decisions (granting ATOs). Initially, we reviewed the POA&M status for [redacted] systems reported in eMASS.[10] Although eMASS did not age the weaknesses by their development date, it indicated that the [redacted] systems had [redacted] high and [redacted] moderate weaknesses that were at least 120 days past their scheduled completion date.

~~(CUI)~~ Based on our initial review, we requested that USTRANSCOM OCIO officials provide the status of all unclassified POA&Ms to determine the extent of the late mitigation of weaknesses. In October 2022, the USTRANSCOM alternate Chief Information Security Officer provided a report identifying [redacted] very high or high weaknesses and [redacted] moderate weaknesses recorded in eMASS. Although eMASS did not age the weaknesses by their development date, it indicated that all [redacted] very high, high, and moderate weaknesses were at least 120 days past their scheduled completion. Furthermore, we reviewed the [redacted] very high or high weaknesses to determine whether any weaknesses were included in the Cybersecurity and Infrastructure Security Agency's known exploited vulnerabilities (weaknesses) catalog, but did not identify any.[11]

(U) By not ensuring that program managers mitigated weaknesses identified in POA&Ms in a timely manner, USTRANSCOM increased the risk of successful cyber attacks, system and data breaches, and data loss and manipulation by malicious actors to its network. Therefore, the USTRANSCOM CIO should direct the program managers, in coordination with the USTRANSCOM Chief Information Security Officer and the AOs, to mitigate all very high, high, and moderate weaknesses identified in POA&Ms that exceed the 30-day and 90-day mitigation requirement as required by USTRANSCOM guidance. The USTRANSCOM CIO should also establish controls, in coordination with the USTRANSCOM Chief Information Security Officer and AOs, to ensure that program managers mitigate weaknesses identified in POA&Ms by their scheduled completion dates and in accordance with the timelines established in USTRANSCOM guidance.

[10] (U) We reviewed the POA&M status information from August 2021 and May 2022.

[11] (U) The Cybersecurity and Infrastructure Security Agency, part of the Department of Homeland Security, is responsible for managing a catalog of known exploited vulnerabilities that carry significant risk to the Federal government. An active exploitation occurs when there is evidence that malicious actors are actively exploiting known system vulnerabilities without knowledge of the system owners.

(U) NIST SP 800-53 defines a vulnerability as a weakness in an information system, system security procedures, internal controls, or the implementation of the controls or procedures that could be exploited.

(U) Protect Function/Data Protection and Privacy Domain

(U) For the Protect Function/Data Protection and Privacy Domain, we assessed two FY 2021 IG FISMA Reporting Metrics.

- (U) Metric 38, which asks, *"To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events?"*[12]
- (U) Metric 39, which asks, *"To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training?"*

(U) Data Breach Response Plan

(U) USTRANSCOM implemented the October 2017 DoD Breach Response Plan and had additional policies and procedures in place for responding to privacy-related breaches.[13] However, USTRANSCOM officials did not always report privacy-related breaches as required. A breach is a privacy incident that results in the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where a person other than an authorized user accesses or potentially accesses PII, or an authorized user accesses PII for an unauthorized purpose.[14] A privacy incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the PII the system processes, stores, or transmits; or an occurrence that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. NIST SP 800-53 requires that organizations develop and implement a response plan for privacy incidents, and provide a response to privacy incidents in accordance with the organizational response plan for privacy incidents.

(U) USTRANSCOM officials did not always report privacy-related breaches as required.

(U) The October 2017 DoD Breach Response Plan aligns with NIST SP 800-53 and provides the DoD with procedures for preparing for and responding to known or suspected privacy-related breaches. USTRANSCOM Instruction 33-35 and the USTRANSCOM PII Breach/Incident Response Plan are USTRANSCOM's implementing guidance that aligns with the DoD Breach Response Plan.[15] The USTRANSCOM guidance requires that the Privacy Act

---

12 (U) A privacy event is any observable occurrence in a system or network, which may indicate that a privacy incident is occurring.

