OFFICE OF INSPECTOR GENERAL

Cybersecurity System Review of the Transportation Security Administration's Selected High Value Asset

Homeland Security

August 28, 2023

OIG-23-44

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

August 28, 2023

MEMORANDUM FOR: The Honorable David P. Pekoske
Administrator
Transportation Security Administration

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI Digitally signed by JOSEPH V CUFFARI Date: 2023.08.28 10:27:51 -04'00'

SUBJECT: *Cybersecurity System Review of the Transportation Security Administration's Selected High Value Asset*

Attached for your action is our final report, *Cybersecurity System Review of the Transportation Security Administration's Selected High Value Asset*. We incorporated the formal comments provided by your office.

The report contains 12 recommendations aimed at actions that the Transportation Security Administration can take to enhance the security of a selected High Value Asset system. TSA concurred with the recommendations. Based on information provided in your response to the draft report, we consider all 12 recommendations open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please contact me with any questions, or your staff may contact Kristen Bernard, Acting Deputy Inspector General for Audits, at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS

Cybersecurity System Review of the Transportation Security Administration's Selected High Value Asset

August 28, 2023

Why We Did This Review

Across the Federal Government, agencies operate critical information systems, also known as HVAs, that contain sensitive information or support critical services. We conducted this review to determine whether TSA implemented effective technical controls to protect the sensitive information that is processed by a selected HVA system.

What We Recommend

We made 12 recommendations to improve TSA's protection of the sensitive information processed by the selected HVA system.

For Further Information:
Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

The Transportation Security Administration (TSA) did not implement effective technical controls to protect the sensitive information processed by the selected High Value Asset (HVA) system. In our review and testing of this HVA, we identified security deficiencies in 8 of 10 security and privacy controls from National Institute of Standards and Technology Special Publication 800-53. Specifically, we identified deficiencies in:

- configuration management;
- risk assessment;
- supply chain risk management;
- access control;
- planning;
- awareness and training;
- assessment, authorization, and monitoring; and
- contingency planning.

The deficiencies we identified demonstrate that TSA must strengthen its management of the selected HVA system to ensure compliance with policies designed to protect sensitive information processed in the system. Until these deficiencies are addressed, TSA is less equipped to protect the selected HVA system and cannot ensure it will be able to quickly detect, respond to, and recover from a cyberattack.

TSA Response

TSA concurred with all 12 recommendations. We included a copy of TSA's comments in Appendix B.

Table of Contents

Appendixes

Abbreviations

CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
DISA	Defense Information Systems Agency
ECD	Estimated Completion Date
FISMA	*Federal Information Security Modernization Act*
HVA	High Value Asset
IT	information technology
KEV	Known Exploited Vulnerabilities
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
POA&M	Plans of Action and Milestones
SP	Special Publication
STIG	Security Technical Implementation Guide
TSA	Transportation Security Administration

Background

The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately, the American people's security and privacy. Therefore, the President has directed the Federal Government to improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors.[1] The use of information technology (IT) systems and data can also introduce risk in an increasingly digital and mobile environment. In recent years, the Federal Government has seen numerous information security incidents affecting the integrity, confidentiality, and/or availability of Government information, systems, and services. The Department of Homeland Security Office of Inspector General and the U.S. Government Accountability Office (GAO) have both identified preventing cyberattacks as a major management and performance challenge.[2]

In response to these threats, in 2015, the Office of Management and Budget (OMB) created the High Value Asset (HVA) security initiative, which required large Federal agencies to identify their most critical assets.[3] Across the Federal Government, agencies operate HVAs that contain sensitive information or support critical services. HVAs include Federal information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to national security interests, foreign relations, the economy, safety, and the security of the American people.[4] In 2018, OMB issued additional guidance, stating agencies may designate Federal information or an information system as an HVA when it is related to any of the following categories: Informational Value, Mission Essential, or Federal Civilian Enterprise Essential.[5]

DHS issued, through the Cybersecurity and Infrastructure Security Agency (CISA),[6] supplemental guidance to Federal agencies for HVA programs. Specifically, CISA categorizes HVA systems into Tier 1 and Non-Tier 1. Tier 1 HVAs represent systems of critical impact to both the agency and the Nation. Non-Tier 1 HVAs represent systems of significant impact to both the agency and the Nation.

---

[1] Executive Order 14028, *Improving the Nation's Cybersecurity*, May 17, 2021.
[2] *Department of Homeland Security's Annual Performance Report (APR) for FY 2021-2023*.
[3] OMB M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirement*, October 30, 2015.
[4] OMB M-17-09, *Management of Federal High Value Assets*, December 9, 2016.
[5] OMB Memorandum-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, December 10, 2018.
[6] High Value Asset Program Management Office.

Guidelines and best practices are in place to help Federal agencies manage security risks and protect their information systems, including HVAs. For example, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53[7] provides guidance for selecting security controls to achieve more secure information systems and effective risk management in the Federal Government. NIST also provides agencies with a common structure to identify and manage cybersecurity risks across the enterprise, in alignment with five functions from its Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover).[8]

The Transportation Security Administration (TSA) was created to oversee security in all modes of transportation and completed federalization of security operations by the end of 2002. TSA makes up a quarter of the DHS workforce and is responsible for the security of commercial and general aviation; mass transit systems; freight and passenger rail; and highways, pipelines, and ports.

We conducted this review as part of our *Federal Information Security Modernization Act of 2014* (FISMA) oversight to determine whether TSA implemented effective technical controls to protect the sensitive information processed by a selected HVA system. We randomly selected one HVA (hereafter referred to as "the selected HVA system") for this review. TSA has designated the selected HVA system as *Tier 1* and categorized it with an overall *Security Categorization*[9] as "High," including "High" for all three security objectives (*Confidentiality*, *Integrity*, and *Availability*). This report is one from a series of reviews on the Department's HVAs. We plan to incorporate the results from this review into our fiscal year 2023 FISMA submission.

