OFFICE OF INSPECTOR GENERAL

Evaluation of DHS' Information Security Program for Fiscal Year 2021

Homeland Security

August 1, 2022

OIG-22-55

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

August 1, 2022

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: 2022.08.01 12:35:14 -04'00'

SUBJECT: *Evaluation of DHS' Information Security Program for Fiscal Year 2021*

Attached is our final report, *Evaluation of DHS' Information Security Program for Fiscal Year 2021.* We incorporated the formal comments provided by the Department.

The report contains three recommendations aimed at improving the Department's information security program. The Department concurred with all three recommendations. Based on information provided in the Department's response to the draft report, we consider recommendations 1 and 3 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. Recommendation 2 is closed and resolved.

Consistent with our responsibility under the *Inspector General Act of 1978, as amended* 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 final report on our website for public dissemination.

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

Attachment

DHS OIG HIGHLIGHTS

Evaluation of DHS' Information Security Program for Fiscal Year Fiscal Year 2021

August 1, 2022

Why We Did This Evaluation

We reviewed the Department of Homeland Security's information security program for compliance with *Federal Information Security Modernization Act of 2014* (FISMA) requirements. We conducted our evaluation according to fiscal year 2021 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 support DHS' operations and assets for FY 2021.

What We Recommend

We made three 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

DHS' information security program for FY 2021 was rated "not effective," according to this year's reporting instructions. To receive an "effective" rating, agencies must achieve a "Level 4 – Managed and Measurable" in three of the five functions outlined in the National Institute of Standards and Technology Cybersecurity Framework. DHS received "Level 4 – Managed and Measurable" in the Protect function, "Level 3 – Consistently Implemented" in the Identify, Detect, and Respond functions, and "Level 2 – Defined" in the Recover function.

Our rating of "not effective" was based on our evaluation of DHS' compliance with the FISMA requirements on unclassified and National Security Systems. We identified the following six deficiencies:

(1) systems in use without an authority to operate;
(2) known information security weaknesses not mitigated timely;
(3) security patches not applied timely to mitigate critical and high-risk security vulnerabilities on selected workstations and network equipment;
(4) one component running an unsupported operating system on its network equipment;
(5) inaccurate reporting of metrics in monthly scorecards and FISMA quarterly submissions; and
(6) outdated information technology security guidance that contradicts other DHS policies.

We recognize DHS was primarily focused on responding to a significant cyber incident during FY 2021. An official stated DHS faced significant challenges in FY 2021, as it diverted resources to respond to the SolarWinds incident.

DHS Response

DHS concurred with all three recommendations. We included a copy of DHS' comments in Appendix B.

Table of Contents

Appendixes

Abbreviations

ATO	Authority to Operate
BYOD	Bring Your Own Device
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
Coast Guard	United States Coast Guard
DoD	Department of Defense
FEMA	Federal Emergency Management Agency
FISMA	*Federal Information Security Modernization Act of 2014*
FLETC	Federal Law Enforcement Training Centers

HQ	Headquarters
ISCM	Information Security Continuous Monitoring
IT	information technology
NIST	National Institute of Standards and Technology
NSS	National Security System
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SCRM	Supply Chain Risk Management
VPN	Virtual Private Network

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 over the information resources that support Federal operations and assets.[3]

FISMA focuses on program management, implementation, and evaluation of the security of unclassified 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. Each agency's Chief Information Officer (CIO), in coordination with senior agency officials, is required to 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 240,000 personnel, all of whom rely on information technology (IT) to perform their duties. It is critical that DHS provide a high level of cybersecurity for the information and information systems supporting day-to-day operations.[8]

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

[1] 44 United States Code § 3551 *et.seq.*
[2] *Id.* at § 3552(a)(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 § 3544(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.

systems classified as "Secret" and "Top Secret," and systems operated by contractors on behalf of DHS. The DHS CISO maintains ongoing awareness of the Department's information security program, vulnerabilities, and potential threats through the execution of three programs: (1) Information Security Continuous Monitoring (ISCM) Data Feeds, (2) Ongoing Authorization Program, and (3) Security Operations Center. Collectively, these programs provide a framework to govern the information systems owned and operated across DHS.

Foremost to all DHS components is adhering to requirements set forth in the Department's security authorization process,[9] which involves comprehensive testing and evaluation of security features of all information systems before becoming operational[10] 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,[11] each component CISO is required to assess the effectiveness of controls implemented before authorizing the systems to operate, and periodically thereafter. According to applicable DHS,[12] Office of Management and Budget (OMB),[13] and NIST[14] 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 for remediating information security weaknesses related to unclassified and Secret-level systems.

FISMA Reporting Instructions

FISMA requires each agency Inspector General to perform an annual independent evaluation to determine the effectiveness of the agency's information security program and practices. The *FY 2021 Inspector General FISMA Reporting Metrics*[15] (FY 2021 FISMA Reporting Metrics) provide reporting

[9] The National Institute of Standards and Technology (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.
[10] According to DHS policy, an information system must be granted an Authority to Operate.
[11] DHS *System Security Authorization Process Guide*, Version 14.1, April 4, 2019.
[12] DHS *System Security Authorization Process Guide*, Version 14.1, April 4, 2019.
[13] OMB *Circular A-130, Managing Information as a Strategic Resource,* July 2016.
[14] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, September 2020.
[15] *FY 2021 Inspector General FISMA Reporting Metrics*, Version 1.1, May 12, 2021, were developed as a collaborative effort among OMB, DHS, and the Council of the Inspectors

requirements for addressing key areas identified during independent evaluations of agency information security programs. Inspectors General are required to 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. 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.[16] The FY 2021 FISMA Reporting Metrics included a new Supply Chain Risk Management (SCRM) domain (see Table 1).

Table 1. NIST Cybersecurity Functions and FY 2021 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 2021 FISMA Reporting Metrics

According to the FY 2021 FISMA Reporting Metrics, each Office of Inspector General evaluates its agency's information security program using a set of questions cited in the reporting instructions for the five cybersecurity functions listed in Table 1. The questions are derived from the maturity models outlined

General on Integrity and Efficiency, in consultation with the Federal CIO Council and other stakeholders.

[16] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018.

within the NIST Cybersecurity Framework. Based on its evaluation, OIG assigns each of its agency's cybersecurity functions a maturity level of 1 through 5 (see Table 2).

Table 2. OIG 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 a changing threat and technology landscape and business/mission needs.

Source: FY 2021 FISMA Reporting Metrics

Per the FY 2021 FISMA Reporting Metrics, when an information security program is rated at "Level 4, Managed and Measurable," the program is operating at an effective level of security.[17] OIGs are encouraged to use the domain ratings to inform overall function ratings and to use the five function ratings to inform the overall agency rating, based on a simple majority.