13 (U) Office of the Deputy Chief Management Officer Memorandum, "DoD Breach Response Plan," October 31, 2017. In November 2018, the Deputy Secretary of Defense issued a memorandum, "Reporting of Breaches of Personally Identifiable Information in Accordance with the Department of Defense Breach Response Plan," to supplement the October 2017 DoD Breach Response Plan.

(U) Effective October 1, 2021, the Deputy Secretary of Defense disestablished the Office of the Chief Management Officer and transferred, among other responsibilities, oversight, privacy, and data breach responsibilities to the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency.

14 (U) PII is information that can be used to distinguish or trace an individual's identity.

15 (U) USTRANSCOM Instruction 33-35, "Privacy Act and Civil Liberties Program," February 4, 2016.

(U) USTRANSCOM PII Breach/Incident Response Plan, May 10, 2018.

(U) program manager submit a privacy-related breach report (DD Form 2959) to the Chief of the DoD's Privacy, Civil Liberties, and Freedom of Information Division through the U.S. Compliance and Reporting Tool within 48 hours of a breach notification.[16]

(U) However, USTRANSCOM privacy officials did not consistently report privacy-related breaches to the DoD's Privacy, Civil Liberties, and Freedom of Information Division as required. For FY 2021, USTRANSCOM experienced two minor breaches between October 2020 and May 2021.[17] Of the two minor breaches identified, USTRANSCOM officials reported one breach within 48 hours, but did not report the other breach to the DoD's Privacy, Civil Liberties, and Freedom of Information Division as required. The two minor breaches involved instances in which documents containing PII were e-mailed without encryption or e-mailed to individuals that did not have a need to know.[18] USTRANSCOM officials stated that they addressed both breaches by ensuring the e-mails were removed from the affected accounts, notifying affected individuals, and requiring additional PII training for the responsible personnel.

(U) Not reporting privacy-related breaches limits the DoD's ability to monitor, track, and evaluate data to ensure that the DoD reduces the potential harm caused by unauthorized access to PII and other sensitive data. Therefore, the USTRANSCOM Senior Component Official for Privacy should establish controls to ensure that the Privacy Act program manager properly reports all breaches in accordance with USTRANSCOM guidance.

(U) Updated DoD Data Breach Response Plan

(U) In May 2021, the DoD issued a revised Data Breach Response Plan for DoD Components to use within their subcomponents.[19] The revised plan included changes to the privacy-related breach reporting process. For example, the updated plan requires that Component privacy officers report breaches to the DoD Component security operations center, which in turn reports the breaches through its chain of command to the U.S. Cyber Command. The U.S. Cyber Command is responsible for reporting the privacy-related breaches to the U.S. Computer Emergency Readiness Team, which is part of the Department of Homeland Security. The U.S. Computer Emergency Readiness Team is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. However, USTRANSCOM officials did not update

(U) USTRANSCOM officials did not update USTRANSCOM Instruction 33-35 to align with the revisions from the May 2021 DoD Data Breach Response Plan.

[16] (U) The U.S. Compliance and Reporting Tool is the system that the DoD uses to report privacy-related incidents.

[17] (U) A major breach is an incident that involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. Minor breaches are those that do not meet the definition of a major breach.

[18] (U) Encryption conceals the data to prevent it from being known or used by unauthorized devices or individuals.

[19] (U) DoD Manual 5400.11, Volume 2, "DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan," May 6, 2021.

(U) USTRANSCOM Instruction 33-35 to align with the revisions from the May 2021 DoD Data Breach Response Plan. Therefore, the USTRANSCOM Senior Component Official for Privacy should update USTRANSCOM Instruction 33-35 to align with DoD Manual 5400.11, including the changes to the breach reporting process.

