U.S. DEPARTMENT OF HOMELAND SECURITY

OFFICE OF INSPECTOR GENERAL

OIG-24-26 June 4, 2024

FINAL REPORT

Evaluation of DHS' Information Security Program for Fiscal Year 2023

OFFICE OF INSPECTOR GENERAL
U.S. Department of Homeland Security
Washington, DC 20528 | www.oig.dhs.gov

June 4, 2024

MEMORANDUM FOR: Eric Hysen
Chief Information Officer
Department of Homeland Security

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

JOSEPH V CUFFARI Digitally signed by JOSEPH V CUFFARI Date: 2024.06.04 10:07:01 -04'00'

SUBJECT: *Evaluation of DHS' Information Security Program for Fiscal Year 2023*

Attached for your action is our final report, *Evaluation of DHS' Information Security Program for Fiscal Year 2023*. We incorporated the formal comments provided by your office.

The report contains two recommendations aimed at improving the Department's information security program. The Department concurred with both recommendations. Based on information provided in your response to the draft report, we consider both 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, Deputy Inspector General for Audits, at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS

Evaluation of DHS' Information Security Program for Fiscal Year 2023

June 4, 2024

Why We Did This Evaluation

We reviewed DHS' information security program for compliance with the *Federal Information Security Modernization Act of 2014*. We conducted our evaluation according to the fiscal year 2023 reporting instructions. Our objective was to determine whether DHS' information security program and practices were adequate and effective to protect the information and information systems that supported DHS' operations and assets for FY 2023.

What We Recommend

We made two recommendations to DHS to address the deficiencies we identified.

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

We rated the Department of Homeland Security's information security program for FY 2023 as "effective," according to this year's reporting instructions. We based this rating on our evaluation of the Department's compliance with requirements of the *Federal Information Security Modernization Act of 2014* for unclassified and national security systems. As recommended by this year's reporting instructions, we used a calculated average approach when determining the effectiveness of the domain, function, and overall program. DHS received a maturity rating of "Level 4 – Managed and Measurable" in the Identify, Protect, Detect, Respond, and Recover functions based on this year's reporting guidance.

DHS can further improve its information security program with stronger department-wide execution of its policies, procedures, and practices at all components. For example, we identified the following deficiencies:

1. Some components were operating systems without an Authority to Operate and tested contingency plans;
2. Plans of Action and Milestones were not being mitigated promptly or were not created for all information security weaknesses cited in one of our reports;
3. DHS provided conflicting guidance on how to prioritize Plans of Action and Milestones;
4. Security configuration settings were not implemented for all systems tested;
5. Some components did not promptly apply security patches to mitigate critical and high-risk security vulnerabilities on selected systems tested; and
6. Selected components had identity and access weaknesses.

DHS Response

DHS concurred with the recommendations. We included a copy of the Department's comments in Appendix B.

Table of Contents

Abbreviations

ATO	Authority to Operate
CBP	U.S. Customs and Border Protection
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CSAM	Cyber Security Assessment and Management
DISA	Defense Information Systems Agency
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Modernization Act of 2014
HQ	Headquarters
HVA	High Value Asset

ICE	Immigration and Customs Enforcement
IG	Inspector General
IT	information technology
NIST	National Institute of Standards and Technology
NSS	National Security Systems
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
Secret Service	United States Secret Service
SCRM	Supply Chain Risk Management
SP	Special Publication
STIG	Security Technical Implementation Guide
TSA	Transportation Security Administration

Background

Recognizing the importance of information security to the economic and national security interests of the United States, Congress enacted the *Federal Information Security Modernization Act of 2014* (FISMA).[1] Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.[2] FISMA provides a framework for ensuring effective security controls are in place to protect the information resources that support Federal operations and assets.[3]

FISMA focuses on program management, implementation, and evaluation of the security of unclassified systems and national security systems (NSS).[4] Specifically, FISMA requires Federal agencies to develop, document, and implement agency-wide information security programs.[5] Each program should protect the data and information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor, or source.[6] According to FISMA, agencies are responsible for conducting annual evaluations of information programs and systems under their purview. In coordination with senior agency officials, each agency's chief information officer must report annually to the agency head on the effectiveness of the agency's information security program, including progress on remedial actions.[7]

The Department of Homeland Security has various missions, such as preventing terrorism, ensuring disaster resilience, managing U.S. borders, administering immigration laws, and securing cyberspace. To accomplish its broad array of complex missions, DHS employs approximately 260,000 personnel, all of whom rely on information technology (IT) to perform their duties. It is critical that DHS provide a high level of cybersecurity[8] for the information and information systems supporting day-to-day operations.

The DHS Chief Information Security Officer (CISO) bears primary responsibility for protecting information and ensuring compliance with FISMA. The DHS CISO heads the Information Security Office and manages the Department's information security program for its unclassified systems, its national security systems classified as "Secret" and "Top Secret," and systems operated by contractors on behalf of DHS. As part of the Department's continuous monitoring strategy, DHS CISO maintains awareness of the Department's information security program through its

[1] 44 United States Code § 3551 et. seq.
[2] *Id.* at § 3552(b)(3).
[3] *Id.* at § 3551(1).
[4] DHS defines NSS as systems that collect, generate, process, store, display, transmit, or receive Unclassified, Confidential, Secret, and Top-Secret information.
[5] *Id.* at § 3554(b).
[6] *Id.* at § 3554(a)(1), (2) and 3554(b).
[7] *Id.* at § 3554(a)(5).
[8] Cybersecurity is the process of protecting information by preventing, detecting, and responding to attacks.

Continuous Diagnostics and Mitigation Program, Ongoing Authorization Program, and Network Operations Security Center.[9]

All DHS components must adhere to the IT security requirements set forth in the Department's security authorization process,[10] which involves comprehensive testing and evaluation of the security features of all information systems before these systems become operational[11] within the Department. This evaluation process results in an Authority to Operate (ATO) decision, whereby a senior official authorizes the operation of an information system based on an agreed-upon set of security controls. Per DHS guidelines,[12] each component CISO must assess the effectiveness of controls implemented before authorizing the systems to operate, and periodically thereafter. According to applicable DHS,[13] Office of Management and Budget (OMB),[14] and National Institute of Standards and Technology (NIST)[15] policies, all systems must undergo the authorization process before they become operational. The DHS CISO relies on two enterprise management systems to keep track of security authorization status and administer the information security program. Enterprise management systems also provide a means to monitor Plans of Action and Milestones (POA&M) for remediating information security weaknesses related to unclassified and Secret level systems.

FISMA Reporting Instructions

FISMA requires each agency's Inspector General (IG) to perform an annual independent evaluation to determine the effectiveness of the agency's information security program and practices. The *FY 2023 - 2024 IG FISMA Reporting Metrics*[16] (FY 2023 FISMA Reporting Metrics) provide reporting requirements for addressing key areas identified during independent evaluations of agency information security programs. IGs must assess the effectiveness of information security programs on a maturity model spectrum, in which the foundational levels ensure that agencies develop sound policies and procedures, while the advanced levels capture the extent to which agencies institutionalize policies and procedures. Within the maturity model context, agencies should perform risk assessments to identify the optimal maturity levels that achieve cost-effective security — based on mission, risks faced, risk appetites, and risk tolerance.