Scope of Our FISMA Evaluation

This report summarizes the results of our evaluation of the Department's information security program based on the FY 2021 FISMA Reporting Metrics. We performed our fieldwork at DHS Headquarters, DHS Office of the CISO, and at selected DHS components. To determine whether DHS components effectively manage and secure their information systems, we reviewed the Department's monthly FISMA Scorecards for unclassified systems and NSS. We also performed technical testing on two selected IT systems at one component (referred to as "Component I") and one system at another component (referred to as "Component K"). Specifically, we tested selected Windows 10 workstations and the effectiveness of controls implemented on selected databases and servers within each component. We responded to the

[17] *FY 2021 Inspector General FISMA Reporting Metrics,* Version 1.1, May 12, 2021.

questions cited in the FY 2021 FISMA Reporting Metrics based on our evaluation of DHS' compliance with applicable FISMA requirements.

To determine the effectiveness of components' implementation of their information security programs, our independent contractor performed work at the United States Coast Guard (Coast Guard), Federal Emergency Management Agency (FEMA), and Federal Law Enforcement and Training Centers (FLETC). The contractor evaluated each component based on the maturity model approach outlined in the FY 2021 FISMA Reporting Metrics and NIST's Cybersecurity Framework. We have incorporated the contractor's work in this report.

On June 2, 2021, the House of Representatives Committee on Oversight and Reform[18] asked that several questions be addressed as part of the FISMA FY 2021 effort. Specifically, we were asked to include an assessment of any vulnerabilities created or exacerbated by the Department's use of remote-access software to facilitate telework during the coronavirus pandemic and whether any such vulnerabilities were effectively mitigated. The contractor provided in its report responses from Coast Guard, FEMA, and FLETC to the Committee questions (see Appendix D).

Results of Evaluation

The Department's information security program for FY 2021 was rated as "not effective," according to the FY 2021 reporting instructions. To receive a rating of "effective," agencies must achieve a "Level 4 – Managed and Measurable" in a simple majority in three of the five functions outlined in the NIST Cybersecurity Framework. DHS received "Level 4 – Managed and Measurable" in the Protect function, "Level 3 – Consistently Implemented" in the Identify, Detect, and Respond functions, and "Level 2 – Defined" in the Recover function.

Our rating of "not effective" was based on our evaluation of DHS' compliance with the FISMA requirements on unclassified and NSS. We identified the following six deficiencies:

(1) systems in use without an authority to operate;
(2) known information security weaknesses not mitigated timely;
(3) security patches not applied timely to mitigate critical and high-risk security vulnerabilities on selected workstations and network equipment;

[18] House of Representatives Committee on Oversight and Reform memorandum from Chairwoman Carolyn B. Maloney to the Honorable Joseph Cuffari, Inspector General, dated June 2, 2021.

(4) one component running an unsupported operating system on its network equipment;
(5) inaccurate reporting of metrics in monthly scorecards and FISMA quarterly submissions; and
(6) outdated IT security guidance that contradicts other DHS policies.

We recognize DHS was primarily focused on responding to a significant cyber incident during this fiscal year. For example, during FY 2021, one DHS official stated the Department faced significant challenges, as its resources were diverted for critical SolarWinds response and recovery efforts. In response to the SolarWinds incident, DHS' Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 21-01, *Mitigate SolarWinds Orion Code Compromise*, which outlined required mitigations for Federal agencies to prevent further exploitation of Federal information systems resulting from the SolarWinds compromise. In addition, the official stated that the Department had developed and approved a set of tailored network architecture and cybersecurity improvements to strengthen the DHS network against future attacks.

DHS Can Further Improve the Management of Its Information Security Program

DHS' information security program earned an overall rating of ineffective, with a maturity rating of "Level 3 – Consistently Implemented" in three of five functions. Our FY 2021 rating did not include Coast Guard when evaluating the overall effectiveness of DHS' information security program for FISMA.[19] A comparison of FY 2020 and FY 2021 ratings is summarized in Table 3.

[19] In May 2020, the Department allowed Coast Guard to meet FISMA requirements according to Department of Defense (DoD) reporting requirements rather than DHS reporting requirements. As part of our review, our independent contractor performed work at selected components and assessed their ratings, including Coast Guard according to FY 2021 FISMA Reporting Metrics. However, we did not use these Coasts Guard ratings when evaluating the overall effectiveness of DHS' information security program for FISMA.

Table 3. DHS' Maturity Level for Each Cybersecurity Function in FY 2020 Compared with FY 2021

Cybersecurity Function	Maturity Level	
	FY 2020	FY 2021
1. Identify	Level 4 – Managed and Measurable	Level 3 – Consistently Implemented
2. Protect	Level 4 – Managed and Measurable	Level 4 – Managed and Measurable
3. Detect	Level 4 – Managed and Measurable	Level 3 – Consistently Implemented
4. Respond	Level 3 – Consistently Implemented	Level 3 – Consistently Implemented
5. Recover	Level 1 – Ad Hoc	Level 2 – Defined

Source: DHS OIG analysis based on our FY 2020 report[20] and FY 2021 FISMA Reporting Metrics

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.*

We determined that DHS was operating at "Level 3 – Consistently Implemented" in this function. This was based on inaccuracies in DHS' quarterly FISMA submissions to OMB, systems we identified as lacking an authority to operate, and security weaknesses that were not remediated timely. The FY 2021 IG metrics included a new SCRM domain within the Identify function. All OIGs were instructed not to formally consider the new domain metrics for the Identify function rating for this fiscal year.

DHS also did not have an effective process to ensure accurate security information is captured, reported, and communicated to relevant stakeholders. DHS uses its monthly scorecards and metrics to manage information system security risks, but we identified inaccuracies in the reporting of these metrics. For example, despite prohibiting the use of personal devices on its networks, the Department consistently reported Bring Your Own Device (BYOD) information in its scorecards for 9 consecutive months (January to September 2021). DHS officials stated this was reported in error, but DHS also reported this BYOD information in its quarterly FISMA submission to OMB in the first, second, and third quarters of FY 2021. This degree of misreporting could be an indicator that the Department and its components do not have an effective oversight process to ensure information is being properly captured and accurately reported in its monthly scorecards.

[20] *Evaluation of DHS' Information Security Program for Fiscal Year 2020*, OIG-21-72, September 30, 2021.

We also identified component systems that were operating with an expired ATO. Without valid ATOs, DHS cannot be assured effective controls are in place to protect sensitive information stored and processed by these systems. We also identified deficiencies in security weakness remediation, as several components did not effectively manage the Plan of Action and Milestones (POA&M) process as required by DHS. POA&M is a tool to correct information security weaknesses found during any review done by, for, or on behalf of the agency, such as audits or vulnerability assessments. A POA&M identifies tasks that need to be accomplished and details the resources required to accomplish elements of the plan, any milestones for meeting tasks, and scheduled completion dates for milestones.[21]

Risk Management

Managing risk is a complex, multifaceted activity that requires involvement of the entire organization. A key component of risk management is the authorization, or ATO, process by which an authorizing official reviews information describing the current security and privacy posture of information systems.[22] Per DHS guidance,[23] components are required to use enterprise management systems[24] that incorporate NIST security controls when performing security assessments of their systems. The security authorization package (also referred to as an ATO package) documents the results of the security assessment and provides the authorizing official with information needed to make a risk-based decision whether to authorize operation of the information system.