(U) Privacy Training

(U) Although USTRANSCOM had privacy-related guidance in place, such as USTRANSCOM Instruction 33-35, it did not have policies and procedures that required its personnel (military members, civilians, and contractors) to take privacy awareness training annually, including role-based training. NIST SP 800-53 directs organizations to oversee basic privacy training and targeted, role-based privacy training at least annually and indicates that, where appropriate, organizations may provide privacy training as part of existing information security training.[20] DoD regulation 5400.11-R also requires DoD Components to develop their own privacy procedures and methodology and to consider whether associated annual privacy training should be mandated.[21] However, privacy guidance used by USTRANSCOM does not align with NIST SP 800-53 requirements. USTRANSCOM Instruction 33-35 requires the Privacy Act program manager to direct periodic privacy training as needed and requires system managers to train personnel on Privacy Act requirements. USTRANSCOM Instruction 33-35 does not specify the minimum frequency or content for training personnel, such as responsibilities under the Privacy Act, consequences of failing to carry out those responsibilities, data collection and use requirements, or privacy incident reporting.

(U) It did not have policies and procedures that required its personnel (military members, civilians, and contractors) to take privacy awareness training annually, including role-based training.

(U) According to USTRANSCOM privacy officials, USTRANSCOM uses the DoD Cyber Awareness Challenge course to provide annual privacy awareness training to its personnel. Although the primary focus of the course is cybersecurity, it also addresses how to identify and safeguard PII. The course is mandatory and is required annually for all users that have access to USTRANSCOM information systems.[22] However, the DoD Cyber Awareness Challenge course does not address other aspects of basic privacy training, such as provisions of the Privacy Act, penalties for violating the act, authorized uses of PII, or procedures to follow in the event of an incident or breach.

[20] (U) Similar to Revision 4, NIST SP 800-53, Revision 5, directs organizations to provide literacy training and role-based privacy training at an organizationally defined frequency. Literacy is familiarity with, and the ability to apply, a core knowledge set of information.

[21] (U) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007.

[22] (U) See the Protect Function/Security Training Domain section (Metric 44) on how USTRANSCOM tracks completion of this privacy training.

(U) Without a clear baseline for privacy awareness training, USTRANSCOM officials cannot determine the adequacy of the training provided. Privacy training increases awareness of PII, presents steps for protecting PII, and explains privacy requirements that reduce the risk of noncompliance with the Privacy Act. Failure to adequately safeguard PII can also increase the risk of potential breaches and loss of PII. Therefore, the USTRANSCOM Senior Component Official for Privacy should update USTRANSCOM Instruction 33-35 to provide minimum frequency and content requirements for USTRANSCOM privacy awareness training. The USTRANSCOM Senior Component Official for Privacy should also develop and implement procedures sufficient to ensure that all USTRANSCOM personnel receive annual privacy awareness training that addresses each of the key elements required by updated USTRANSCOM guidance.

(U) Protect Function/Security Training Domain

(U) For the Protect Function/Security Training Domain, we assessed FY 2021 IG FISMA Reporting Metric 44, which asks, *"To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems?"*

(U) USTRANSCOM had policies and procedures in place that required all network users to complete security awareness training annually and ensured that the training was tailored based on mission, risk environment, and types of information systems as required. In addition, USTRANSCOM officials established a process to track that users (military members, civilians, and contractors) completed the annual security awareness training in a timely manner.

(U) USTRANSCOM officials established a process to track that users (military members, civilians, and contractors) completed the annual security awareness training in a timely manner.

(U) NIST SP 800-53 directs organizations to provide basic security awareness training to information system users as part of initial training, when required by system changes, and at an organizationally defined frequency thereafter. USTRANSCOM Instruction 33-1 aligns with the NIST SP 800-53 requirement and states that all personnel must complete initial and annual cybersecurity awareness training as a condition of access to the network.[23] USTRANSCOM uses the DoD Cyber Awareness Challenge course to meet the initial and annual requirements for cybersecurity awareness training, which include cybersecurity instruction in key areas such as e-mail, mobile devices, social media, phishing, malware, and physical security and provides DoD users with actions they should take to defend against the associated risks.

[23] (U) USTRANSCOM Instruction 33-1, "Information Systems Security Education, Training, and Awareness Program," March 27, 2017. The awareness training used by USTRANSCOM is a DoD course updated annually by the DoD CIO to remain current with the DoD information system environment.