[9] *DHS Information Security Continuous Monitoring Strategy*, Version 5.0, May 20, 2022.
[10] NIST defines a security authorization as a management decision by a senior organizational official authorizing operation of an information system and explicitly accepting the risk to agency operations and assets, individuals, other organizations, and the Nation based on implementation of an agreed-upon set of security controls.
[11] According to DHS policy, an information system must be granted an ATO.
[12] DHS *System Security Authorization Process Guide*, Version 14.1, April 4, 2019.
[13] *Id.*
[14] *Managing Information as a Strategic Resource,* OMB Circular A-130, July 2016.
[15] *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publication (SP) 800-53, Revision 5, September 2020.
[16] The *FY 2023 FISMA Reporting Metrics*, Version 1.1, February 10, 2023, were based on coordinated discussions between representatives from OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), with review and feedback provided by several stakeholders, including the Federal CIO and CISO councils.

NIST provides agencies with a common structure to identify and manage cybersecurity risks across the enterprise, in alignment with five functions from its Cybersecurity Framework.[17]

Table 1. NIST Cybersecurity Functions and FY 2023 FISMA Domains

Cybersecurity Functions		FISMA Domains
Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	• Risk Management • Supply Chain Risk Management
Protect	Develop and implement the appropriate safeguards to ensure delivery of critical services.	• Configuration Management • Identity and Access Management • Data Protection and Privacy • Security Training
Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	• Information Security Continuous Monitoring
Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	• Incident Response
Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.	• Contingency Planning

Source: NIST Cybersecurity Framework and FY 2023 FISMA Reporting Metrics

According to the FY 2023 FISMA Reporting Metrics, OMB and the CIGIE issued guidance transitioning the IG FISMA metrics to a multi-year cycle — with a set of core metrics that must be evaluated annually, and the remaining metrics to be evaluated on a 2-year cycle, beginning in FY 2023. As required by the FY 2023 FISMA Reporting Metrics, each IG evaluates its agency's information security program for their applicability to critical efforts emanating from Executive Order 14028[18] and OMB M-23-03,[19] and cited in the reporting instructions for the five

[17] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, NIST, April 16, 2018.
[18] *Improving the Nation's Cybersecurity*, Executive Order 14028, May 12, 2021.
[19] *Memorandum for the Heads of Executive Departments and Agencies*, OMB Memorandum 23-03, December 2, 2022.

cybersecurity functions listed in Table 1. The FY 2023 FISMA Reporting Metrics provide questions that are derived from the maturity models outlined within the NIST Cybersecurity Framework. Based on its evaluation, the IG assigns each cybersecurity function a maturity level of one through five, as shown in Table 2.

Table 2. IG Evaluation Maturity Levels

Maturity Level	Maturity Level Description
Level 1 – Ad-Hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2 – Defined	Policies, procedures, and strategies are formalized and documented, but not consistently implemented.
Level 3 – Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4 – Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5 – Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on changing threats and technology landscape and business/mission needs.

Source: FY 2023 FISMA Reporting Metrics [20]

This year's reporting instructions recommend IGs use a calculated average approach when determining the effectiveness of the domain, function, and overall program.[21] According to OMB, when an information security program is rated at "Level 4 – Managed and Measurable," the program is operating at an effective level of security.

[20] The FY 2023 maturity levels were based on the FY 2023 FISMA Reporting Metrics.
[21] According to the FY 2023 FISMA Reporting Metrics, IGs use the average of the metrics in a particular domain to determine the effectiveness of individual function areas and the overall program. OMB and CIGIE determined that a non-weighted (e.g., calculated) average more closely aligned with the OIG's assessed maturity levels, expressed in a numeric format.

Scope of Our FISMA Evaluation

This report summarizes the results of our evaluation of the Department's information security program based on the FY 2023 FISMA Reporting Metrics. Our objective was to determine whether DHS' information security program and practices were adequate and effective to protect the information and information systems that support DHS' operations and assets for FY 2023. We responded to the core questions cited in the FY 2023 FISMA Reporting Metrics based on our evaluation of DHS' compliance with applicable FISMA requirements.

We performed our fieldwork at the DHS Headquarters (HQ) Office of the CISO. We also reviewed the Department's monthly FISMA Scorecards for unclassified systems and NSS; these scorecards include results from 11 components. Lastly, as part of the discretionary audits DHS OIG conducted over the past year, we performed technical testing to assess database security practices, configuration management compliance, and patch management compliance on four selected systems at three components (referred to as "Component C," "Component G," and "Component I"). These four systems were designated as High Value Assets[22] (HVAs).

Additionally, to determine whether components implemented their information security programs effectively, our independent contractor performed fieldwork at three components: U.S. Customs and Border Protection (CBP), the Transportation and Security Administration (TSA), and the United States Secret Service (Secret Service). The contractor evaluated each component based on the maturity model approach outlined in the FY 2023 FISMA Reporting Metrics and NIST's Cybersecurity Framework. We have incorporated the contractor's work in this report.

Results of Evaluation

We rated DHS' information security program for FY 2023 as "effective," according to this year's reporting instructions. We based this rating on our evaluation of the Department's compliance with requirements of the FISMA for unclassified and NSS. As recommended by this year's reporting instructions, we used a calculated average approach when determining the effectiveness of the domain, function, and overall program. Based on this year's reporting guidance, DHS received a maturity rating of "Level 4 – Managed and Measurable" in the Identify, Protect, Detect, Respond, and Recover functions.

DHS can further improve its information security program with stronger department-wide execution of its policies, procedures, and practices at all components. For example, we identified the following deficiencies:

[22] An HVA is information or an information system so critical to the Department that the loss or corruption of this information or loss of access to the system would have a serious impact on the organization's ability to perform its mission or conduct business.

1. Some components were operating systems without an Authority to Operate and tested contingency plans;
2. POA&Ms were not being mitigated promptly or were not created for all information security weaknesses cited in one of our reports;
3. DHS provided conflicting guidance on how to prioritize POA&Ms;
4. Security configuration settings were not implemented for all systems tested;
5. Some components did not promptly apply security patches to mitigate critical and high-risk security vulnerabilities on selected systems tested; and
6. Selected components had identity and access weaknesses.

DHS Improved the Effectiveness of Its Information Security Program

DHS earned a maturity rating[23] of "Level 4 – Managed and Measurable" in the Identify, Protect, Detect, Respond, and Recover functions, according to this year's reporting guidance. Table 3 summarizes the Department's FY 2022 and FY 2023 ratings.

Table 3. DHS' Maturity Level for Each Cybersecurity Function in FY 2022 and FY 2023

Cybersecurity Function		Maturity Level	
		FY 2022	FY 2023
1.	Identify	Level 4 – Managed and Measurable	Level 4 – Managed and Measurable
2.	Protect	Level 4 – Managed and Measurable	Level 4 – Managed and Measurable
3.	Detect	Level 3 – Consistently Implemented	Level 4 – Managed and Measurable
4.	Respond	Level 4 – Managed and Measurable	Level 4 – Managed and Measurable
5.	Recover	Level 4 – Managed and Measurable	Level 4 – Managed and Measurable

Source: DHS OIG analysis based on our FY 2022 report[24] and FY 2023 FISMA Reporting Metrics

To strengthen its information security program, DHS has issued or revised the following policies:

- *DHS Policy Directive Number 4300A, Information Technology System Security Program, Sensitive Systems, Attachment BB, Ongoing Authorization Program*, Version 2.0, January 26, 2023.