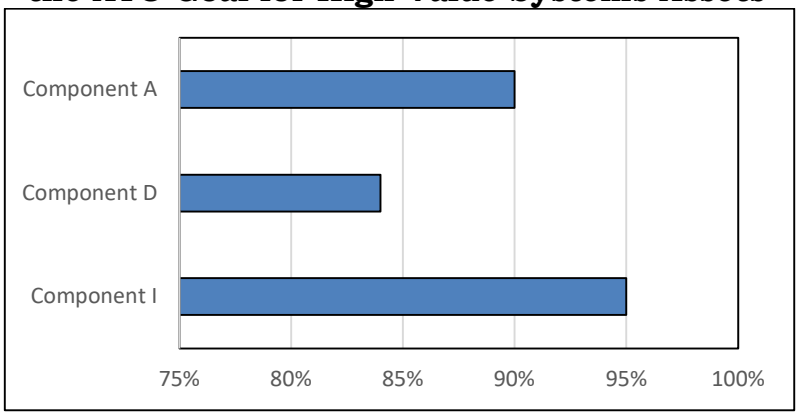
Based on OMB and NIST guidance,[25] system ATOs are typically granted for a specific period of time, in accordance with terms and conditions established by the authorizing official. In October 2013, DHS began allowing its components to enroll in an ongoing authorization program established by NIST.

DHS maintains a target goal of ensuring ATOs for 100 percent of its 145 high-value systems assets. The ATO target goal is 95 percent for its 427 operational

[21] OMB Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001.
[22] A Federal information system is an information system used or operated by an executive agency, a contractor of an executive agency, or another organization on behalf of an executive agency.
[23] DHS *FY21 Information Security Performance Plan*, Version 1.0, January 11, 2021.
[24] Enterprise management systems enable centralized storage and tracking of all documentation required for the authorization package of each system.
[25] OMB Circular A-130, *Managing Information as a Strategic Resource,* July 2016; NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* December 2018.

non-high value assets. Our independent review of DHS' August 2021 FISMA Scorecard for unclassified systems found that three components did not meet the required authorization target of 100 percent for high-value assets, as shown in Figure 1.

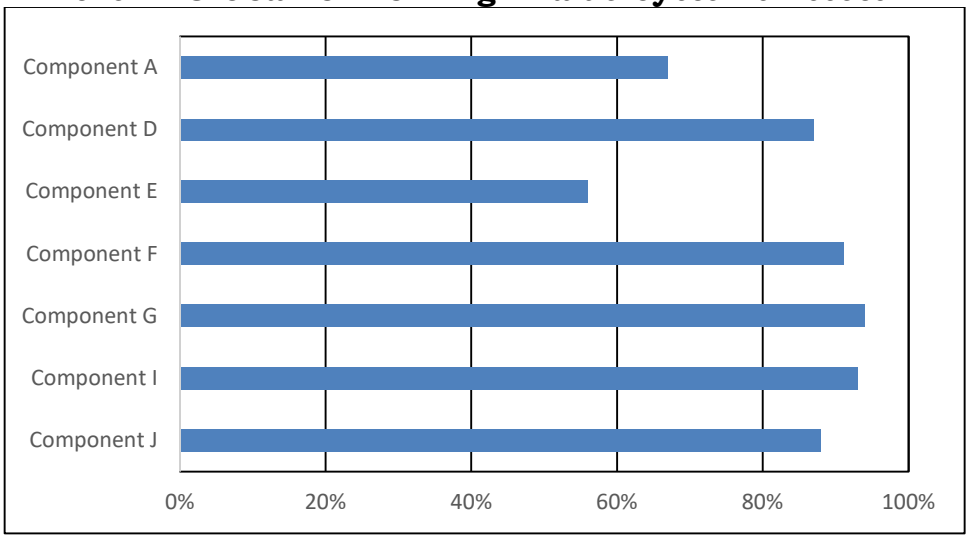
Figure 1. Selected Components' Performance Meeting the ATO Goal for High-Value Systems Assets



Source: DHS OIG analysis of DHS' August 2021 FISMA Scorecard

In addition, according to DHS' August 2021 FISMA Scorecard, 7 of 11 DHS components did not meet the security authorization target of 95 percent compliance for other operational non-high value assets, as shown in Figure 2.

Figure 2. Selected Components' Performance Meeting the ATO Goal for Non-High Value Systems Assets



Source: DHS OIG analysis of DHS' August 2021 FISMA Scorecard

To determine the components' compliance meeting DHS' NSS security authorization target, we examined the Department's August 2021 NSS Scorecard. We found that all components met DHS' NSS ATO target of 90 percent.

The total number of unclassified systems operating without ATOs has decreased by 25 percent since FY 2020. Our analysis of June 30, 2021 data from DHS' unclassified enterprise management system showed 56 of 568 systems across DHS did not have current ATOs. Table 4 outlines the number of unclassified systems operating without ATOs at selected components from FY 2019 to FY 2021.

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

Component	FY 2019	FY 2020	FY 2021
Component A	5	2	6
Component B	21	N/A	N/A
Component C	0	0	0
Component D	6	10	12
Component E	44	61	35
Component F	2	1	1
Component G	2	1	1
Component H	0	0	0
Component I	0	0	1
Component K	1	0	0
Total	**81**	**75**	**56**

Source: DHS OIG-compiled data from *Evaluation of DHS' Information Security Program for Fiscal Year 2019*, OIG-20-77, September 30, 2020; *Evaluation of DHS' Information Security Program for Fiscal Year 2020,* OIG-21-72, September 30, 2021

We also determined that DHS had not yet incorporated key security controls from 2018 NIST guidance.[26] Specifically, NIST increased the number of steps in its Risk Management Framework from six to seven by adding a new "Prepare" step in 2018. DHS had not yet updated its 4300A Policy,[27] Handbook,[28] and DHS Ongoing Authorization Methodology[29] to reflect these changes. We also noted that, in some cases, DHS' policies provided components with guidance that contradicted other DHS policies, as they refer to a rescinded version of a NIST publication. For example, DHS issued its

[26] NIST SP 800-37 Rev 2 *Risk Management Framework for Information Systems and Organizations,* December 2018.
[27] *DHS Sensitive Systems Policy Directive 4300A,* Version 13.1, July 27, 2017.
[28] *DHS 4300A Sensitive Systems Handbook,* Version 12.0, November 15, 2015.
[29] *DHS Ongoing Authorization Methodology,* Version 1.8, September 9, 2016.

System Security Authorization Process Guide, version 14.1 in April 2019, which accurately reflects NIST's seven-step Risk Management Framework. Yet, in October 2019, the former CIO issued minor changes to 4300A Policy 13.1.1 through a memorandum[30] that still reflected the prior six-step risk process NIST withdrew in December 2019. NIST published its SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations*, in December 2018.