Results of Review

TSA did not implement effective controls to protect the sensitive information processed by the selected HVA system. Based on our review and testing of the selected HVA system, we identified security deficiencies in 8 of 10 security and

[7] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.
[8] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018.
[9] Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization in accomplishing its assigned mission, protecting its assets, fulfilling its legal responsibilities, or maintaining its day-to-day functions when certain events occur that may affect the information and information systems needed by the organization.

privacy controls from NIST SP 800-53. Specifically, we identified deficiencies in:

- configuration management;
- risk assessment;
- supply chain risk management;
- access control;
- planning;
- awareness and training;
- assessment, authorization, and monitoring; and
- contingency planning.

The deficiencies we identified demonstrate that TSA must strengthen its management of the selected HVA system to ensure compliance with policies designed to protect sensitive information processed in the system. Until these deficiencies are addressed, TSA is less equipped to protect the selected HVA system and cannot ensure it will be able to quickly detect, respond to, and recover from a cyberattack.

TSA Did Not Implement Effective Security and Privacy Controls to Protect Sensitive Information Processed by the Selected HVA System

TSA did not implement effective controls for the selected HVA system in accordance with Federal and departmental requirements. Specifically, TSA did not implement 8 of 10 NIST SP 800-53 control families,[10] which correspond to 4 of 5 functions in the NIST Cybersecurity Framework needed to protect the sensitive information processed by the selected HVA system. Since we completed our review, TSA has taken steps to correct the deficiencies we identified. For example, according to TSA, it has applied security patches to remediate the vulnerabilities we identified.[11] TSA officials also stated the component is working to strengthen its policies and procedures covering areas such as user account management, supply chain risk management, and contingency planning.

Table 1 shows the deficiencies we identified through control family testing and the corresponding functions in the NIST Cybersecurity Framework.

[10] According to NIST SP 800-53 Revision 5, there are 20 control families. Our review focused on 10 of 20 control families listed in NIST SP 800-53 Revision 5.
[11] We did not perform technical testing to verify if TSA had remediated the vulnerabilities identified because our fieldwork had concluded.

Table 1. Deficiencies Identified in NIST SP 800-53 Control Families Tested and Corresponding Functions in the NIST Cybersecurity Framework

NIST SP 800-53		NIST Cybersecurity Framework	
Control Family Tested	Deficiencies Identified	Function	FISMA Domain
Risk Assessment	Yes	Identify	Risk Management
Supply Chain Risk Management	Yes		Supply Chain Risk Management
Configuration Management	Yes	Protect	Configuration Management
Access Control	Yes		Identity and Access Management
Planning	Yes		Identity and Access Management
Audit and Accountability	No		Data Protection and Privacy
Awareness and Training	Yes		Security Training
Assessment, Authorization, and Monitoring	Yes	Detect	Information Security Continuous Monitoring
Incident Response	No	Respond	Incident Response
Contingency Planning	Yes	Recover	Contingency Planning

Source: DHS OIG-compiled based on NIST SP 800-53, NIST Cybersecurity Framework, and FY 2023 FISMA reporting metrics

Control Family 1 – Risk Assessment

TSA Did Not Remediate Critical and High-Risk Vulnerabilities

TSA did not ensure all known software updates were promptly applied to the assessed servers and workstations to remediate critical and high-risk vulnerabilities, as required by the Department. Through our vulnerability assessments of the selected HVA system, we identified 274 unique critical and high-risk vulnerabilities on servers and workstations; TSA had not addressed these vulnerabilities within DHS' remediation compliance timeframes. For example, we identified three unique vulnerabilities (two critical and one

high-risk) related to a specific weakness that occurred 99 times. Table 2 shows the results of our vulnerability assessment.

Table 2. Vulnerability Assessment Results

Operating System	Assets Scanned	Unique Critical Vulnerabilities	Unique High-Risk Vulnerabilities	Critical Vulnerability Instances	High-Risk Vulnerability Instances
Server Operating System A	9	0	1	0	6
Server Operating System B	24	0	4	0	50
Server Operating System C	29	3	12	68	123
Workstation Operating System	1,024	93	161	6,263	16,771
Total	**1,086**	**96**	**178**	**6,331**	**16,950**

Source: DHS OIG technical testing

According to TSA, in May 2022, its vulnerability management software became unable to deploy patches to more than 700 workstations. This issue occurred because these workstations were configured with the same Globally Unique Identifier.[12] Additionally, TSA officials stated that the component's vulnerability assessment software applications have not been able to communicate with, and collect data from, these workstations since August 2022.

DHS requires that information security patches be installed in accordance with component plans, following the timeline for remediation published by the DHS Enterprise Security Operations Center.[13] In addition, CISA Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities,* established a CISA-managed catalog of Known Exploited Vulnerabilities (KEV) that pose significant risk to the Federal enterprise.

[12] A Globally Unique Identifier is a unique string used to differentiate one computer from another. If multiple devices have the same Globally Unique Identifier, applications that deploy patches or assess vulnerabilities cannot properly request or receive information from the devices.
[13] DHS Policy Directive 4300A, *Information Technology System Security Program, Sensitive Systems* (ITSSP SS), Version 13.2, September 20, 2022.

Federal civilian agencies must identify and remediate these KEVs on their information systems according to the timelines set forth in the KEV catalog.

During the period from May 2022 until the end of our testing in November 2022, CISA added 203 vulnerabilities to the KEV catalog. However, because TSA's vulnerability management software was unable to communicate with some workstations, TSA could not deploy patches to address these vulnerabilities. As shown in Table 3, 12 of the unique vulnerabilities we identified during our vulnerability assessment were also published in CISA's KEV catalog. The 12 vulnerabilities occurred 431 times on the workstations and servers we assessed, giving attackers more opportunity to exploit these unpatched weaknesses.