(U) USTRANSCOM Instruction 33-1 requires USTRANSCOM officials to document and maintain the status of user awareness training. USTRANSCOM officials explained that new users must complete initial cybersecurity awareness training as part of the onboarding process. USTRANSCOM officials further explained that they use a learning management system to track whether USTRANSCOM network users completed annual cybersecurity awareness training. USTRANSCOM officials stated that they reviewed a monthly report from the system to identify network users who had not taken the training by their annual date and then provided those users 10 business days to complete the training. USTRANSCOM officials then reviewed another report from the system and deactivated the network accounts of those users who still had not taken the annual training. Once the user completed cybersecurity awareness training, USTRANSCOM officials said that they reactivated the user account.

(U) Because USTRANSCOM had policies and procedures for security awareness training and demonstrated that it consistently implemented the policies and procedures to ensure that users completed annual security awareness training, we are not making a recommendation for this metric.

(U) Detect Function/Information Security Continuous Monitoring Domain

(U) For the Detect Function/Information Security Continuous Monitoring Domain, we assessed FY 2021 IG FISMA Reporting Metric 49, which asks, *"How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls?"*

(U) USTRANSCOM had policies and procedures in place that require information system owners to conduct system assessments, obtain system authorizations, develop and maintain system security plans, and monitor security controls. USTRANSCOM officials also established a process to ensure that all systems had a valid ATO before connecting to the USTRANSCOM network.

(U) USTRANSCOM officials also established a process to ensure that all systems had a valid ATO before connecting to the USTRANSCOM network.

(U) NIST SP 800-53 requires that organizations assess the security controls for information systems and their operational environment to determine whether the controls are correctly implemented. NIST SP 800-53 also requires organizations to produce a security assessment report that documents the results of the assessment. DoD Instruction 8510.01 aligns with NIST SP 800-53. DoD Instruction 8510.01 requires DoD Component Heads to operate only

(U) authorized information systems and requires controls to be documented in the DoD Risk Management Framework (RMF) security authorization package or ATO.[24] USTRANSCOM implements the DoD RMF process and uses eMASS to document the cybersecurity risk management and system authorization process. USTRANSCOM AOs granted ATOs after they had verified that the overall system risk was at an acceptable level for mission and network. USTRANSCOM officials also explained that they met with leadership on a weekly basis to discuss any issues regarding the ATOs. As of September 2021, USTRANSCOM officials reported that all unclassified information systems were operating with a valid ATO. We requested an update from USTRANSCOM officials in October 2022, and they confirmed that all 40 unclassified information systems were operating with a valid ATO.

(U) Because USTRANSCOM had policies and procedures for performing ongoing security control assessments, including granting ATOs, and consistently implemented those policies and procedures to ensure that all unclassified systems were operating with a valid ATO, we are not making a recommendation for this metric.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

(U) We recommend that the U.S. Transportation Command Chief Information Officer:

a. (U) Direct the program managers, in coordination with the U.S. Transportation Command Chief Information Security Officer and Authorizing Officials, to mitigate all very high, high, and moderate weaknesses identified in plans of action and milestones that exceed the 30-day and 90-day mitigation requirement as required by U.S. Transportation Command guidance.

(U) U.S. Transportation Command Chief Information Officer Comments

(U) The USTRANSCOM CIO partially agreed, stating that they agreed with the finding but did not agree with the draft recommendation as written. The CIO agreed that USTRANSCOM officials failed to mitigate POA&Ms within the timeframes established in the March 2020 USTRANSCOM POA&M Guidebook, but that those timeframes were no longer in effect. The CIO explained that USTRANSCOM replaced the POA&M Guidebook with the POA&M Standard Operating Procedure in September 2021, and that the Standard Operating Procedure does not require USTRANSCOM officials to meet the 30 and 90-day timeframes for mitigating high and moderate weaknesses but instead requires programs to perform monthly reviews

[24] (U) DoD Instruction 8510.01 outlines the DoD RMF process and provides procedural guidance for the acceptance of authorization decisions within the DoD for the authorization and connection of information systems (granting ATOs). The DoD RMF process is a step-by-step, risk-based approach to identify the security controls needed to protect systems, networks, and data consisting of six steps throughout the information system's life cycle: 1) categorize the system, 2) select security controls, 3) implement security controls, 4) assess security controls, 5) authorize the system, and 6) monitor security controls.