DHS' inability to consistently update its policies and guidance to reflect NIST SP 800-37 Rev 2 resulted in noncompliance with OMB guidance. Specifically, OMB Circular A-130, *Managing Information as a Strategic Resource,* July 2016, requires agencies to meet the requirements of, and comply with, new or revised NIST standards and guidelines within 1 year of publication, unless otherwise directed by OMB. At the time of this evaluation, DHS was nearly 3 years behind to implement the changes from NIST's 2018 revision.

Weakness Remediation

OMB and DHS require using POA&Ms to track and plan the resolution of information security weaknesses. A POA&M details the resources required to accomplish elements of the plan, any milestones for meeting tasks, and scheduled completion dates for milestones.[31]

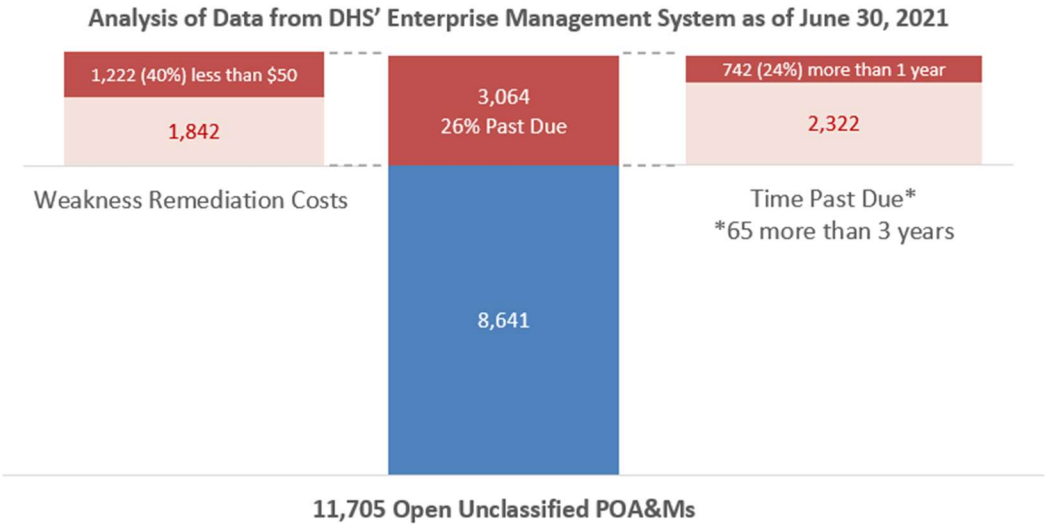
We found several components did not effectively manage the POA&M process as required by DHS. For example, although DHS requires[32] components to update POA&Ms monthly, not all components consistently maintained complete and accurate information on progress remediating security weaknesses. They also did not resolve all POA&Ms within 12 months as required[33] or consistently include estimates for resources needed to mitigate identified weaknesses.

Our analysis of 11,705 open unclassified POA&Ms from DHS' enterprise management system as of June 30, 2021, showed that 3,064 were past due; 742 were overdue by more than a year; and 65 were overdue by more than 3

[30] *DHS Change 13.1.1 to Department of Homeland Security Sensitive Systems Policy Directive 4300A*, October 2, 2019.
[31] OMB Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001.
[32] *DHS 4300A Sensitive Systems Handbook, Attachment H, Process Guide for Plan of Action and Milestones,* Version 14.0, June 21, 2019.
[33] *DHS Sensitive Systems Policy Directive 4300A,* Version 13.1, July 27, 2017.

years. Of the 3,064 past due unclassified POA&Ms, 1,222 had weakness remediation costs estimated at less than $50,[34] as shown in Figure 3.

Figure 3. Review of 11,705 Open Unclassified POA&MS



Our analysis of the August 2021 NSS FISMA Cybersecurity Scorecard identified DHS Headquarters (HQ) did not meet DHS' NSS weakness remediation metrics for POA&Ms. This has been a consistent finding in our FISMA reporting since 2003. We recognize the level of effort required by DHS to respond to the SolarWinds significant cyber incident in December 2020. An official from the Department's Office of the Chief Information Security Officer stated that DHS faced significant challenges in FY 2021, as its resources were diverted for critical SolarWinds response and recovery efforts.

Without valid ATOs and aggregated POA&M information, DHS cannot be assured that effective controls are in place to protect sensitive information stored and processed by these systems.

According to FY 2021 FISMA Reporting Metrics, our independent contractor rated components' Identify function at "Level 4 - Managed and Measurable" for Coast Guard and FLETC and "Level 5 – Optimized" for FEMA.

[34] To ensure sufficient resources are available to mitigate known information security weaknesses, DHS requires that components include a nominal weakness remediation cost of $50 when the cost cannot be estimated due to the complexity of tasks or other unknown factors.

Supply Chain Risk Management

According to the FY 2021 FISMA Reporting Metrics, OIGs were asked not to consider the new domain SCRM in the Identify function rating. However, OMB included SCRM within this function in the FY 2021 FISMA Reporting Metrics. The SCRM domain focuses on the maturity of agency SCRM strategies, policies and procedures, plans, and processes to ensure that 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*.

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 that DHS was operating at "Level 4 – Managed and Measurable" for the Protect function. For example, DHS employs automation to help maintain a complete, accurate, and readily available view of the security configurations for information systems connected to the network. DHS did not provide evidence that it consistently implemented or monitored its department-wide security awareness training strategy, and one component did not replace or update an unsupported operating system and did not apply security patches and updates timely to mitigate critical and high-risk security vulnerabilities on workstations, switches, and routers. DHS should focus on improving these key configuration management activities to ensure components are replacing unsupported operating systems and implementing security patches timely.

Configuration Management

We determined DHS was operating at "Level 3 – Consistently Implemented" in the Configuration Management Domain. DHS requires components manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches, and eliminating or disabling unnecessary services.

Although the components we reviewed implemented a vulnerability patch management program, they did not ensure that all known patch and software updates for critical and high-risk vulnerabilities were remediated timely. The results from our security scans on the three selected High Value Assets[35]

[35] A High Value Asset is information or an information system that is so critical to the Department that the loss or corruption of this information or loss of access to the system

systems identified critical and high-risk[36] patch vulnerabilities on selected workstations, switches, and routers, potentially exposing DHS data to unnecessary risk. The unique "individual" weaknesses we identified for these deficiencies were:

- three high-risk missing patches on 6 of 75 Windows 10 workstations tested at Component I;
- three critical missing patches on 42 switches and/or routers, and 35 high-risk missing patches on 1,912 switches and/or routers out of 1,977 network devices tested at Component I; and
- one critical missing patch on 336 switches and/or routers, and 13 high-risk missing patches on 957 switches and/or routers out of 1,193 network devices tested at Component K.

According to the components' officials, they mitigated the vulnerabilities identified by the next patching cycle. We did not perform subsequent testing to confirm whether the vulnerabilities identified were remediated.

Without implementing all proper configuration settings, sensitive information stored on components' systems may be exploited. DHS can further improve its key configuration management activities by replacing unsupported operating systems and applying timely security patches.