Table 3. KEV Catalog Vulnerabilities Identified on Assessed TSA Workstations[14]

Operating System	Unique KEV Critical Vulnerabilities	Unique KEV High-Risk Vulnerabilities	Critical KEV Vulnerability Instances	High-Risk KEV Vulnerability Instances
Workstation Operating Systems	3	9	13	418
Total	**3**	**9**	**13**	**418**

Source: DHS OIG technical testing

Further, we requested a copy of the selected HVA system's patch management policy at the beginning of this review. We learned that TSA only created the selected HVA system's *Patch Management Policy*, dated November 17, 2022, after we held an entrance conference for this review and requested the document.

Control Family 2 – Supply Chain Risk Management

TSA Did Not Have an HVA System-specific Plan for Supply Chain Risk Management

The system administrators stated that TSA did not currently have a system-specific plan for managing the selected HVA system's supply chain risks. In response to our review, the component is currently drafting one. Similarly, according to selected HVA system administrators, TSA does not have an overall supply chain risk management plan for its IT assets but was developing a draft at the time of our review.

[14] We did not identify CISA KEV vulnerabilities on 62 servers tested under Table 2.

Supply chains produce the information, communications, and operational technology products and services that power the U.S. economy.[15] NIST requires organizations to develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of systems, system components, or system services.[16] Additionally, Executive Order 14028 directs agencies to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software.[17]

Control Family 3 – Configuration Management

TSA Did Not Implement All Required Configuration Management Settings for the Selected HVA System

TSA has not implemented all required configuration management settings or obtained the required waivers for noncompliant settings on the selected HVA system. To determine whether TSA had implemented the DHS-required baseline configuration settings, we performed technical testing on selected servers and workstations to assess the selected HVA system's compliance with applicable Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs). Table 4 summarizes TSA's compliance with DISA STIG configuration management security settings:

Table 4. Configuration Management Assessment Results

Operating System	Assets Scanned	DISA STIG Compliance Percentage
Server Operating System A	9	79%
Server Operating System B	24	96%
Server Operating System C	29	94%
Workstation Operating System	1,024	72%
Total	**1,086**	**--**

Source: DHS OIG technical testing

[15] *National Cybersecurity Strategy*, March 2023.
[16] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.
[17] Executive Order 14028, *Improving the Nation's Cybersecurity*, May 12, 2021.

NIST requires agencies to develop, document, and implement a configuration management plan and document a current baseline configuration of the system. In addition, NIST requires that system baseline configurations be documented, formally reviewed, and agreed upon.[18] TSA did not provide sufficient documentation to support that it had established a secure baseline configuration of the selected HVA system or to confirm whether any settings were different from the DISA STIG requirements.

Control Family 4 – Access Controls

TSA's Policies and Procedures for Administering System User Accounts Did Not Meet All NIST and DHS Standards

TSA could not provide adequate documentation of its access agreement policies or procedures. NIST requires that (1) access agreements be developed and documented; (2) access agreements be reviewed and updated at a frequency determined by the organization; and (3) organizations verify that individuals sign appropriate access agreements before being granted access to systems.[19] Similarly, DHS requires users to sign access agreements before being granted access to systems; components to document access agreements for information systems; and system owners to review information system accounts supporting their programs at least annually.[20]

To determine whether users were given proper access to the selected HVA system, we asked system administrators for the system's access control policy and procedures when we began our review in October 2022. Subsequently, system administrators for the selected HVA provided us with the *User Access Request Standard Operating Procedure (SOP)*, dated November 9, 2022; they could not provide documentation to prove a prior version of the document existed. We reviewed the *User Access Request Standard Operating Procedure (SOP)* and determined it did not address all NIST and DHS requirements for managing user access. Specifically, the document did not:

- ensure access agreements were developed and documented for the selected HVA system;
- ensure individuals requiring access to the selected HVA system sign access agreements before being granted access;

[18] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.
[19] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.
[20] DHS Policy Directive 4300A, *Information Technology System Security Program, Sensitive Systems*, Version 13.2, September 20, 2022.

- require access agreements be re-signed by all parties when agreements have been updated; or
- require access agreements be reviewed at least annually.

We also requested the policy for privileged users of the selected HVA system. In response, system administrators provided us with TSA 1400-501, *Privileged Access Standard Operating Procedure*, which was not dated. The *Privileged Access Standard Operating Procedure* did document the use of access agreements, as required by NIST and DHS.

TSA Did Not Maintain Current User Lists for the Selected HVA System

TSA does not maintain a current list of the selected HVA system users and their authorized level of access. NIST requires that the types of accounts allowed and specifically prohibited for use within a system be defined and documented. Additionally, authorized users of the system, group and role membership, and access authorizations (i.e., privileges) should be specified for each account.[21]

TSA did not provide an accurate or current list of selected HVA system users. System administrators initially stated that the selected HVA system had 859 active users. Subsequently, TSA provided us with a list of 3,228 users who were assigned to the various system membership groups. When asked about the discrepancy, system administrators for the selected HVA stated they were not sure of the exact number of active HVA system users but estimated the number was probably more than 3,000. Based on our review of the information TSA provided, we determined 858 (849 non-privileged and 9 privileged) users had logged onto the selected HVA system from November 8, 2021, through November 8, 2022.

TSA also could not provide system documentation defining the user groups. Our review of various documents revealed discrepancies. For example, TSA identified 5 groups in the *System Security Plan* and 13 groups in the *System Design Document*. However, we identified 30 groups in a membership group list TSA provided. In addition, TSA could not confirm whether any users had been granted emergency or temporary access to the system. Lastly, we determined the system had legacy administrator groups that were not in use but had not yet been removed.

[21] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.

TSA Did Not Ensure That Access for Non-Privileged Users Was Always Authorized, Updated, or Removed, as Required

TSA did not implement effective controls for the selected HVA system to ensure non-privileged users' system access was properly authorized, updated as necessary, and removed according to established procedures. Both NIST and DHS require that access agreements be developed and documented.[22] DHS requires that access be reviewed at least annually. TSA requires that user accounts be disabled after a period of inactivity for systems categorized as having a "High" impact on the *Confidentiality* security objective.