[23] We rated DHS' information security program according to the following five functions outlined in the 2023 reporting instructions: Identify, Protect, Detect, Respond, Recover. The five functions are based on the FY 2023 FISMA Reporting Metrics.
[24] *Evaluation of DHS' Information Security Program for Fiscal Year 2022*, OIG-23-21, August 17, 2023.

- *DHS Policy Directive Number 4300A, Information Technology System Security Program, Sensitive Systems*, *Attachment DD, DHS FISMA System Inventory Methodology,* Version 15, January 26, 2023.
- *DHS Policy Directive Number 4300A, Attachment W, Sensitive Systems Roles and Responsibilities*, Version 1.0, April 28, 2022.
- *DHS Policy Directive Number 4300A, Attachment CC, NIST 800-53r5 Control Baselines and Organizational Defined Parameters*, May 31, 2023.

DHS demonstrated a comprehensive, accurate, and near real-time centralized information system inventory through automation. Additionally, DHS demonstrated it maintains up-to-date hardware and software asset inventories, as well as an associated inventory of software licenses.

Despite the Department's actions to improve its overall information security program, we identified several deficiencies that the Department must address to strengthen its security posture. The following is a complete discussion of all progress and deficiencies we identified in each cybersecurity function as part of this evaluation.

1. Identify

The "Identify" function requires developing an organizational understanding to manage cybersecurity risks to systems, assets, data, and capabilities on two FISMA domains: (1) Risk Management and (2) Supply Chain Risk Management.

We determined DHS was operating at "Level 4 – Managed and Measurable" in the Identify function. DHS can further improve this area by enforcing applicable policies and procedures to remediate security weaknesses. For example, we identified component systems that were operating with expired ATOs. Without current ATOs, DHS cannot be assured effective controls are in place to protect sensitive information stored and processed by these systems. We also identified the following deficiencies in security weakness remediation, such as:

- several components did not effectively manage the POA&M process, as required by DHS;
- Components E and G had not created POA&Ms for the information security weaknesses identified in one of our reports; and
- conflicting guidance on how to prioritize POA&Ms.

DHS contracts with an independent auditor to develop a report of the Department's consolidated financial statements and internal control over financial reporting. In 2023, the independent auditor issued an unmodified (clean) opinion on DHS' consolidated financial

statements.[25] However, the independent auditor identified a material weakness in Information Technology Controls and Information Systems.

Risk Management

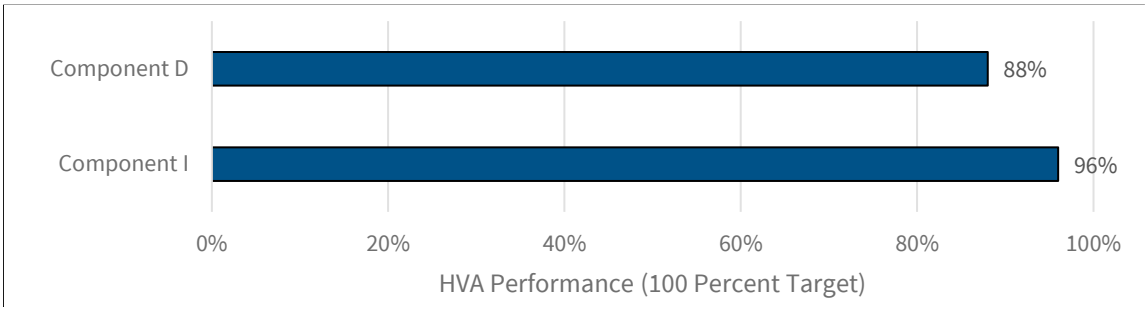
We determined DHS was operating at "Level 5 – Optimized" in the Risk Management domain of the Identify function. DHS demonstrated a comprehensive, accurate, and near real-time centralized information system inventory through automation. Additionally, DHS demonstrated it maintains up-to-date hardware and software asset inventories, as well as associated inventory of software licenses.

Managing risk is a complex, multifaceted activity that requires the involvement of the entire organization. A key component of risk management is the security authorization package (also referred to as an ATO package), which documents the results of the security assessment. The ATO process provides the authorizing official with information needed to make a risk-based decision whether to authorize operation of the information system.[26] Based on NIST guidance,[27] system ATOs are typically granted for a specific period, in accordance with terms and conditions established by the authorizing official. DHS allows its components to enroll in an Ongoing Authorization Program established by NIST.

During our review of the Department's monthly FISMA Scorecard, we determined 2 of 11 DHS components did not meet the required authorization target for HVAs. DHS maintains a target goal of having ATOs for 100 percent of its 144 high-value systems assets. In our review of DHS' May 2023 FISMA Scorecard for unclassified systems, we found two components did not meet the required authorization target of 100 percent for HVAs, as shown in Figure 1.

[25] *Independent Auditors' Report on the DHS's Consolidated Financial Statements for FYs 2023 and 2022 and Internal Control over Financial Reporting,* OIG-24-06, November 14, 2023.
[26] A Federal information system is an information system used or operated by an agency, a contractor of an agency, or another organization on behalf of an agency.
[27] *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST SP 800-37, Revision 2, December 2018.

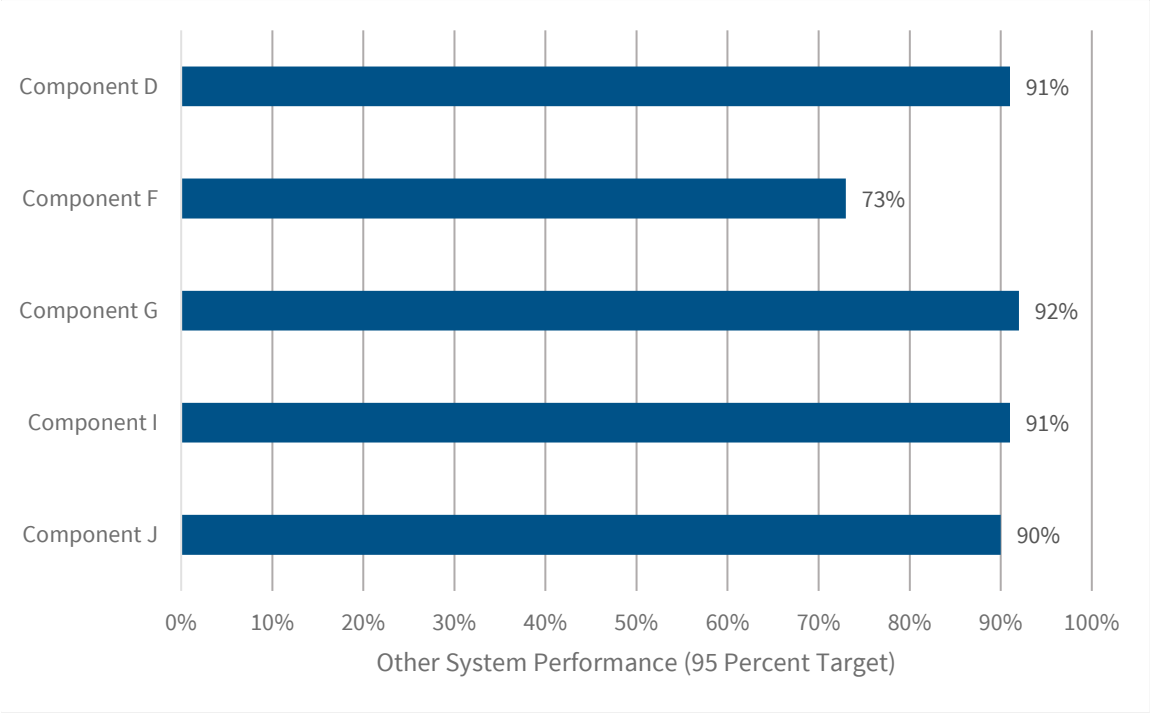
Figure 1. Selected Components Did Not Meet ATO Goal for HVAs



Source: DHS OIG analysis of DHS' May 2023 FISMA Scorecard

In addition, DHS maintains a target goal of having ATOs for 95 percent for the Department's 487 other (i.e., non-HVA) operational systems. According to DHS' May 2023 FISMA Scorecard, 30 other systems from 5 of 11 DHS components did not meet the security authorization target of 95 percent, as shown in Figure 2.