Unsupported Operating System

Known or new vulnerabilities can be exploited on operating systems for which vendors no longer provide software patch updates or technical support. For this reason, DHS requires components to discontinue use of unsupported operating systems. We identified a total of 21 switches and routers running unsupported operating systems at Component I that may expose DHS sensitive data to potential exploitation. Specifically, the manufacturer discontinued its support of the operating system for 2 switches in September 2019, 1 router in March 2021, and the remaining 18 switches between May and July 2021. According to Component I officials, due to pandemic travel restrictions it has been difficult to send technicians to replace all the unsupported hardware on site.

would have serious impact to the organization's ability to perform its mission or conduct business.

[36] Critical vulnerabilities have a score between 9 and 10 on the Common Vulnerability Scoring System (CVSS) version 3.0 scale, and High vulnerabilities are identified by having a CVSS version 3.0 score between 7.0 and 8.9.

Increased risk exists that DHS' sensitive information stores and processes by these workstations and network devices are subjected to potential exploitation when security patches are not applied timely to mitigate vulnerabilities. When unsupported network devices are not replaced timely, the product will become obsolete and may subject DHS sensitive information to significant security risks.

According to FY 2021 FISMA Reporting Metrics, our independent contractor rated components' Configuration Management domain at "Level 2 – Defined" for Coast Guard, "Level 3 - Consistently Implemented" for FEMA, and "Level 4 - Managed and Measurable" for FLETC.

Identity and Access Management

We determined DHS was operating at "Level 4 – Managed and Measurable" in the Identity and Access Management domain. Identity and access management is critical to ensure only authorized users can log onto DHS systems. DHS has taken a decentralized approach to identity and access management, leaving its components individually responsible for issuing Personal Identity Verification cards (access cards) for computer and building access, pursuant to Homeland Security Presidential Directive-12.[37] DHS requires all privileged and unprivileged employees and contractors to use Personal Identity Verification cards to log onto DHS systems. DHS did not demonstrate that its identity, credential, and access management program was properly resourced as required by FY 2021 FISMA Reporting Metrics. In addition, DHS did not have automatic mechanisms to manage its systems' user accounts.

According to FY 2021 FISMA Reporting Metrics, our independent contractor rated components' Identity and Access Management domain at "Level 4 – Managed and Measurable" for Coast Guard, FEMA, and FLETC.

Data Protection and Privacy

We determined that DHS was operating at "Level 4 – Managed and Measurable" in the Data Protection and Privacy domain. DHS provided evidence showing that the Department conducts its own independent review of its privacy program to make necessary improvements. DHS did not ensure that all of its users received the required privacy awareness training. In addition, DHS has

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

yet to complete its corrective actions to address the deficiencies cited in our report from November 2020 to improve the monitoring of its users to complete the annual privacy awareness training.[38]

According to FY 2021 FISMA Reporting Metrics, our independent contractor rated components' Data Protection and Privacy domain at "Level 1 – Ad Hoc" for Coast Guard and FLETC and "Level 2 – Defined" for FEMA.

Security Training Program

We determined DHS was operating at "Level 2 – Defined" in the Security Training domain. Educating employees about acceptable practices and rules of behavior is critical for an effective information security program. DHS has a security training program that is collaboratively managed by DHS HQ, the Office of the Chief Human Capital Officer, and the components. Specifically, the Department uses a Performance and Learning Management System to track employee completion of training, including security awareness courses. Components are required to ensure all employees and contractors receive annual IT security awareness training, as well as specialized training for employees with significant responsibilities.

DHS did not demonstrate that its security awareness and training program was properly resourced per the FY 2021 FISMA Reporting Metrics. Although DHS has assessed the knowledge, skills, and abilities of its cyber workforce, it has not finalized a strategy to address identified gaps outlined in its Cybersecurity Workforce Strategy. Without a cybersecurity workforce strategy, DHS cannot ensure its employees possess the knowledge and skills necessary to perform job functions, or that qualified personnel are hired to fill cybersecurity-related positions.

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 required configuration settings;
- discontinuing use of unsupported operating systems;
- applying security patches timely; and
- finalizing a strategy to address identified gaps outlined in its Cybersecurity Workforce Assessment.

[38] *DHS Privacy Office Needs to Improve Oversight of Department-wide Activities, Programs, and Initiatives*, OIG-21-06, November 4, 2020.

According to FY 2021 FISMA Reporting Metrics, our independent contractor rated components' Security Training domain at "Level 1 – Ad Hoc" for FEMA, "Level 3 – Consistently Implemented" for Coast Guard, and "Level 4 – Managed and Measurable" for FLETC.

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 that DHS was operating at "Level 3 – Consistently Implemented" in this function. We based this rating on our conclusion that DHS did not demonstrate that it has defined, documented, or communicated its ISCM roles and responsibilities in accordance with NIST SP 800-137. Also, DHS did not establish an ongoing authorization program for its NSS.

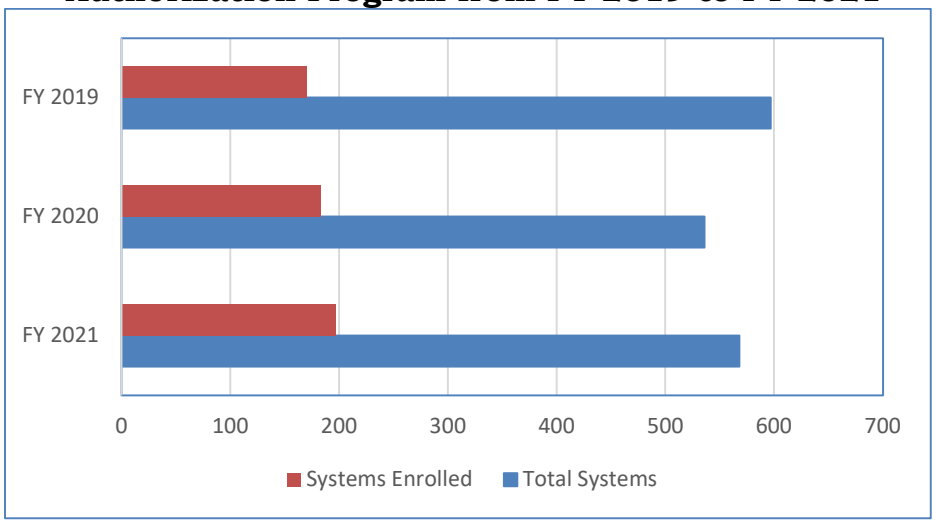
According to NIST, an effective ISCM program should begin with developing a comprehensive strategy addressing ISCM requirements and activities at each organizational tier (organization, mission/business processes and information systems) and include metrics that provide meaningful indications of security status at all organizational tiers.

We determined that DHS has not clearly defined its ISCM stakeholder's responsibilities. We reviewed DHS' *Information Security Continuous Monitoring Strategy, An Enterprise View*, dated October 19, 2017, and DHS 4300A Policy, but did not see evidence of roles and responsibilities needed to execute the ISCM strategy process as defined in NIST SP 800-137 (Define, Establish, Implement, Analyze/Report, Respond, and Review/Update).