TSA could not provide user access request documentation to prove access was authorized or approved for a sample of 40 non-privileged users of the selected HVA system. Without the supporting documentation, we could not determine if access was properly authorized according to an established procedure. Further, 372 of 849 non-privileged users (44 percent) had not logged onto the system for an extended period, contrary to TSA's policy.

TSA Did Not Always Ensure That Access for Privileged Users Was Authorized, Updated, or Removed, as Required

TSA did not ensure access for privileged users of the selected HVA system was properly authorized, updated as necessary, and removed according to established procedures. Although TSA provided us with a list of 61 privileged users, it did not maintain their authorized level of access.

To determine if access was authorized according to established procedures, we judgmentally sampled 9 of the 61 privileged users and requested documentation associated with their access requests. After reviewing the documentation TSA provided, we determined the access request forms (TSA Form 1429) for two of nine privileged users sampled were not completed and signed, as required. Specifically, we found an instance in which TSA had identified one user as a privileged user on a list provided to us on November 4, 2022, but this user's TSA Form 1429 was not signed until after we requested the information on November 17, 2022. Also, TSA could not provide the TSA Form 1429 for a second user but did provide online approvals to prove access was authorized. However, without the applicant's signature date on the request form, we could not conclude when the access was requested and when the form was signed.

[22] *Id.* DHS Policy Directive 4300A, *Information Technology System Security Program, Sensitive Systems*, Version 13.2, September 20, 2022.

Further, we determined that 54 of 61 privileged users had not logged onto the system for an extended period, contrary to TSA policy. TSA did not provide evidence these accounts were disabled, as required. Further, we reviewed TSA's Annual Privilege Audit in the *Security Assessment Report Version 1.2*, which included the results for the selected HVA system, but was not signed or dated. Because the Annual Privilege Audit was not signed or dated, we could not determine whether the system owner had reviewed which users had privileged access to the selected HVA system at least annually and when major changes occurred to the system environments, as required.

TSA Did Not Effectively Track and Manage Separated Individuals' Selected HVA System Access

TSA does not have an effective process to manage user account access for the selected HVA system when employees and contractors separate from the component. TSA requires that TSA Form 1402, *Separating Non-Screener Employee and Contractor IT Certificate*, be completed by separating employees and signed by the employee's supervisor.[23] In addition, TSA requires that the signed TSA Form 1402 be maintained by the individual's supervisor for Federal employees, and by the contracting officer's representative for contractors, and retained in accordance with TSA retention schedules.

We determined that TSA did not remove access for separated individuals, as required. Initially, system administrators identified one HVA system user who had separated from the component within the 12 months before our review (from November 8, 2021, through November 8, 2022) whose access should have been removed but was not. Subsequently, we obtained and analyzed records from TSA Human Resources for the same 12-month period and identified 60 separated employees and contractors who inappropriately retained access to the system. In response to our analysis, the Information System Security Officer disputed the two previously provided figures (1 and 60) but confirmed that 17 of the 60 employees and contractors should have had their system access removed. However, the Information System Security Officer did not provide an explanation of how the 17 individuals were determined. We also requested documentation to support whether TSA had removed or disabled the system access for these 17 individuals. TSA did not provide a TSA Form 1402, TSA Form 1429 for account removal, or any other documentation to show the access had been removed. Without supporting documents, we could not determine if the user accounts were properly disabled and removed, as required.

[23] *TSA Information Assurance Handbook*, Version 14.0, July 27, 2018.

Control Family 5 – Planning

Four of 50 Selected Users Had Not Acknowledged the Rules of Behavior/Computer Access Agreement

TSA did not ensure all selected HVA system users acknowledged and signed the rules of behavior presented in the Computer Access Agreement. DHS requires that components train users on rules of behavior and that each user signs a rules of behavior agreement before being granted a user account or access to information systems or data.[24] In addition, components must develop specific rules of behavior for their information systems, ensure users of the systems read and acknowledge the rules via physical or electronic signature, and maintain the signed rules of behavior.[25] Further, users must sign the system rules of behavior before being granted access to the system.[26]

We reviewed the Computer Access Agreements for a sample of 50 HVA system users to determine if they had acknowledged the rules of behavior and signed off on these rules before being granted access to the selected HVA system, as required. We found 4 of 50 users had access to the system even though they had not acknowledged and signed a Computer Access Agreement.

Control Family 6 – Awareness and Training

Three of 51 System Users Did Not Receive Required Training

TSA did not ensure all HVA system users received the required security awareness training. FISMA, OMB, and DHS all require agencies to provide security awareness training annually to educate employees and contractors about information security risks, teach them how to reduce these risks, and make them aware of their security responsibilities.[27]

We judgmentally selected 51 HVA system users and requested training records to ensure the selected users received security awareness training from May 2021 through November 2022. Based on this review, we determined that 3 of 51 users sampled did not receive the required security awareness training. Of the three users who did not complete the required security awareness training, two were non-privileged users and one was a privileged user.

[24] DHS Policy Directive 4300A, *Information Technology System Security Program, Sensitive Systems*, Version 13.2, September 20, 2022.
[25] DHS Policy Directive 4300A, *Information Technology System Security Program, Sensitive Systems,* Attachment G, Revision 1.0, April 2022.
[26] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.
[27] OMB Circular A-130, *Managing Information as a Strategic Resource*, July 2016.

One of Nine Privileged Users Did Not Receive Role-Based Training

Although TSA developed role-based training for privileged users of the selected HVA system, it did not ensure these users received the required training annually. DHS and NIST require agencies to provide role-based training to system users with elevated privileges. TSA did not ensure one of nine sampled privileged HVA system users received the required role-based training from May 2021 through November 2022.