Figure 2. Selected Components Did Not Meet ATO Goal for Other Systems



Source: DHS OIG analysis of DHS' May 2023 FISMA Scorecard

To determine the components' compliance with DHS' NSS security authorization target, we examined the Department's May 2023 NSS FISMA Cybersecurity Scorecard. We found three systems at two components did not meet DHS' NSS ATO target of 100 percent.

As of May 31, 2023, our analysis of DHS' unclassified enterprise management system showed 30 of 632 systems across DHS did not have current ATOs. Five of these systems were HVAs. This represents a 30 percent increase in unclassified systems operating without ATOs when compared to FY 2022. Table 4 outlines the number of unclassified systems operating without ATOs at selected components from FYs 2021 to 2023.

Table 4. Number of Unclassified Systems Operating without ATOs at Selected Components

Component	FY 2021	FY 2022	FY 2023
Component A	6	0	3
Component B	N/A	N/A	N/A
Component C	0	0	0
Component D	12	11	8
Component E	35	1	5
Component F	1	3	3
Component G	1	0	0
Component H	0	2	1
Component I	1	3	6
Component J	N/A	3	4
Component K	0	0	0
Total	**56**	**23**	**30**

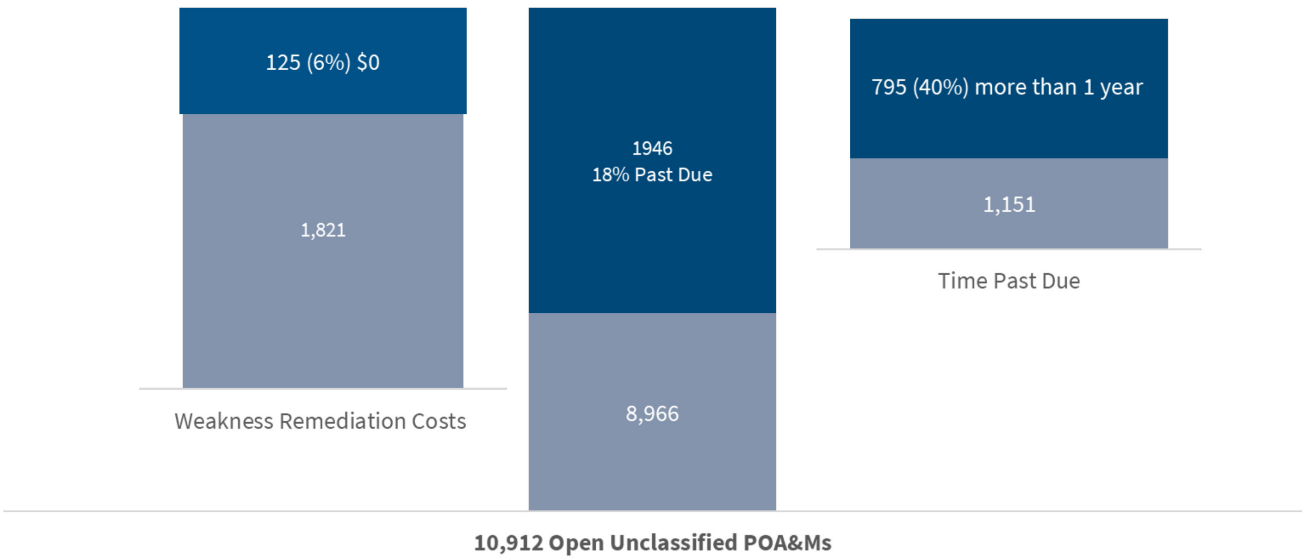
Source: DHS OIG-compiled data from *Evaluation of DHS' Information Security Program for Fiscal Year 2021,* OIG-22-55, August 1, 2022; *Evaluation of DHS' Information Security Program for Fiscal Year 2022,* OIG-23-21, April 17, 2023; and analysis of data from DHS' unclassified enterprise management system as of May 31, 2023.

Weakness Remediation

OMB and DHS require using POA&Ms to track and plan the resolution of information security weaknesses.[28] We found several components did not effectively manage the POA&M process, as required by DHS. For example, components did not resolve all POA&Ms within 12 months or consistently include estimates for resources needed to mitigate identified weaknesses, as required.

Our analysis of 10,912 open unclassified POA&Ms from DHS' enterprise management system showed that 1,946 (18 percent) were overdue as of May 31, 2023. Of those overdue, 795 (41 percent) were overdue by more than a year, including 328 POA&Ms created for HVAs. Of the 1,946 overdue unclassified POA&Ms, 125 (6 percent) had $0 costs to remediate, as shown in Figure 3.

Figure 3. Review of 10,912 Open Unclassified POA&MS



Source: DHS OIG analysis of data from DHS' enterprise management system as of May 31, 2023

Based on our review of four IT reports with identified information security weaknesses, issued between September 2022 and August 2023, two components had not created POA&Ms for the information security weaknesses identified, as required by applicable OMB and DHS guidance.

[28] *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, OMB Memorandum 02-01, October 17, 2001; and *Information Technology System Security Program, Sensitive Systems,* Policy Directive No. 4300A, Version 13.2, September 20, 2022.

We also identified conflicting guidance between *DHS 4300A, Attachment H, POA&M Guide*, v3.0, July 28, 2022, and the *DHS Enterprise Management System User Guide*, January 31, 2023. Specifically, the *POA&M Guide* allows the system owner to define POA&Ms criticality as: (1) Low, (2) Medium, or (3) High. Meanwhile, the *Enterprise Management System User Guide* defines the criticality values as: (1) Very Low, (2) Low, (3) Moderate, (4) High, and (5) Very High. In addition, during our review of DHS' unclassified enterprise management system data, the user criticality field for some POA&Ms was left empty or contained the word "None," which is against applicable DHS guidance for how to identify the criticality of POA&Ms for remediation.

Further, during review of the May 2023 NSS FISMA Cybersecurity Scorecard, we found DHS HQ did not meet DHS' NSS weakness remediation metrics for POA&Ms. This has been a consistent finding in our FISMA reporting since 2020.

Without the system ATOs and all information security weaknesses being incorporated into POA&Ms with required information and cost estimates to monitor the remediation status, DHS cannot be assured effective controls are in place to protect sensitive information stored and processed by these systems. According to FY 2023 reporting metrics, our independent contractor rated CBP, TSA, and Secret Service as operating at "Level 5 – Optimized" in the Risk Management domain of the Identify function.