(U) and quarterly updates of all ongoing POA&Ms until resolution has been achieved or risk acceptance has been granted. The CIO stated that the Standard Operating Procedure aligns with DoD guidance concerning POA&Ms.

(U) The CIO added that the USTRANSCOM Chief Information Security Officer issued a memorandum in February 2023 to reinforce program manager and information system security manager adherence to the requirements outlined in the USTRANSCOM Information Security Continuous Monitoring Strategy and the POA&M Standard Operating Procedure. The CIO stated that the Chief Information Security Officer memorandum emphasizes the importance of reviewing very high and high weaknesses and any weaknesses 30 days beyond the scheduled POA&M completion date. The USTRANSCOM CIO also stated that the status of open POA&Ms will be briefed for all programs starting in February 2023.

(U) Our Response

(U) Although the USTRANSCOM CIO partially agreed, their comments addressed the specifics of the recommendation. We verified that USTRANSCOM did not include the 30 and 90-day timeframes for mitigating high and moderate weaknesses in the POA&M Standard Operating Procedure but did include a requirement to perform monthly reviews and quarterly updates of all POA&Ms until resolution or risk acceptance has been granted. Since we determined that USTRANSCOM was not mitigating weaknesses identified in POA&Ms in a timely manner, we agree that it is important for program managers and information system security managers to perform monthly reviews to ensure that open POA&Ms items are mitigated within timeframes established in USTRANSCOM guidance. We also verified that the USTRANSCOM Chief Information Security Officer issued a memorandum to information system program managers and information system security managers on February 2, 2023, requiring the immediate implementation of the monthly reviews and quarterly updates of open POA&M items with an emphasis on very high and high weaknesses and items more than 30 days beyond their scheduled completion date. Therefore, this recommendation is closed, and no further comments are required.

b. (U) Establish controls, in coordination with the U.S. Transportation Command Chief Information Security Officer and Authorizing Officials, to ensure that program managers mitigate weaknesses identified in plans of action and milestones by their scheduled completion dates and in accordance with the timelines established in U.S. Transportation Command guidance.

(U) U.S. Transportation Command Chief Information Officer Comments

(U) The USTRANSCOM CIO agreed, stating that USTRANSCOM implemented a revised weekly Security Posture meeting schedule starting in February 2023 that includes the review of open POA&Ms. The CIO explained that the revised Security Posture meetings will operate on a 6-week cycle in which information system program managers and information system

(U) security managers will brief the status of their open POA&Ms to the CIO and Chief Information Security Officer on a rotational basis. The CIO explained that this 6-week cycle will consist of POA&M status briefings to the Chief Information Security Officer in the first week and the CIO in the second week, leaving the remaining 4 weeks for officials to make any necessary updates.

(U) Our Response

(U) Comments from the USTRANSCOM CIO partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. Although the CIO stated that USTRANSCOM implemented a revised weekly Security Posture meeting schedule that includes the review of open POA&Ms, the CIO did not state where this process is documented within USTRANSCOM guidance. Therefore, we request that the USTRANSCOM CIO provide additional comments within 30 days in response to the final report that describes the USTRANSCOM's planned actions to include the requirement for weekly Security Posture meeting schedule into USTRANSCOM guidance.

(U) Recommendation 2

(U) We recommend that the U.S. Transportation Command Senior Component Official for Privacy:

a. (U) Establish controls to ensure that the Privacy Act program manager properly reports all breaches in accordance with U.S. Transportation Command guidance.

(U) U.S. Transportation Command Senior Component Official for Privacy Comments

(U) The USTRANSCOM Senior Component Official for Privacy agreed, stating that USTRANSCOM Instruction 5050-03, "Privacy and Civil Liberties," was updated to align with DoD Manual 5400.11, volume 2. The Senior Component Official for Privacy also stated that the updated guidance was submitted for approval, and should be finalized by May 2023.