Control Family 7 – Assessment, Authorization, and Monitoring

TSA Did Not Effectively and Continuously Monitor the Information Security of the Selected HVA System

TSA did not continuously monitor the information security of the selected HVA system, as required. Continuous monitoring, or Information Security Continuous Monitoring, facilitates ongoing awareness of threats, vulnerabilities, and information security to support risk-based decisions. NIST recommends that agencies establish a continuous monitoring program to collect information in accordance with preestablished metrics.[28] OMB also requires agencies to develop Plans of Action and Milestones (POA&M) to identify tasks that need to be accomplished to resolve information security weaknesses. POA&Ms should include an estimate of what it will cost to resolve the weakness.[29]

During the review, we requested multiple required policies and procedures; however, TSA could not provide evidence the provided documents had been reviewed or approved. For example, some documents were not signed until after we requested the information; and some documents contained incorrect, outdated, or incomplete information. Specifically:

- TSA's Information Assurance and Cyber Security Division provided us with the selected HVA system's draft *Continuous Monitoring Standard Operating Procedure*, dated October 2022. The document was not signed until November 18, 2022, after we requested a signed version. TSA also could not provide a version of the *Continuous Monitoring Standard Operating Procedure* that had been approved before we started our review. Additionally, the *Continuous Monitoring Standard Operating*

[28] NIST SP 800-12, Revision 1, *An Introduction to Information Security*, June 2017.
[29] OMB Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001.

Procedure does not contain procedures for testing patches before they are deployed, does not address the tools needed to deploy the patches.
- The System Security Plan identifies 5 user groups; the System Design Document identifies 13 groups; and the membership group list that TSA provided places users in 30 different groups.
- TSA has 11 open POA&Ms for the selected HVA system, 5 of which have a criticality of high. We determined that all 11 POA&Ms were overdue. The oldest POA&M was dated September 22, 2017, meaning that it had been open for more than 5 years. In addition, selected HVA system administrators did not always include estimates for resources needed to mitigate identified weaknesses in the POA&Ms, as required by OMB and DHS. Specifically, 5 of the 11 POA&Ms did not identify an associated cost estimate.
- TSA could not provide evidence that the selected HVA system's Contingency Plan and Contingency Plan Test results had been reviewed and approved.

Control Family 8 – Contingency Planning

TSA's Contingency Planning for the Selected HVA System Was Not Effective

TSA did not perform effective contingency planning for the selected HVA system. DHS and NIST require that components' Chief Information Officers review and approve component-level information system contingency plans.[30] OMB requires agencies to develop POA&Ms to identify tasks that need to be accomplished to resolve information security weaknesses. POA&Ms should include an estimate of what it will cost to resolve the weakness.[31]

We assessed the selected HVA system's Contingency Plan and Contingency Plan Testing and found no evidence that the Contingency Plan was reviewed and approved or tested, as required. For example, both documents were not signed. The Contingency Plan, dated August 2022, references a version of NIST SP 800-53 (revision 4) that has been outdated since September 2020 when NIST issued revision 5. According to the Contingency Plan Testing, which is dated March 2022, the selected HVA system does not have an alternate process site capability, which should be captured and monitored as a security

[30] DHS Policy Directive 4300A, *Information Technology System Security Program, Sensitive Systems* (ITSSP SS), Version 13.2, September 20, 2022. NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.
[31] OMB Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001.

weakness until it is remediated.[32] The date for the data center failover site completion is listed as "To Be Determined."

We also reviewed the selected HVA system's existing POA&Ms to determine whether TSA had captured and monitored the remediation status, as required. One of the overdue POA&Ms, related to Contingency Plan Testing, was created on November 4, 2020, with a scheduled completion date of December 19, 2020. However, this POA&M is listed as "delayed" in the DHS Enterprise management tool and has been past due for more than 2 years. Additionally, the estimated cost associated with this POA&M is $0, which does not comply with applicable OMB and DHS policies to include an estimated cost for resolving identified weaknesses.

TSA Needs to Strengthen its Management of the Selected HVA System

The issues we identified occurred primarily due to inadequate management oversight and because TSA did not have an effective Information Security Continuous Monitoring program, as defined by NIST, to ensure the selected HVA system was properly managed according to applicable Federal and Department requirements.

According to NIST, the authorizing official should be provided with current and accurate security information to make risk-based decisions about the system. The following security control deficiencies we identified demonstrate that TSA must strengthen its management of the selected HVA system to ensure compliance with Federal and DHS policies designed to protect the sensitive information processed by the selected HVA system:

- TSA vulnerability management software became unable to deploy patches to more than 700 workstations in May 2022. Additionally, TSA's vulnerability assessment software applications have not been able to communicate with and collect data from these workstations since August 2022, meaning that TSA cannot deploy patches to address new vulnerabilities added to the KEV catalog.
- TSA did not have an accurate user list for the selected HVA system.
- The *Continuous Monitoring Standard Operating Procedure*, dated October 2022, was not signed until November 18, 2022, only after we requested a signed version.
- A POA&M for conducting contingency plan testing on the selected HVA system, listed as "delayed" in the POA&M database, has been past due for more than 2 years, and did not include all required information.

[32] *Id.*

- The System Security Plan contains outdated information about the selected HVA system.
- TSA did not remove separated individuals' access to the selected HVA system.
- TSA did not disable inactive accounts for the selected HVA system.
- 54 of 61 privileged users had not logged onto the selected HVA system for an extended period.
- TSA did not have accurate documentation defining the selected HVA system's user groups.

Conclusion

Without effective controls in place to better manage the selected HVA system, TSA cannot be assured that sensitive information processed by the system is protected and secure. In addition, the authorizing official cannot make credible, risk-based decisions about the system without the most current and accurate system information. Until these deficiencies are addressed, TSA is less equipped to protect the selected HVA system and cannot ensure it will be able to quickly detect, respond to, and recover from a cyberattack.

Recommendations

Recommendation 1: We recommend the TSA Chief Information Officer require the selected High Value Asset system owner to document an approved secure baseline configuration and perform testing to verify that all approved settings are implemented.

Recommendation 2: We recommend the TSA Chief Information Officer enforce the requirement for the selected High Value Asset system owner to apply security updates and service patches to remediate vulnerabilities on all devices, as required by applicable DHS policies.