Supply Chain Risk Management

We determined DHS was operating at "Level 3 – Consistently Implemented" in the Supply Chain Risk Management (SCRM) domain of the Identify function. We assessed the SCRM domain based on SCRM strategies, policies and procedures, plans, and processes to ensure products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and SCRM requirements. This domain aligns with SCRM criteria in NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*. The Department has developed SCRM policies and procedures to ensure products, system components, systems, and services of external providers are consistent with applicable cybersecurity supply chain requirements. DHS did not achieve "Level 4 – Managed and Measurable" because the Department did not provide evidence of quantitative and qualitative performance measures of its SCRM strategy. In addition, as part of one discretionary project, we issued a recommendation for TSA to develop and implement an SCRM plan for a selected HVA system.[29]

According to FY 2023 reporting metrics, our independent contractor rated components as follows in the SCRM domain of the Identify function: "Level 2 – Defined" for TSA, "Level 3 – Consistently Implemented" for CBP, and "Level 4 – Managed and Measurable" for Secret Service.

[29] *Cybersecurity System Review of the Transportation Security Administration's Selected High Value Asset*, OIG-23-44, August 28, 2023.

2. Protect

The "Protect" function entails developing and implementing the appropriate safeguards to ensure delivery of critical services based on four FISMA domains: (1) Configuration Management, (2) Identity and Access Management, (3) Data Protection and Privacy, and (4) Security Training.

We determined DHS was operating at "Level 4 – Managed and Measurable" in the Protect function.

Although the Department has made overall progress in the "Protect" function, DHS components can further safeguard the Department's information systems and sensitive data by:

- implementing all configuration settings;
- improving identity and access weaknesses at selected components; and
- implementing security patches in a timely manner.

Configuration Management

We determined DHS was operating at "Level 4 – Managed and Measurable" in the Configuration Management domain of the Protect function. We performed technical testing as part of three discretionary projects on four HVA systems. The results from our security assessment revealed critical and high-risk vulnerabilities, as well as misconfigured security settings on selected servers and workstations, that may expose DHS data. For example, we identified 13 unique critical vulnerabilities, occurring 432 times, that are listed in the Cybersecurity and Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities catalog.

We conducted configuration management assessments on four HVA systems at three components.

- Component C implemented 99 percent of the required Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) baseline settings.
- Component G implemented between 40 and 84 percent of the required DISA STIG baseline settings.
- Component I implemented between 72 and 96 percent of the required DISA STIG baseline settings.

We also determined components could improve their flaw-remediation processes to ensure patches and antivirus/malware software updates are identified, prioritized, tested, and installed in a timely manner. For example:

- At Component C, we assessed one HVA system and identified 2 unique critical and 2 high-risk vulnerabilities on 54 databases and servers tested.

- At Component G, we assessed 2 HVA systems for patch/vulnerability assessments and identified 8 unique critical and 31 unique high-risk vulnerabilities on 508 workstations, domain controllers, and servers tested.
- At Component I, we assessed one HVA system and identified 96 unique critical and 178 high-risk vulnerabilities on 1,092 workstations, databases, and servers tested.

When security patches are not applied in a timely fashion, components could be vulnerable to potential exploitation.

Our independent contractor rated components as follows in the Configuration Management domain of the Protect function: "Level 4 – Managed and Measurable" for Secret Service, and "Level 5 – Optimized" for CBP and TSA.

Identity and Access Management

We determined DHS was operating at "Level 4 – Managed and Measurable" in the Identity and Access Management domain of the Protect function. Identity and access management focuses on access to physical and logical assets and associated facilities; is limited to authorized users, processes, and devices; and is managed consistent with the assessed risk. DHS has taken a decentralized approach to identity and access management by allowing its components to take responsibility for issuing Personal Identity Verification (PIV) cards for computer and building access, pursuant to Homeland Security Presidential Directive-12.[30] DHS requires all privileged and unprivileged employees and contractors to use PIV cards for system access.

During our security assessment conducted at Component G as one of our discretionary projects, we determined the use of PIV cards as a multi-factor authentication for privileged accounts was not enforced. In addition, Component G allowed 116 users (of 47,810 total) the ability to reset the password for a powerful privileged account. After we advised Component G of the issue, component officials stated the account permissions were set incorrectly due to human error. Component G officials stated the team would review and correct misconfigured account permissions.

During the August 2023 evaluation we conducted at Component I, we determined the component did not:

- have policies and procedures for administering system user accounts;
- maintain current user lists for the selected HVA system;

[30] *Policy for a Common Identification Standard for Federal Employees and Contractors*, Homeland Security Presidential Directive-12, August 27, 2004, requires Federal agencies to use a standard form of identification to gain physical and logical access to federally controlled facilities and information systems.

- ensure access for non-privileged users was always authorized, updated, or removed, as required;
- always ensure access for privileged users was authorized, updated, or removed, as required; and
- effectively track and manage separated individuals' HVA system access.

Our independent contractor rated CBP, TSA, and Secret Service as "Level 5 – Optimized" in the Identity and Access Management domain of the Protect function.

Data Protection and Privacy

We determined DHS was operating at "Level 3 – Consistently Implemented" in the Data Protection and Privacy domain of the Protect function. DHS did not provide supporting evidence for its qualitative and quantitative performance measures. The Department also did not provide evidence to support that it audited Domain Name Service records.

Our independent contractor rated components as follows in the Data Protection and Privacy domain of the Protect function: "Level 4 – Managed and Measurable" for CBP and Secret Service, and "Level 5 – Optimized" for TSA.

Security Training

We determined DHS was operating at "Level 4 – Managed and Measurable" in the Security Training domain of the Protect function. Educating employees about rules of behavior and roles and responsibilities is critical for an effective information security program. Components are required to ensure all employees and contractors receive IT security awareness training and that employees with significant responsibilities receive specialized training.[31] However, TSA did not ensure all its users receive the required annual security awareness training to mitigate risk.[32]

DHS is also required to promote effective cybersecurity talent development and management for its cybersecurity workforce.[33] DHS has established and implemented a security awareness and training program to ensure all employees and contractors understand their roles and responsibilities. Yet DHS has only implemented this program at DHS HQ and plans to release it to DHS components in phases. Additionally, DHS has established minimum role-based knowledge requirements and role-based training standards.

[31] *Security and Privacy Controls for Information Systems and Organizations,* NIST SP 800-53, Rev. 5, September 2020.
[32] *Cybersecurity System Review of the Transportation Security Administration's Selected High Value Asset*, OIG-23-44, August 28, 2023.
[33] *Federal Cybersecurity Workforce Strategy*, OMB M-16-15, July 12, 2016.

DHS is applying its workforce strategy to prioritize hiring and to procure the required knowledge, skills, and abilities to close critical gaps in the workforce. The Department is also using a talent management system to analyze the current skill sets of its cyber workforce to identify knowledge, skills, and abilities gaps. DHS has only implemented this talent management program at two components and plans to release it to two others in the future.

According to FY 2023 reporting metrics, our independent contractor rated components as follows in the Security Training domain of the Protect function: "Level 4 – Managed and Measurable" for Secret Service and "Level 5 – Optimized" for CBP and TSA.