(U) Our Response

(U) Comments from the USTRANSCOM Senior Component Official for Privacy partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. Although the Senior Component Official for Privacy stated that USTRANSCOM Instruction 5050-03 was updated to include controls to ensure that officials reported all required breaches, they did not state what specific controls were included. Therefore, we request that the Senior Component Official for Privacy provide additional comments within 30 days in response to the final report that describe the controls included in USTRANSCOM Instruction 5050-03 to ensure that the Privacy Act program manager reports all required breaches. In our response to Recommendations 2.b, 2.c, and 2.d, we request that the Senior Component Official for Privacy

(U) provide a copy of USTRANSCOM Instruction 5050-03, to validate that updates to the Instruction are sufficient to close the recommendations. If USTRANSCOM Instruction 5050-03 includes controls to ensure that USTRANSCOM officials report all required breaches, then we will close this recommendation.

b. (U) Update U.S. Transportation Command Instruction 33-35, "Privacy Act and Civil Liberties Program," February 4, 2016, to align with DoD Manual 5400.11, Volume 2, "DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan," May 6, 2021, including the changes to the breach reporting process.

(U) U.S. Transportation Command Senior Component Official for Privacy Comments

(U) The USTRANSCOM Senior Component Official for Privacy agreed, stating that USTRANSCOM Instruction 5050-03, "Privacy and Civil Liberties," was updated to include the breach reporting process as outlined in DoD Manual 5400.11, volume 2. The Senior Component Official for Privacy also stated that the updated guidance was submitted for approval, and should be finalized by May 2023.

(U) Our Response

(U) Comments from the USTRANSCOM Senior Component Official for Privacy addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once USTRANSCOM provides the updated guidance and we verify that the guidance aligns with DoD Manual 5400.11, volume 2, to include the breach reporting process.

c. (U) Update U.S. Transportation Command Instruction 33-35, "Privacy Act and Civil Liberties Program," February 4, 2016, to provide minimum frequency and content requirements for U.S. Transportation Command privacy awareness training.

(U) U.S. Transportation Command Senior Component Official for Privacy Comments

(U) The USTRANSCOM Senior Component Official for Privacy agreed, stating that USTRANSCOM Instruction 5050-03, "Privacy and Civil Liberties," was updated to include minimum frequency and content requirements for USTRANSCOM privacy awareness training. The Senior Component Official for Privacy also stated that the updated guidance was submitted for approval, and should be finalized by May 2023.

(U) Our Response

(U) Comments from the USTRANSCOM Senior Component Official for Privacy addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once USTRANSCOM provides the updated guidance and we verify that the guidance includes the minimum frequency and content requirements for privacy awareness training.

d. (U) Develop and implement procedures sufficient to ensure that all U.S. Transportation Command personnel receive annual privacy awareness training that addresses each of the key elements required by the updated U.S. Transportation Command Instruction.

(U) U.S. Transportation Command Senior Component Official for Privacy Comments

(U) The USTRANSCOM Senior Component Official for Privacy agreed, stating that USTRANSCOM Instruction 5050-03, "Privacy and Civil Liberties," was updated to ensure that USTRANSCOM personnel receive annual privacy awareness training that addresses each of the key elements as required. The Senior Component Official for Privacy also stated that the updated guidance was submitted for approval, and should be finalized by May 2023. The Senior Component Official for Privacy further explained that USTRANSCOM would include the updated training in its internal Learning Management System as an annual requirement for all personnel.

(U) Our Response

(U) Comments from the USTRANSCOM Senior Component Official for Privacy addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once USTRANSCOM provides the updated guidance and Learning Management System documentation and we verify that the guidance includes a requirement for personnel to complete annual privacy awareness training and that the annual training requirement was added to the Learning Management System.