Recommendation 3: We recommend the TSA Chief Information Officer require the selected High Value Asset system owner to develop and implement a supply chain risk management plan to address and mitigate risks associated with the hardware components and software being used on the selected High Value Asset system.

Recommendation 4: We recommend the TSA Chief Information Officer direct the selected High Value Asset system owner to strengthen its user account management procedures to ensure user access agreements are developed and signed by users before users are given access to the selected High Value Asset system or when the agreement is revised.

Recommendation 5: We recommend the TSA Chief Information Officer require the selected High Value Asset system owner develop and implement detailed procedures on granting system access, including emergency or temporary access. In addition, the TSA Chief Information Officer should require the selected High Value Asset system owner to maintain a current list of system users and remove or disable inactive accounts according to applicable DHS and TSA policies.

Recommendation 6: We recommend the TSA Chief Information Officer direct the selected High Value Asset system owner to require all non-privileged users' system access requests be reviewed, authorized, and documented before granting system access. In addition, users' system access should be reviewed periodically and removed if it is no longer needed.

Recommendation 7: We recommend the TSA Chief Information Officer direct the selected High Value Asset system owner to review and document the approval of all privileged users' system access before granting system access. In addition, privileged users' system access should be reviewed and removed according to applicable DHS and TSA requirements if it is no longer needed.

Recommendation 8: We recommend the TSA Chief Information Officer require the selected High Value Asset system owner to develop and implement procedures to remove system access for separated users.

Recommendation 9: We recommend the TSA Chief Information Officer direct the selected High Value Asset system owner to require all system users sign Computer Access Agreements to acknowledge the rules of behavior when accessing the system.

Recommendation 10: We recommend the TSA Chief Information Officer direct the selected High Value Asset system owner to enforce users to receive security awareness training when they are given system access and annually thereafter.

Recommendation 11: We recommend the TSA Chief Information Officer direct the selected High Value Asset system owner to strengthen its system-level Information Security Continuous Monitoring by ensuring (1) security documents contain current and accurate information about the system; (2) relevant policies and procedures are developed, reviewed, and approved; and (3) Plans of Action and Milestones are remediated promptly and include all required information.

Recommendation 12: We recommend the TSA Chief Information Officer require the selected High Value Asset System's Contingency Plan and Contingency Plan Test to be reviewed and approved in accordance with DHS and National Institute of Standards and Technology guidance.

TSA Comments and OIG Analysis

We obtained written comments on a draft of this report from TSA. We reviewed TSA's management comments, as well as the technical comments previously submitted and updated the report as appropriate. TSA concurred with all 12 recommendations, which we consider resolved and open. In the comments, TSA indicated it appreciated our work on this review. TSA said it remains committed to implementing effective security controls to protect sensitive information processed in its HVA systems. A summary of TSA's responses and our analysis follows.

TSA Comments to Recommendation #1: Concur. TSA currently secures all baseline configuration of the selected HVA in accordance with applicable DISA STIG requirements. TSA continuously reviews the configuration management process and will make updates to the process as appropriate to ensure industry best practices. Estimated Completion Date (ECD): August 30, 2024.

OIG Analysis: TSA's actions are responsive to the recommendation, which will remain open and resolved until TSA provides documentation showing that all planned corrective actions are completed.

TSA Comments to Recommendation #2: Concur. TSA is currently creating a management directive to formalize the change management process and procedures for the selected HVA. This directive will outline the entire asset change management process to include testing and release management. ECD: August 30, 2024.

OIG Analysis: TSA's actions are responsive to the recommendation, which will remain open and resolved until TSA provides documentation showing that all planned corrective actions are completed.

TSA Comments to Recommendation #3: Concur. The owner of the selected HVA is currently working with stakeholders to develop a specific plan for each system. The policy and plan documents will impact and require approvals by many stakeholders before implementation. ECD: August 29, 2025.

OIG Analysis: TSA's actions are responsive to the recommendation, which will remain open and resolved until TSA provides documentation showing that all planned corrective actions are completed.

TSA Comments to Recommendation #4: Concur. The system owner of the selected HVA system will continuously review, and audit to verify, that the users have an up-to-date agreement to validate system access authorization. TSA is also implementing an automated capability to support its login policy, as well as updating its system to track and provide reports on all users to further support account management. ECD: August 30, 2024.

OIG Analysis: TSA's actions are responsive to the recommendation, which will remain open and resolved until TSA provides documentation showing that all planned corrective actions are completed.

TSA Comments to Recommendation #5: Concur. The selected HVA system owner is working with TSA Training and Development and its Online Learning Center to coordinate for user training. In addition, the system owner is coordinating with TSA Information Technology to strengthen access approval procedures and implement an automated capability to remove or disable inactive accounts according to DHS and TSA policies. ECD: August 30, 2024.

OIG Analysis: TSA's actions are responsive to the recommendation, which will remain open and resolved until TSA provides documentation showing that all planned corrective actions are completed.

TSA Comments to Recommendation #6: Concur. TSA is currently reviewing and strengthening its process to document and route all non-privileged users for Information Systems Security Officer and system owner approval and have monthly manual reviews of all active accounts to ensure non-privileged users who have access are still active and require accounts. ECD: August 30, 2024.

OIG Analysis: TSA's actions are responsive to the recommendation, which will remain open and resolved until TSA provides documentation showing that all planned corrective actions are completed.

TSA Comments to Recommendation #7: Concur. The selected HVA system owner will review and document the approval of all privileged users' system access before granting system access. Also, the selected HVA system owner is implementing automated procedures to deactivate inactive accounts. ECD: August 30, 2024.

OIG Analysis: TSA's actions are responsive to the recommendation, which will remain open and resolved until TSA provides documentation showing that all planned corrective actions are completed.

TSA Comments to Recommendation #8: Concur. TSA is currently implementing an automated process to deactivate inactive accounts as required. The selected HVA system owner or authorized supervisor will continue to validate user access periodically to ensure the user requires continued access to the system and correct privileges have been assigned. ECD: August 30, 2024.