DHS also relied on data calls via email to maintain visibility into each component's NSS, instead of using the enterprise management tool or other information validation procedures that create security artifacts for monitoring and authorizing each system. In addition, DHS did not establish an ongoing authorization program for its NSS.

As of July 2021, seven components were enrolled in the Department's ongoing authorization program. The Department had increased the number of systems enrolled in the program by 13 percent from FY 2019 to FY 2021, see Figure 4.

Figure 4. DHS Systems Enrolled in the Ongoing Authorization Program from FY 2019 to FY 2021



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

DHS did not ensure accurate reporting of the data supporting metrics in its monthly scorecard. Our review of DHS' monthly scorecards identified misreported metrics for nine consecutive months, from January to September 2021. Specifically, DHS officials stated the BYOD metrics were reported in error, as the Department prohibits the use of BYOD on its networks. But DHS also included this data in its quarterly FISMA submission to OMB in the first, second, and third quarters of FY 2021.

Without accurate reporting of information and updating policies, DHS' senior leadership cannot make sound risk-based decisions about the information security program. This degree of misreporting can be an indicator that the Department and its components do not have an effective oversight process to ensure its security information is being properly captured and accurately reported in its monthly scorecards or quarterly FISMA submissions to OMB.

According to FY 2021 FISMA Reporting Metrics, our independent contractor rated components' Detect function at "Level 3 – Consistently Implemented" for Coast Guard, "Level 4 - Managed and Measurable" for FLETC, and "Level 5 – Optimized" for FEMA.

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

We determined that DHS was operating at "Level 3 – Consistently Implemented" in this function as the Department did not demonstrate that it (1) has developed qualitative metrics to measure the effectiveness of its overall incident response capability, (2) allocates resources (people, processes, and technology) in a risk-based manner for stakeholders to effectively implement its incident response activities, (3) has developed qualitative performance measures to evaluate the effectiveness of its incident detection and analysis policies and procedures, (4) has developed qualitative performance measures to evaluate the effectiveness of its incident handling policies and procedures, and (5) uses metrics to measure and manage the timely reporting of incident information to Department officials and external stakeholders.

Incident Response

In FY 2021, DHS reported one major incident. According to applicable FISMA major incident reporting requirements, the Department notified selected congressional oversight committees of the following:

- December 11, 2020: The DHS Cybersecurity and Infrastructure Security Agency notified DHS Office of the Chief Information Officer of a potential cybersecurity incident. The Microsoft Detection and Response Team analysis found that 34 Federal employee and contractor mailboxes had been accessed since at least August 2020, with a belief that all mail in the affected users' mailboxes had been transferred off network to systems controlled by a potentially malicious actor. Attackers were able to insert malicious code at an early stage of the software build (supply chain compromise) affecting SolarWinds Orion products. Combined response efforts on DHS systems impacted by the campaign identified and mitigated the compromise between December 2020 and February 2021.

According to FY 2021 FISMA Reporting Metrics, our independent contractor rated components' Respond function at "Level 3 – Consistently Implemented" for Coast Guard, "Level 4 - Managed and Measurable" for FLETC, and "Level 5 – Optimized" for FEMA.

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.*

We determined DHS' "Recover" function was operating at "Level 2 – Defined." DHS did not achieve "Level 3 – Consistently Implemented" because it did not provide evidence that its system-level Business Impact Analysis is integrated with the Department level Business Impact Analysis.

DHS defined its policies, procedures, and strategies for information contingency planning, but did not fully test these plans. For example, as of June 2021, 24 unclassified systems contingency plans had not been tested. Further, DHS did not demonstrate (1) it has consistently implemented its policies and procedures to perform information system backups, and (2) its information system contingency plans are being consistently developed and implemented or integrated with other continuity areas, such as organization and business process continuity, disaster recovery planning, incident management, insider threat implementation plan, and occupant emergency plans.

Contingency Planning

DHS has a department-wide business continuity program to respond to emergency events, restore essential business functions, and resume normal operations. As part of this program, DHS implemented a Reconstitution Requirements Functions Worksheet to collect information on components' key business requirements and capabilities needed to recover from attack or disaster. DHS used this information to develop a Reconstitution Plan that outlines procedures at a macro level for all DHS senior leadership, staff, and components to follow 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.

DHS components are responsible for developing and periodically testing such contingency plans outlining backup and disaster recovery procedures for the respective information systems.[39] However, as of June 30, 2021, we identified the following deficiencies:

- Our review of the June 2021 NSS Scorecard identified that DHS HQ did not meet DHS' NSS compliance target for contingency plan testing.

[39] *DHS Sensitive Systems Policy Directive 4300A,* Version 13.1, July 27, 2017.

- CISA, DHS HQ, FEMA, U.S. Immigration and Customs Enforcement, Transportation Security Administration, and U.S. Citizenship and Immigration Services had not tested contingency plans for 24 of 568 unclassified systems, based on our analysis data from DHS' enterprise management system as of June 30, 2021.

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 timely.

According to FY 2021 FISMA Reporting Metrics, our independent contractor rated components' "Recover" function at "Level 3 - Consistently Implemented" for Coast Guard, FEMA, and FLETC.

Summary of Selected Components' Implementation of Information Security Programs

Our independent contractor rated component information security programs effective for FEMA and FLETC, as each achieved "Level 4 – Managed and Measurable" or higher in three of the five functions. Because the Department performs several security functions on FEMA's and FLETC's behalf, these components have not yet developed component-specific policies, procedures, and business processes, as required by DHS policy. Coast Guard's overall information security program was not effective because it only achieved "Level 4 – Managed and Measurable" in two of five functions. Table 5 summarizes the implementation of information security programs by FEMA, FLETC, and Coast Guard.

Table 5. Summary Status of FEMA, FLETC, and Coast Guard Information Security Programs for FY 2021

Function	FEMA	FLETC	Coast Guard
Identify	Level 5 – Optimized	Level 4 – Managed and Measurable	Level 4 – Managed and Measurable
Protect	Level 3 – Consistently Implemented	Level 4 – Managed and Measurable	Level 4 – Managed and Measurable
Detect	Level 5 – Optimized	Level 4 – Managed and Measurable	Level 3 – Consistently Implemented
Respond	Level 5 – Optimized	Level 4 – Managed and Measurable	Level 3 – Consistently Implemented
Recover	Level 3 – Consistently Implemented	Level 3 – Consistently Implemented	Level 3 – Consistently Implemented
Overall Rating	**Effective**	**Effective**	**Ineffective**

Source: DHS OIG contractor

Since 2019, our independent contractor has performed fieldwork at nine selected components and rated four components' information security programs as "ineffective" because the components achieved below "Level 4 – Managed and Measurable" in three of five functions, in accordance with the FY 2021 FISMA Reporting Metrics.

Recommendations

We recommend the DHS Chief Information Officer:

Recommendation 1: Enforce requirements for components to obtain authority to operate, resolve critical and high-risk vulnerabilities, and apply sufficient resources to mitigate security weaknesses.