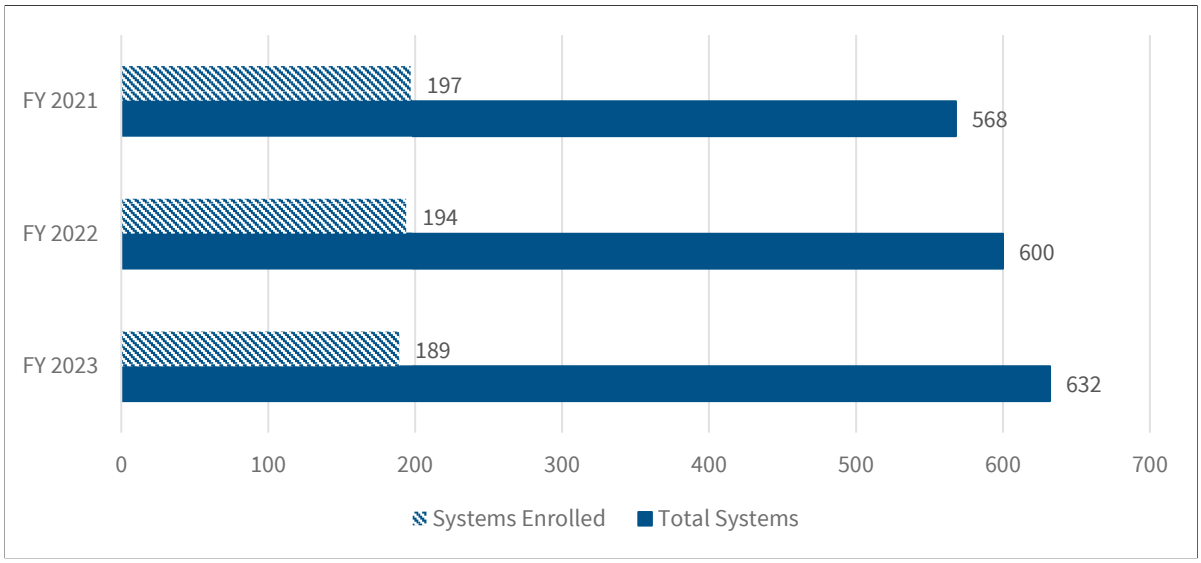
3. Detect

The "Detect" function entails developing and implementing appropriate activities, including ongoing systems authorization and continuous monitoring, to identify any irregular system activity.

Information Security Continuous Monitoring

We determined DHS was operating at "Level 4 – Managed and Measurable" in the Information Security Continuous Monitoring domain of the Detect function. DHS has not fully allocated resources to implement Information Security Continuous Monitoring requirements and activities for Sensitive but Unclassified systems effectively. For NSS, the Department has not developed system-level continuous monitoring strategies/policies that define its processes for performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans, monitoring security controls for individual systems, and time-based triggers for ongoing authorization. Additionally, as part of the discretionary project we conducted at Component I, we determined the component did not perform effective continuous monitoring on the HVA system we reviewed. As of May 2023, only 189 of 632 (30 percent) Sensitive but Unclassified systems from nine components are participating in the Ongoing Authorization Program. The number of systems enrolled in the program decreased by five systems from FYs 2022 to 2023, as shown in Figure 4.

Figure 4. DHS Systems Enrolled in the Ongoing Authorization Program from FYs 2021 to 2023



Source: DHS OIG-compiled based on DHS Office of the CISO data

According to FY 2023 reporting metrics, our independent contractor rated components as follows in the Information Security Continuous Monitoring domain of the Detect Function: "Level 4 – Managed and Measurable" for TSA and Secret Service, and "Level 5 – Optimized" for CBP.

4. Respond

The "Respond" function entails developing and implementing appropriate responses to detected cybersecurity events.

Incident Response

We determined DHS was operating at "Level 4 – Managed and Measurable" in the Incident Response domain of the Respond function. Our August 2023 evaluation on a cybersecurity system review[34] revealed TSA can better protect its sensitive data from potential cyberattacks by strengthening the management of technical controls, in accordance with OMB policy.

[34] *Cybersecurity System Review of the Transportation Security Administration's Selected High Value Asset*, OIG-23-44, August 28, 2023. As of March 2024, all recommendations cited in the report remain open and resolved.

Our independent contractor rated components as follows in the Incident Response domain of the Respond function: "Level 4 – Managed and Measurable" for TSA and Secret Service, and "Level 5 – Optimized" for CBP.

5. Recover

The "Recover" function entails developing and implementing plans for resiliency and restoration of any capabilities or services impaired due to outages or other disruptions from a cybersecurity event.

Contingency Planning

We determined DHS was operating at "Level 4 – Managed and Measurable" in the Contingency Planning domain of the Recover function. DHS defined its policies, procedures, and strategies for information contingency planning, but did not fully test these plans. For example, as of May 2023, six components had not tested contingency plans for 16 unclassified systems.

DHS has developed a department-wide business continuity program to restore essential business functions and resume normal operations in response to emergency events. As part of this program, DHS leads exercises that involve all DHS components' participation to collect information about their key business requirements and capabilities needed to recover from an attack or disaster. DHS used this information to develop a Reconstitution Plan outlining macro-level procedures for all DHS senior leadership, staff, and components to follow and to resume normal operations as quickly as possible in the event of an emergency. The procedures may involve both manual and automated processing at alternate locations, as appropriate.

Components are responsible for developing and periodically testing the backup and disaster recovery procedures outlined in the information system contingency plans.[35] As of May 2023, we identified the following deficiencies:

- Our review of the May 2023 NSS FISMA Cybersecurity Scorecard showed DHS HQ did not meet DHS' NSS compliance target for contingency plan testing.
- More specifically, United States Citizenship and Immigration Services, the Management Directorate, the Federal Emergency Management Agency, the Federal Law Enforcement Training Centers, Immigration and Customs Enforcement (ICE), and CISA had not tested contingency plans for 16 of 632 unclassified systems, based on the data we analyzed from DHS' enterprise management system.

[35] *Information Technology System Security Program, Sensitive Systems,* DHS Policy Directive Number 4300A, Version 13.3, February 13, 2023.

A well-documented and tested contingency plan can ensure the recovery of critical network operations. Untested plans may create a false sense of security and an inability to recover operations in a timely manner.

As part of the discretionary project that we conducted at Component I, we found no evidence that the contingency plan for the system was reviewed, approved, or tested, as required, as both the contingency plan and contingency plan testing results were not signed.

According to FY 2023 FISMA Reporting Metrics, our independent contractor rated components as follows in the Contingency Planning domain of the Recover function: "Level 4 – Managed and Measurable" for TSA and Secret Service, and "Level 5 – Optimized" for CBP.

Summary of Selected Components' Implementation of Information Security Programs

Our independent contractor rated component information security programs "effective" for CBP, TSA, and Secret Service, as each achieved "Level 4 – Managed and Measurable" or higher in four of the five functions. Table 5 summarizes CBP, TSA, and Secret Service's implementation of their information security programs.

Table 5. Summary Status of CBP, TSA, and Secret Service Information Security Programs for FY 2023

Function	CBP	TSA	Secret Service
Identify	Level 4 – Managed and Measurable	Level 4 – Managed and Measurable	Level 4 – Managed and Measurable
Protect	Level 5 – Optimized	Level 5 – Optimized	Level 4 – Managed and Measurable
Detect	Level 5 – Optimized	Level 4 – Managed and Measurable	Level 4 – Managed and Measurable
Respond	Level 5 – Optimized	Level 4 – Managed and Measurable	Level 4 – Managed and Measurable
Recover	Level 5 – Optimized	Level 4 – Managed and Measurable	Level 4 – Managed and Measurable
Overall Rating	**Effective**	**Effective**	**Effective**

Source: DHS OIG contractor-compiled summary status information

Since 2020, our independent contractor has performed fieldwork at nine selected components and rated four components' information security programs as ineffective, in accordance with the FISMA Reporting Metrics, because the components achieved below "Level 4 – Managed and Measurable" in three of five functions.