OIG Analysis: TSA's actions are responsive to the recommendation, which will remain open and resolved until TSA provides documentation showing that all planned corrective actions are completed.

TSA Comments to Recommendation #9: Concur. The selected HVA system owner is working with stakeholders to require points of contact in the field to complete Computer Access Agreements and to document their acknowledgement of the rules of behavior when accessing the system. ECD: August 30, 2024.

OIG Analysis: TSA's actions are responsive to the recommendation, which will remain open and resolved until TSA provides documentation showing that all planned corrective actions are completed.

TSA Comments to Recommendation #10: Concur. The selected HVA system owner is working with stakeholders to review and strengthen its process to document completions of cybersecurity awareness training. No user will be granted access to the selected HVA system until training has been confirmed and documented. The selected HVA Information System Security Officer and system-owner will perform monthly manual reviews of all active accounts. ECD: August 30, 2024.

OIG Analysis: TSA's actions are responsive to the recommendation, which will remain open and resolved until TSA provides documentation showing that all planned corrective actions are completed.

TSA Comments to Recommendation #11: Concur. TSA is currently reviewing and revising policies, procedures, and technical security documentation to support continuous monitoring and remediation actions, as appropriate. The selected HVA system owner will continue tracking and monitoring the Plans of Action and Milestones. ECD: August 30, 2024.

OIG Analysis: TSA's actions are responsive to the recommendation, which will remain open and resolved until TSA provides documentation showing that all planned corrective actions are completed.

TSA Comments to Recommendation #12: Concur. In March 2023, the selected HVA system owner completed updates to its Contingency Plan and held a Contingency Plan Test. A complete, fully functional exercise is planned in March 2024. ECD: May 31, 2024.

OIG Analysis: TSA's actions are responsive to the recommendation, which will remain open and resolved until TSA provides documentation showing that all planned corrective actions are completed.

Appendix A
Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107–296), which amended the *Inspector General Act of 1978*.

The objective of our review was to determine whether TSA implemented effective technical controls to protect the sensitive information that is processed by a selected HVA system. We focused our review on one TSA HVA system. To accomplish our objective, we determined whether TSA had developed and implemented policies and procedures in the following areas:

- patch and configuration management;
- supply chain risk management;
- user account access management;
- audit trails;
- incident response;
- security awareness and role-based training;
- contingency planning; and
- data privacy protection.

Additionally, we relied on the work of internal specialists from DHS OIG's Office of Innovation, Cybersecurity Risk Assessment Division, to perform technical assessments on the selected HVA system. Their work included patch and configuration management assessments on selected servers and workstations on the selected HVA system. The information obtained from the assessments was used to identify weaknesses such as missing security patches and misconfigured security settings. We also performed a technical assessment on the system to identify potential vulnerabilities, missing patches, and any noncompliance with applicable DISA STIG configuration settings. To ensure the accuracy of testing results and OIG reporting, TSA was given the opportunity to review our preliminary observations from testing to verify the initial testing results and to identify "false-positive" results. We reviewed TSA's feedback and updated our analysis as needed.

We also reviewed documentation and artifacts TSA provided for the selected HVA system to evaluate TSA's implementation of selected NIST SP 800-53 Revision 5 controls.[33] Additionally, we performed judgmental sampling in the areas of user account management, security awareness training, and role-

[33] NST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.

based training. We also analyzed system user and privileged user lists TSA provided and reviewed information from DHS' enterprise management system.

When writing the report, we considered the potential for sensitivity issues under DHS Management Directive 11042.1, *Safeguarding Sensitive But Unclassified Information,* and generalized findings as appropriate to avoid disclosing information designated as sensitive by the Department.

We conducted this review between September 2022 and February 2023, under the authority of the *Inspector General Act of 1978*, 5 U.S.C. §§ 401-424, and according to the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

DHS OIG's Access to DHS Information

During this review, TSA provided timely responses to our requests for information and did not deny or delay access to the information we requested.

Appendix B
TSA Comments to the Draft Report

U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

July 13, 2023

MEMORANDUM FOR: Joseph V. Cuffari, PhD
Inspector General

FROM: David P. Pekoske
Administrator
Transportation Security Administration

SUBJECT: Management Response to Draft Report: "Cybersecurity System Review of a Transportation Security Administration Selected High Value Asset"
(Project No. 22-055-AUD-TSA)

Thank you for the opportunity to comment on this draft report. The Department of Homeland Security (DHS)/Transportation Security Administration (TSA) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report on its review of a single TSA High Value Asset.

TSA leadership is pleased to note OIG's positive recognition of TSA's application of security patches to remediate identified vulnerabilities. OIG also acknowledged TSA's ongoing efforts to strengthen policies and procedures for user account management, supply chain risk management, and contingency planning. TSA remains committed to implementing effective security controls to protect sensitive information processed in High Value Asset (HVA) systems.

The draft report contained 12 recommendations with which TSA concurs. Enclosed find our detailed response to each recommendation. TSA previously submitted technical comments addressing several inaccuracies, contextuals, sensitivities and other issues under a separate cover for OIG's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Enclosure

Enclosure: Management Response to Recommendations Contained in OIG 22-055-AUD-TSA

OIG recommended that the TSA Chief Information Officer:

Recommendation 1: Require the specific High Value Asset system owner to document an approved secure baseline configuration and perform testing to verify that all approved settings are implemented.

Response: Concur. TSA currently secures all baseline configuration of the selected HVA in accordance with applicable Defense Information Systems Agency Security Technical Implementation Guide (STIG) requirements. TSA continuously reviews the configuration management process, and will make updates to the process as appropriate to ensure industry best practices. Estimated Completion Date (ECD): August 30, 2024.

Recommendation 2: Enforce the requirement for the selected High Value Asset system owner to apply security updates and service patches to remediate vulnerabilities on all devices, as required by applicable DHS policies.