Recommendation 2: Strengthen the review and validation process to ensure accurate security information is reported in the monthly scorecards and CIO's quarterly submission to OMB.

Recommendation 3: Revise DHS 4300A Policy, Handbook, and Ongoing Authorization methodology to incorporate applicable changes from NIST Special Publications, including SP 800-37, Revision 2, SP 800-53 Revision 5, and SP 800-137A to maintain consistency between the documents.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Director of the Departmental GAO-OIG Liaison Office (Director), who expressed the Department's appreciation for OIG's work in planning and conducting its review and issuing this report. The Department did not provide any technical comments to the draft report, as part of its response or under a separate cover.

The following is our evaluation of the Department's written comments and its response to each recommendation in the draft report.

OIG Response to Overall Management Comments

According to the Director, "senior DHS leadership disagrees with OIG's overall assessment and believes that OIG's rating of "Not Effective" for fiscal year (FY) 2021 is more reflective of OIG having completed a compliance review, rather than the risk-based assessment envisioned by Office of Management and Budget (OMB) as described in its FY 2021 OIG Federal Information Security Modernization Act (FISMA) Reporting Metrics guidance."[40] The Director cited OMB M-22-05 as the source of this comment. However, OMB issued M-22-05 in December 2021 for the FY 2022 FISMA reporting period. We performed our work by following all applicable FY 2021 OMB reporting requirements[41] and applying the applicable scoring methodology cited in FY 2021 FISMA Reporting Metrics,[42] not OMB M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*.

Per FY 2021 FISMA Reporting Metrics, one of the annual FISMA evaluation's goals is to assess agencies' progress toward achieving outcomes that strengthen Federal cybersecurity, including implementing the Administration's cybersecurity priorities and best practices. Each OIG is required to evaluate its agency's information security program using a set of questions that are derived

[40] *See* https://www.whitehouse.gov/wp-content/uploads/2021/12/M-22-05-FY22-FISMA-Guidance.pdf for OMB M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*, December 6, 2021.
[41] FY 2021 guidance, which we used in our evaluation, is put forth in OMB M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*, November 9, 2020.
[42] *FY 2021 Inspector General FISMA Reporting Metrics*, Version 1.1, May 12, 2021.

from the maturity models outlined within the NIST Cybersecurity Framework. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides OIGs with guidance for assessing the maturity of controls to address those risks. Using this approach, we assessed the overall effectiveness of the program and the rating for each of the functions based on our analysis of the maturity level of the Department's current practices and existing policies and procedures.

Further, OIGs have the discretion to determine the overall effectiveness rating and rating for each of the Cybersecurity Framework functions at the maturity level of their choosing.[43] Using this approach, the OIG may determine that a particular function area and/or the agency's information security program is effective at a maturity level lower than Level 4. As such, there is no requirement for the OIG to come to agreement with the CIO on the Department's effectiveness rating and the rating for each of the Cybersecurity Framework functions.

Response to Report Recommendations:

The Department concurred with all three recommendations. Following is a summary of DHS' response to each recommendation and the OIG's analysis.

DHS Comments to Recommendation #1: Concur. In FY 2021, the Office of the CISO initiated efforts to standardize the Department's Ongoing Authorization program across all components. This effort will migrate most of the Department's systems to Ongoing Authorization, which will improve security control oversight, while reducing the administrative burden of authority to operate renewals. Further, the Office of the CISO's Vulnerability Assessment Team is currently working to address high-risk vulnerabilities by improving visibility through custom queries of the Department's Continuous Diagnostics and Monitoring data for the critical vulnerabilities reported to be actively exploited. Also in 2021, the DHS Vulnerability Assessment Team, in coordination with the components, developed tailored protection and discovery mechanisms for emerging vulnerabilities. Estimated Completion Date: September 30, 2022.

[43] *FY 2021 Inspector General FISMA Reporting Metrics*, Version 1.1, May 12, 2021.

OIG Analysis of DHS Comments
DHS' actions are responsive to this recommendation, which will remain open and resolved until DHS provides documentation showing that all planned corrective actions are completed.

DHS Comments to Recommendation #2: Concur. DHS acknowledges that an administrative oversight resulted in government-issued mobile devices being incorrectly reported as personally-owned mobile devices and that this information was included in the DHS Monthly FISMA Scorecard until the issue was discovered and corrected. In response to this incident, DHS OCIO restructured the process by which component inputs are incorporated into the Scorecard to include monthly component cross checks, along with additional analysis and reviews. Altogether, this revised Scorecard production process has reduced the opportunity for human error to impact future Monthly Scorecards. DHS requests the OIG consider this recommendation resolved and closed, as implemented.

OIG Analysis of DHS Comments

DHS' actions are responsive to this recommendation. Based on the Department's corrective actions and the supporting documentation provided, this recommendation is closed and resolved.

DHS Comments to Recommendation #3: Concur. Officials stated that DHS' 4300A, *Sensitive Systems Handbook*, dated November 15, 2015, is currently undergoing a significant update to better align with applicable Federal mandates, DHS Management Directive standards, and industry common practices, including the documents mentioned in this recommendation. In FY 2021, the intensity of the response to the SolarWinds incident, and the pace of procedural changes afterward, hindered this update and integration of new policies with the revision of existing policies in 4300A. However, DHS' Office of CIO is simplifying the 4300A policy process and procedures, eliminating the *Sensitive Systems Handbook*, shortening the 4300A Policy Directive from several hundred pages to 84 pages, and socializing the updated policies with DHS components. This effort will culminate in a full update to 4300A, and all dependent policies, by the end of FY 2022. Estimated Completion Date: September 30, 2022.

OIG Analysis of DHS Comments

DHS' actions are responsive to this recommendation, which will remain open and resolved until DHS 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) by amendment to the *Inspector General Act of 1978*.

The objective of our evaluation was to determine whether DHS' information security program and practices are adequate and effective to protect the information and information systems that support DHS' operations and assets for FY 2021. Our independent evaluation focused on assessing DHS' information security program against requirements outlined in the *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (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 Office of the CISO and at selected organizational components and offices: DHS HQ, United States Secret Service, and Transportation Security Administration. 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:

- referenced our FY 2018, FY 2019, and FY 2020 FISMA evaluations as a baseline for the FY 2021 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.

Using scanning tools, OIG internal specialists conducted vulnerability assessments of controls implemented at two components. We also reviewed

information from DHS' enterprise management systems to determine data reliability and accuracy. We found no discrepancies or errors in the data. OIG contractors performed fieldwork at Coast Guard, FEMA, and FLETC to support our evaluation.

We conducted this review between July 2021 and March 2022, under the authority of the *Inspector General Act of 1978*, *as amended*, 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 OIG's compliance with FISMA requirements during our review.

Appendix B
Management Comments to the Draft Report

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

Homeland Security

July 12, 2022

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

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

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2022.07.12 13:30:32 -04'00'

SUBJECT: Management Response to Draft Report: "Evaluation of DHS' Information Security Program for Fiscal Year 2021" (Project No. 21-038-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.