(U) Appendix

(U) IG FISMA Reporting Metrics Reviewed at USTRANSCOM

(U) FISMA Function *(Domain)*	Metric No.	Metric Question
Identify *(Risk Management)*	8	To what extent has the organization ensured that POA&Ms are utilized for effectively mitigating security weaknesses?
Protect *(Data Protection and Privacy)*	38	To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events?
Protect *(Data Protection and Privacy)*	39	To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training?
Protect *(Security Training)*	44	To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems? (Note: Awareness training topics should include, as appropriate, consideration of organizational policies, roles, and responsibilities; secure e-mail; browsing and remote access practices; mobile device security; secure use of social media; phishing; malware; physical security; and security incident reporting.)
Detect *(Information Security Continuous Monitoring)*	49	How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls? **(U)**

(U) Source: The DoD OIG.

(U) Management Comments

(U) U.S. Transportation Command Chief Information Officer

UNITED STATES TRANSPORTATION COMMAND
508 SCOTT DRIVE
SCOTT AIR FORCE BASE, ILLINOIS 62225-5357

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

FROM: U.S. Transportation Command (USTRANSCOM) Chief Information Officer (CIO)

SUBJECT: DODIG Discussion Draft for Audit of Compliance With the Federal Information Security Modernization Act of 2014 (D2021-D000CP-0034.002)

1. USTRANSCOM has reviewed the subject report and provides the attached response to the report's recommendations.

2. The point of contact in this matter is [redacted] if you have any questions or concerns.

HAYWORTH.MICH ELLE.L [redacted] Digitally signed by [redacted]

MICHELLE L. HAYWORTH
Brigadier General, USAF
CIO, USTRANSCOM

Attachments:
USTRANSCOM Response

cc:
TCJA

(U) U.S. Transportation Command Chief Information Officer (cont'd)

USTRANSCOM Response

DOD IG Draft Report (Project No. D2021-D000CP-0034.002)
"The U.S. Transportation Command's Compliance with the Federal Information Security Modernization Act of 2014" Dated 23 January 2023

Recommendation 1: (U) We recommend that the U.S. Transportation Command Chief Information Officer:

a. (U) Direct the Program Managers, in coordination with the U.S. Transportation Command Chief Information Security Officer and Authorizing Officials, to identify and mitigate all very high, high, and moderate weaknesses identified in plans of action and milestones that exceed the 30-day and 90-day mitigation requirement as required by U.S. Transportation Command guidance.

USTRANSCOM Position: (U) Partially Concur. USTRANSCOM concurs with the finding as stated in the subject report but does not concur with the proposed remediation requirement. Specifically, USTRANSCOM agrees with the DOD IG that in FY2021 it failed to meet Plan of Action and Milestones (POA&M) timelines established in the USTRANSCOM POA&M Guidebook. However, in September 2021, USTRANSCOM rescinded the USTRANSCOM POA&M Guidebook and replaced it with a document titled "Plan of Action and Milestones (POA&M) Standard Operating Procedure (SOP)." The September 2021 SOP removes date defined mitigation deadlines such as the 30 and 90 day requirements present in the USTRANSCOM POA&M Guidebook. The publication of the September 2021 SOP brings USTRANSCOM's mitigation guidance, when requiring POA&Ms, in line with current DOD guidance and policy, which requires programs to perform monthly review and quarterly updates of all ongoing findings in the program's POA&M until resolution has been achieved or risk acceptance has been granted.

(U) As it relates to ensuring tracking and monitoring of Very High, High, and Moderate weakness POA&Ms, the USTRANSCOM CISO issued a Memorandum to reinforce PM and ISSM adherence to the timelines outlined in the USTRANSCOM Information Security Continuous Monitoring (ISCM) Strategy and the September 2021 POA&M SOP with special emphasis on reviewing Very High / High severity items and items 30 days past the scheduled completion date. Furthermore, the status of these open POA&M items will be briefed by all programs starting 8 February 2023 as part of an updated Security Posture status meeting effort.

Estimated Completion Date (ECD): 8 February 2023, and ongoing thereafter

b. (U) Establish controls, in coordination with the U.S. Transportation Command Chief Information Security Officer and Authorizing Officials, to ensure that program managers mitigated weaknesses identified in plans of action and milestones by their scheduled completion dates and in accordance with the timelines established in U.S. Transportation Command guidance.