Response: Concur. TSA is currently creating a management directive to formalize the change management process and procedures for the selected HVA. This directive will outline the entire asset change management process to include testing and release management. ECD: August 30, 2024.

Recommendation 3: Require the selected High Value Asset system owner to develop and implement a supply chain risk management plan to address and mitigate risks associated with the hardware components and software being used on the selected High Value Asset system.

Response: Concur. The owner of the selected HVA is currently working with stakeholders to develop a specific plan for each system that will also be in compliance with the *Federal Information Security Modernization Act of 2014* within the supported boundary. The policy and plan documents will impact and require approvals by many stakeholders before implementation. ECD: August 29, 2025.

Recommendation 4: Direct the selected High Value Asset system owner to strengthen its user account management procedures to ensure user access agreements are developed and signed by users before users are given access to the selected High Value Asset system or when the agreement is revised.

Response: Concur. The system owner of the selected HVA system will continuously review, and audit to verify, that the users have an up-to-date agreement to validate system access authorization. TSA is also implementing an automated capability to support a 45-day TSA login policy, as well as update its system to track and provide reports on all users to further support account management. ECD: August 30, 2024.

Recommendation 5: Require the selected High Value Asset system owner to develop and implement detailed procedures on granting system access, including emergency or temporary access. In addition, require the High Value Asset system owner to maintain a current list of system users and remove or disable inactive accounts according to applicable DHS and TSA policies.

Response: Concur. The selected HVA system owner is working with TSA Training and Development and its Online Learning Center to coordinate for user training. The system owner is also coordinating with TSA Information Technology to strengthen access approval procedures. The selected HVA system owner is also implementing an automated capability for a 45-day TSA login policy to remove or disable inactive accounts, in compliance with DHS and TSA policies. ECD: August 30, 2024.

Recommendation 6: Direct the selected High Value Asset system owner to require all non-privileged users' system access requests be reviewed, authorized, and documented before granting system access. In addition, users' system access should be reviewed periodically and removed if it is no longer needed.

Response: Concur. TSA is currently reviewing and strengthening its process to document and route all non-privileged users for Information Systems Security Officer (ISSO) and system-owner approval and have monthly manual reviews of all active accounts to ensure non-privileged users who have access are still active and require accounts. The selected HVA system owner is also implementing an automated capability for a 45-day TSA login policy for deactivation using a system help desk. ECD: August 30, 2024.

Recommendation 7: Direct the selected High Value Asset system owner to review and document the approval of all privileged users' system access before granting system access. In addition, privileged users' system access should be reviewed and removed according to applicable DHS and TSA requirements if it is no longer needed.

Response: Concur. The selected HVA system owner will continue to use the TSA Form 1429, "Privileged Access Request," and process to review and document the approval of all privileged users' system access before granting system access. Also, the selected HVA system owner is implementing automated

procedures for a 45-day TSA login policy for deactivation supported by a system help desk. ECD: August 30, 2024.

Recommendation 8: Require the selected High Value Asset system owner to develop and implement procedures to remove system access for separated users.

Response: Concur. TSA is currently implementing an automated process for deactivation of accounts if no log-in has occurred within 30 days for the selected HVA system as required by the TSA Form 1429 deactivation process. The selected HVA system owner or authorized supervisor will continue to validate user access monthly to ensure the user requires continued access to the system and correct privileges have been assigned. ECD: August 30, 2024.

Recommendation 9: Direct the selected High Value Asset system owner to require all system users sign Computer Access Agreements to acknowledge the rules of behavior when accessing the system.

Response: Concur. The selected HVA system owner is working with stakeholders to require points of contact in the field to complete Computer Access Agreements and to document their acknowledgement of the rules of behavior when accessing the system. ECD: August 30, 2024.

Recommendation 10: Direct the selected High Value Asset system owner to enforce users to receive security awareness training when they are given system access and annually thereafter.

Response: Concur. The selected HVA system owner is working with stakeholders to review and strengthen its process to document completions of cybersecurity awareness training. No user will be granted access to the selected HVA system until training has been confirmed and documented. The selected HVA ISSO and system-owner will perform monthly manual reviews of all active accounts. ECD: August 30, 2024.

Recommendation 11: Direct the selected High Value Asset system owner to strengthen its system-level Information Security Continuous Monitoring by ensuring (1) security documents contain current and accurate information about the system; (2) relevant policies and procedures are developed, reviewed, and approved; and (3) Plans of Action and Milestones are remediated promptly and include all required information.

Response: Concur. TSA is currently reviewing and revising policies, procedures, and technical security documentation to support continuous monitoring and remediation actions, as appropriate. The selected HVA system owner will continue tracking and monitoring the Plans of Action and Milestones. ECD: August 30, 2024.

Recommendation 12: Require the selected High Value Asset System's Contingency Plan and Contingency Plan Test to be reviewed and approved in accordance with DHS and National Institute of Standards and Technology guidance.

Response: Concur. In March 2023, the selected HVA system owner completed updates to its Contingency Plan and held a Contingency Plan Test. A complete, fully-functional exercise is planned in March 2024. ECD: May 31, 2024

5

Appendix C
Office of Audits Major Contributors to This Report

Chiu-Tong Tsang, Director, Cybersecurity and Intelligence Division
Shawn Hatch, Audit Manager
Lawrence Polk, IT Cybersecurity Specialist
Tanisha Bethea, Auditor-in-Charge
Sonya Griffin, Auditor
Bridgette OgunMokun, Auditor
Omar Russel, Auditor
Lauren Barrick, Auditor
Lance Watkins, Auditor
Thomas Rohrback, Director, Cybersecurity Risk Assessment Division
Jason Dominguez, IT Cybersecurity Specialist
Rashedul Romel, IT Cybersecurity Specialist
Taurean McKenzie, IT Specialist
Maria Romstedt, Communications Analyst
Saajan Paul, Referencer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Administrator, TSA
CIO, TSA
Audit Liaison, TSA

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" box. If you cannot access our website, call our hotline at (800) 323-8603, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305