Recommendations

Recommendation 1: We recommend the DHS Chief Information Officer strengthen its oversight to ensure components adhere to DHS' policies to remediate all known information security weaknesses in a timely manner and obtain the Authority to Operate for their systems.

Recommendation 2: We recommend the DHS Chief Information Officer resolve any conflicting guidance on prioritizing information security weaknesses by reviewing all Department policies and procedures to determine whether revision is needed and to ensure DHS' policies and procedures are clearly defined and consistent with applicable OMB requirements.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Director of the Departmental Government Accountability Office-OIG Liaison Office (Director), who expressed the Department's appreciation for OIG's work planning and conducting its review and issuing this report. We reviewed the Department's comments, as well as the technical comments previously submitted under separate cover, and updated the report as appropriate. The Department concurred with the recommendations. We have included a copy of the comments in their entirety in Appendix B. A summary of DHS' responses and our analysis follows.

DHS Comments to Recommendation #1: Concur. The Department has taken corrective actions to strengthen its oversight. For example, the Department increased the percentage of "systems operating with an ATO" and "updated contingency plans" metrics to 98 percent for HVA systems, and 95 percent for non-HVA systems, as of September 2023. DHS plans to achieve 100 percent compliance for "systems operating with an ATO" and "updated contingency plans" metrics by September 30, 2024, for HVAs and Sensitive but Unclassified systems; and September 30, 2025, for NSS.

DHS plans to prioritize the patching of all vulnerabilities, especially those included in the "CISA Known Exploited Vulnerabilities Catalog." Accordingly, DHS OCIO has prioritized improving components' centralized patching capabilities, with the goal of reaching 100 percent of component endpoints. In addition, DHS OCIO will continue to monitor components' compliance on applying security patches via the Continuous Diagnostic Monitoring program to ensure continued improvement. Since FY 2023, DHS OCIO, through the CISO Council, worked to develop

an updated attachment to *DHS Policy Directive 4300A*, which is anticipated to be completed by April 30, 2025. Estimated Completion Date for all corrective actions: September 30, 2025.

OIG Analysis of DHS Comments:

DHS' actions are responsive to the recommendation, which will remain open and resolved until DHS provides documentation showing all planned corrective actions are completed.

DHS Comments to Recommendation #2: Concur. DHS OCIO will review DHS policy and components' policies, as appropriate, to ensure POA&M prioritization is clearly defined and consistent. Specifically, DHS will leverage the Unified Cybersecurity Maturity Model to prioritize critical and overdue POA&Ms. DHS OCIO will ensure policy updates provide clarity and include the Unified Cybersecurity Maturity Model as an additional tool for managing risk, as well as prioritizing funding and resources for weakness remediation. Estimated Completion Date: September 30, 2024.

OIG Analysis of DHS Comments:

DHS' actions are responsive to the recommendation, which will remain open and resolved until DHS provides documentation showing 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* (Pub. L. No. 107−296) by amendment to the *Inspector General Act of 1978*.

The objective of our evaluation was to determine whether DHS' information security program and practices were adequate and effective to protect the information and information systems that support DHS' operations and assets for FY 2023. Our independent evaluation focused on assessing DHS' information security program using requirements outlined in the FY 2023 FISMA Reporting Metrics. Specifically, we evaluated DHS' information security program's compliance with requirements outlined in five NIST cybersecurity functions.

We performed our fieldwork at the DHS HQ Office of the CISO, and our independent contractors performed fieldwork at CBP, TSA, and Secret Service. To conduct our evaluation, we interviewed relevant DHS HQ and component personnel; assessed DHS' current operational environment; and determined compliance with FISMA requirements and other applicable information security policies, procedures, and standards. Specifically, we:

- reviewed the results from our FY 2020, FY 2021, and FY 2022 FISMA evaluations and used them as baselines for the FY 2023 evaluation;
- evaluated policies, procedures, and practices DHS implemented at the program and component levels;
- reviewed DHS' POA&Ms and ongoing authorization procedures to determine whether security weaknesses were identified, tracked, and addressed;
- evaluated processes and the status of the department-wide information security program reported in DHS' monthly information security scorecards regarding risk management, contractor systems, configuration management, identity and access management, security training, information security continuous monitoring, incident response, and contingency planning; and
- developed an independent assessment of DHS' information security program.

We incorporated technical testing results from other discretionary projects conducted during the same FY. We reviewed information from DHS' enterprise management systems to determine data reliability and accuracy. We found no discrepancies or errors in the data. DHS OIG contractors performed fieldwork at CBP, TSA, and Secret Service to support our evaluation.

We conducted this review between March 2023 and November 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. We did not evaluate DHS OIG's compliance with FISMA requirements during our review.

DHS OIG's Access to DHS Information

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

Appendix B:
DHS Comments on the Draft Report

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

May 6, 2024

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

JIM H CRUMPACKER
Digitally signed by JIM H CRUMPACKER
Date: 2024.05.06 15:35:16 -04'00'

SUBJECT: Management Response to Draft Report: "Evaluation of DHS' Information Security Program for Fiscal Year 2023" (Project No. 23-024-AUD-DHS)

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS, or the Department) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

DHS leadership is pleased to note OIG's positive recognition that the Department's effectiveness of the domain, function, and overall information security program resulted in a maturity rating of "Level 4 –Managed and Measurable" in the Identify, Protect, Detect, Respond, and Recover functions. DHS remains committed to sustaining a strong information security program that effectively protects data and information systems, while supporting DHS's mission of protecting the American people from threats to their security.

The draft report contained two recommendations with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments 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 this office if you have any questions. We look forward to working with you again in the future.

Enclosure

1

Enclosure: Management Response to Recommendations Contained in OIG (23-024-AUD-DHS)

OIG recommended that the DHS Chief Information Officer (CIO):

Recommendation 1: Strengthen its oversight to ensure components adhere to DHS's policies to remediate all known information security weaknesses in a timely manner and obtain the Authority to Operate [ATO] for their systems.

Response: Concur. The DHS Chief Information Security Officer (CISO) within the Management Directorate (MGMT) will continue to lead the Department's cybersecurity program through the DHS CISO Council, engaging with all Component CISOs and stakeholders. As a result of this engagement and oversight, the percentage of DHS systems operating with a current ATO and updated contingency plans reached 98 percent for High Value Asset (HVA) systems, and 95 percent for non-HVA systems on the Fiscal Year (FY) 2023 September Federal Information Security Modernization Act of 2014 (FISMA) Scorecard, which is expected to only improve.

The Department also continues to enlarge its Ongoing Authorization (OA) program,[1] which eliminates the need to renew ATOs every three years, as the OA program ensures systems are monitored continuously. By April 30, 2024, 20 systems were enrolled in the OA program after its policy release in February 2023, and the Department continues to enroll new eligible systems upon request from Components. Currently, there are 198 systems across DHS that are enrolled in the OA program.