USTRANSCOM Position: (U) Concur. In conjunction with this Corrective Action Plan, USTRANSCOM TCJ6-X implemented a revised weekly Security Posture meeting, complete with elements specifically designed to review the status of open POA&Ms. A six-week rotating cycle has been established where Program Managers and ISSMs will brief the status of their POA&Ms to the CISO on week one, then the CIO on week two, and then will have four weeks to make necessary updates while other programs brief their POA&M statuses.

(U) U.S. Transportation Command Chief Information Officer (cont'd)

3

Estimated Completion Date (ECD): Ongoing, starting 8 February 2023. Development of the revised weekly Security Posture meeting format has been ongoing for several weeks. Programs have been participating in test runs, template materials have been developed, and schedules have been created.

(U) U.S. Transportation Command Senior Component Official for Privacy

UNITED STATES TRANSPORTATION COMMAND
508 SCOTT DRIVE
SCOTT AIR FORCE BASE, ILLINOIS 62225-5357

8 February 2023

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

FROM: TCJA

SUBJECT: U.S. Transportation Command (USTRANSCOM) Response to DODIG Draft Report "The U.S. Transportation Command's Compliance With the Federal Information Security Modernization Act of 2014"

1. USTRANSCOM has reviewed the subject draft report and provides the attached response to the report's recommendations.

2. For additional information or assistance, please contact [redacted]

ANDRAS M. MARTON
Colonel, JA
Senior Component Official for Privacy

Attachment
USTRANSCOM Response

cc: TCJA

(U) U.S. Transportation Command Senior Component Official for Privacy (cont'd)

DOD IG Draft Report (Project No. D2021-D000CP-0034.002)
"Audit of The U.S. Transportation Command's Compliance with the Federal Information Security Modernization Act of 2014," dated 23 January 2023

Recommendation 2: (U) We recommend that the U.S. Transportation Command Senior Component Official for Privacy:

a. (U) Establish controls to ensure that the Privacy Act Program Manager properly reports all breaches in accordance with U.S. Transportation Command guidance.

USTRANSCOM Position: Concur. USTRANSCOM submitted changes to its internal policy updating USTRANSCOM Instruction 5050-03 "Privacy and Civil Liberties," which included necessary changes to align with DOD Manual 5400.11, Volume 2, "DOD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan," dated 6 May 2021.

Estimated Completion Date (ECD): 8 May 2023

b. (U) Update U.S. Transportation Command Instruction 33-35, "Privacy Act and Civil Liberties Program," dated 4 February 2016, to align with DOD Manual 5400.11, Volume 2, "DOD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan," dated 6 May 2021, including the changes to the breach reporting process.

USTRANSCOM Position: Concur. USTRANSCOM submitted changes to internal policy updating USTRANSCOM Instruction 5050-03, which included necessary changes to breach reporting processes to align with DOD Manual 5400.11, Volume 2.

Estimated Completion Date (ECD): 8 May 2023

c. (U) Update U.S. Transportation Command Instruction 33-35, "Privacy Act and Civil Liberties Program," dated 4 February 2016, to provide minimum frequency and content requirements for U.S. Transportation Command privacy awareness training.

USTRANSCOM Position: Concur. USTRANSCOM submitted changes to internal policy updating USTRANSCOM Instruction 5050-03, which included necessary changes to provide minimum frequency and content requirement for USTRANSCOM privacy awareness training.

Estimated Completion Date (ECD): 8 May 2023

d. (U) Develop and implement procedures sufficient to ensure that all U.S. Transportation Command personnel receive annual privacy awareness training that addresses each of the key elements required by updated U.S. Transportation Command Instruction guidance.

USTRANSCOM Position: Concur. USTRANSCOM submitted changes to internal policy updating USTRANSCOM Instruction 5050-03, which included necessary changes to ensure USTRANSCOM personnel receive annual privacy awareness training addressing each of the required key elements. Additionally, USTRANSCOM is including the training in the internal USTRANSCOM Learning Management System as an annual requirement for all personnel.

Estimated Completion Date (ECD): 8 May 2023

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