In addition, beginning in August 2023, to better focus authorization efforts, the DHS Office of the Chief Information Officer (OCIO) National Security Systems (NSS) Governance team revised the "NSS Cybersecurity Scorecard," produced each month. This revision adds a means to differentiate between systems that lack an ATO because they are still in development, and those systems that are operating without an ATO. Beginning in November 2023, the NSS Governance team also reestablished the Information Safeguarding and Risk Management Council (ISRMC) which oversees risk executive functions for all DHS NSS. To date, the ISRMC focused attention on expired NSS ATOs, conducted new NSS designations, and recommended ATOs for three systems that were previously operating with expired ATOs. The ISRMC will provide the means to focus institutional attention on NSS improvements, and to manage NSS

[1] Documented in Attachment BB of the DHS Policy Directive 4300A, "Information Technology System Security Program, Sensitive Systems," version 13.3, dated February 13, 2023; https://www.dhs.gov/sites/default/files/2023-05/V2.508%20Working%20file_DHS_4300A%20ITSSP%20SS%20Policy%20Directive%20FINAL%202023.02.13_kwb.pdf

designations, authorizations, and policy updates proactively going forward.

For HVAs and Sensitive but Unclassified systems, the Department will strive for 100 percent compliance of ATO's and Contingency Plan testing by September 30, 2024, while all NSS will be compliant with ATO and Contingency Test Plan requirements by September 30, 2025. In addition, DHS will continue to leverage the Unified Cybersecurity Maturity Model (UCMM) to prioritize mitigation of Plans of Action and Milestones (POA&M) for known security weaknesses, as well as prioritizing overall cybersecurity posture improvements in the most efficient manner. UCMM is a framework of the cybersecurity standards based on the National Institute of Standard and Technology (NIST) Cyber Security Framework,[2] and includes an integrated quantitative measurement system, which provides DHS Component CIOs and CISOs and system stakeholders tailored risk views to support prioritization, planning, and budgeting.

Utilizing UCMM, POA&Ms are analyzed to determine which ones are causing the greatest impact by generating an Enterprise, Component, and a per system prioritization of a POA&Ms impact on overall system security. An informational UCMM performance metric was added to the "FY24 Information Security Performance Plan (ISPP) for HVAs," August 14, 2023with a target metric of "maturity level 4," as an initial programmatic step for including UCMM in performance metrics and reporting by September 2024.

With regard to security configuration settings, it important to note that the DHS ISPP requires that DHS Components comply with the Defense Information System Agency's Security Technical Implementation Guides, which the DHS MGMT CISO enforces through tracking and reporting on the monthly Department scorecard. As a result, the Department Configuration Management score was at 92 percent for HVA, and 90 percent for non-HVA systems on the "FY24 Information Security Monthly FISMA Scorecard." This security configuration compliance metric is expected to continue to improve Department-wide, and DHS will continue to strive for 100 percent compliance despite constantly changing conditions and security vulnerabilities.

DHS also continues to prioritize the patching of all vulnerabilities, especially those included in the "Cybersecurity Infrastructure Security Agency Known Exploited Vulnerabilities Catalog."[3] Accordingly, the DHS OCIO prioritized improving Component centralized patching capabilities, with the goal of reaching 100 percent of Components' endpoints through the Department's Cybersecurity Service Provider program. DHS OCIO will continue to monitor patch compliance via the Continuous Diagnostic Monitoring program to ensure continued improvement.

[2] "The NIST Cybersecurity Framework (CSF) 2.0" dated February 26, 2024; https://doi.org/10.6028/NIST.CSWP.29
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Further, with regard to Component Multifactor Authentication (MFA) enforcement standards, OCIO continues to lead the adoption of MFA for 100 percent of the Department FISMA systems. This standard, established by Executive Order (EO) 14028,[4] requires all systems to institute MFA mechanisms. Since issuance of EO 14028, DHS OCIO worked with all Components to implement the necessary infrastructure and processes to support system-wide MFA compliance. As of March 29, 2024, the Department stood at 96 percent compliance, which is a leading example of EO 14028 compliance among Chief Financial Officer Act agencies.

On October 1, 2022, OCIO initiated an overhaul of the entire Department's standards for privileged account issuance and management by establishing a "Headquarters and Management Directorate Identity, Credential, and Access Management (ICAM)" policy.[5] Further, since FY 2023, DHS OCIO, through the CISO Council and ICAM Executive Steering Committee, worked to develop an updated attachment to DHS Policy Directive 4300A, which is anticipated to be complete by April 30, 2025. Once updated, the policy will clearly reflect the minimum standards for the review, approval, and issuance of privileged accounts on any DHS FISMA system. This effort will also standardize the process (independent of the underlying tool or tracking software) for the provisioning and deprovisioning of privileged accounts.

Estimated Completion Date (ECD): September 30, 2025.

Recommendation 2: Resolve any conflicting guidance on prioritizing information security weaknesses by reviewing all Department policies and procedures to determine whether revision is needed and to ensure DHS' policies and procedures are clearly defined and consistent with applicable Office of Management and Budget requirements.

Response: Concur. The DHS OCIO CISO Cybersecurity Policy Branch will review DHS Policy Directive 4300A and Component policies, as appropriate, to ensure POA&M prioritization is clearly defined and consistent. Specifically, DHS will continue to leverage the UCMM to prioritize critical and overdue POA&Ms to achieve the greatest improvement in the cybersecurity posture for all systems in the most efficient manner. This capability is part of the larger UCMM framework, and will continue to reduce the Department's population of POA&Ms, especially those that are overdue. DHS OCIO will ensure policy updates provide clarity and include UCMM as an additional tool for managing risk, prioritizing funding, and resources for weakness remediation.

ECD: September 30, 2024.

[4] "Executive Order on Improving the Nation's Cybersecurity" dated May 12, 2021; https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[5] Version 1 dated September 18, 2023.

Appendix C:
Major Contributors to This Report

Chiu-Tong Tsang, Director
Shawn Hatch, Audit Manager
Lawrence Polk, Cybersecurity Specialist
Omar Russell, Auditor-in-Charge
Sonya Griffin, Auditor
Bridgette OgunMokun, Auditor
Lauren Barrick, Auditor
Aishia LaCount, Auditor
Thomas Rohrback, Director, Cybersecurity Risk Assessment Division
Rashedul Romel, Supervisory IT Specialist
Jason Dominguez, IT Specialist
Taurean McKenzie, IT Specialist
Kevin Dolloson, Communications Analyst
Alicia Lewis, 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
Chief Information Officer
Chief Information Security Officer
Audit Liaison, Office of the Chief Information Officer
Audit Liaison, Office of the Chief Information Security Officer
Audit Liaisons, CBP, Federal Emergency
Management Agency, ICE, Office of Intelligence and Analysis,
United States Citizenship and Immigration Services, CISA, Science and Technology Directorate,
TSA, United States Coast Guard, and Secret Service

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information

To view this and any other DHS OIG reports, Please visit our website: www.oig.dhs.gov

For further information or questions, please contact the DHS OIG Office of Public Affairs via email: DHS-OIG.OfficePublicAffairs@oig.dhs.gov

DHS OIG Hotline

To report fraud, waste, abuse, or criminal misconduct involving U.S. Department of Homeland Security programs, personnel, and funds, please visit: www.oig.dhs.gov/hotline

If you cannot access our website, please contact the hotline by phone or mail:

Call: 1-800-323-8603

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