Senior DHS leadership *disagrees* with OIG's overall assessment and believes that OIG's rating of "Not Effective" for fiscal year (FY) 2021 is more reflective of OIG having completed a compliance review, rather than the risk-based assessment envisioned by Office of Management and Budget (OMB) as described in its FY 2021 OIG Federal Information Security Modernization Act (FISMA) Reporting Metrics guidance.[1] As a result, the OIG's report does not sufficiently account for risk-based innovation, such as the Department's development of processes outside the checklist's scope designed to effectively protect the information and information systems that supported DHS' operations and assets during FY 2021, thus the report misrepresents the Department's overall information security efforts.

It is important to note that, since January 2021, DHS has been transitioning to risk-based cybersecurity management processes, as has the rest of the federal government, to materially improve information systems' resistance to, and recovery from, cyber-attack. For example, DHS addressed the most significant risk to the organization in FY 2021 by accelerating its Cyber Supply Chain Risk Management (C-SCRM) implementation in the wake of the Solar Winds (SW) incident, which emphasizes supply chain security for both commercial software products/services, as well as vendor cyber hygiene. While the OIG

[1] https://www.whitehouse.gov/wp-content/uploads/2021/12/M-22-05-FY22-FISMA-Guidance.pdf

did an *excellent* job evaluating compliance-related issues, none of this really contributed to an overall effectiveness analysis because supply chain risk management was not included in the OIG's compliance checklist for FY 2021.

Further, DHS leadership is concerned that that the limited scope of the OIG's audit leaves readers with an incomplete assessment of the Department's activities, and is unhelpful for promoting innovation with regard to measuring cybersecurity currently emerging from the Executive and Legislative branches of the Federal government. For example, DHS notes the interest from Congress in FISMA Reform, and as expressed in OMB M22-05, "Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements," dated December 6, 2021, which emphasizes adopting a risk-based approach to security management.

Building on the foundation which gained the Department an "Effective" rating in FY 2020, the significant accomplishments DHS has achieved in FY 2021 to improve the effectiveness of cybersecurity management processes, while migrating to a risk-based approach include, but are not limited to the following examples. DHS leadership believes that these examples of success should be evaluated during future annual FISMA audits as part of a risk-based (and not compliance-oriented) focus:

- Beginning in quarter 1 (Q1) of FY 2021, initiating the development of a DHS Unified Cybersecurity Maturity Model (UCMM) in support of cross-enterprise recovery efforts, which results in DHS having the means to view prioritization, planning, and budgeting to align Department-wide cybersecurity investment to maturing cybersecurity posture.

- Accelerating DHS information communications technology SCRM implementation throughout FY 2021 by establishing programmatic and process discipline to: (1) manage information flows; (2) assess security of critical software product development; (3) assess vendor cyber maturity to ensure proper handling of DHS data; and (4) exercise routine monitoring of products, services, and software across the enterprise to understand where corporate changes (e.g., mergers, buy-outs, offshoring, foreign interests) may pose risks.

- Throughout FY 2021 in modernizing the DHS telecommunications infrastructure and establishing software-defined wide area networks, thereby reducing the Department's attack surface.

- Expanding the DHS Cybersecurity Services Provider Program to assess the effectiveness and efficiency not only of Security Operation Centers (completed for DHS in FY 2020) but also Network Operation Centers, based on an interagency standard best practice framework in FY 2021.

- Reaching final operational capability for the DHS Network Operations Security Center in Q4 FY 2021, which included consolidating network and cybersecurity operations from eleven operational entities and three tenant enclaves throughout DHS into a single enterprise-wide service network, cybersecurity, and cloud service provider.

- Planning the Department's first bug bounty program, "Hack DHS," which utilized Congressionally-provided authorities to engage external researcher and "white hat" hacker communities to provide assessment of high value systems across the Department reaching full capability in Q1 FY 2022.

- Aligning cybersecurity training oversight under the DHS Chief Information Security Officer (CISO) Council – the Department cybersecurity governance body headed by the DHS CISO - which approved a work plan to improve cybersecurity training and awareness across the enterprise.

- Implementing a Cyber Operational Risk Management process (in development by DHS since FY 2020) to assess all DHS High Value Assets in FY 2021. This process visualizes enterprise risk, and equips cybersecurity decision-makers with prioritized actions to reduce system risks (such as those managed through Plans of Action & Milestones) in alignment with the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF).

- Prioritizing implementation of innovative mission-driven, person-focused, market-sensitive approaches to hiring, compensating, and developing cybersecurity talent across the Department, such as the Cyber Talent Management System, a personnel system launched in November 2021 that will enable DHS to more effectively recruit, develop, and retain our nation's top cybersecurity professionals.

The draft report contained three recommendations with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual 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 Project No. 21-038-AUD-DHS

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

Recommendation 1: Enforce requirements for components to obtain authority to operate, resolve critical and high-risk vulnerabilities, and apply sufficient resources to mitigate security weaknesses.

Response: Concur. In FY 2021, The DHS Office of the Chief Information Security Officer (OCISO) Cybersecurity Compliance Branch initiated efforts to standardize the Department's Ongoing Authorization program (OA) across all Components. This effort will migrate most of the Department's systems to OA, which will improve security control oversight, while also reducing the administrative burden of authority to operate renewals.

The OCISO Vulnerability Assessment Team (VAT) is currently working to address high-risk vulnerabilities by improving visibility through custom queries of the Department's Continuous Diagnostics and Monitoring data for the critical vulnerabilities reported to be actively exploited. Also in 2021, the DHS VAT, in coordination with subordinate Component VATs, developed tailored protection and discovery mechanisms for emerging vulnerabilities.

In addition, the UCMM, which is aligned to the NIST CSF and other Federal guidance, provides a platform by which investment effectiveness can be measured, and future investments planned, based on their potential to improve cybersecurity functions and reduce system risk.

Estimated Completion Date (ECD): September 30, 2022.

Recommendation 2: Strengthen the review and validation processes to ensure accurate security information is reported in the monthly scorecards and CIO's quarterly submission to OMB.

Response: Concur. DHS acknowledges that an administrative oversight resulted in government-issued mobile devices being incorrectly reported as personally-owned mobile devices, and that this information was included in the DHS Monthly FISMA Scorecard until the issue was discovered and corrected. In response to this incident, DHS OCIO restructured the process by which Component inputs are incorporated into the Scorecard to include Component cross checks on a monthly basis, along with additional analysis and reviews. Altogether, this revised Scorecard production process has reduced the opportunity

for human error to impact future Monthly Scorecards.

DHS requests the OIG consider this recommendation resolved and closed, as implemented.

Recommendation 3: Revise DHS 4300A Policy, Handbook, and Ongoing Authorization methodology to incorporate applicable changes from NIST Special Publications, including SP 800-37, Revision 2, SP 800-53 Revision 5, and SP 800-137A to maintain consistency between the documents.

Response: Concur. DHS 4300A, "Sensitive Systems Handbook," dated November 15, 2015, is currently undergoing a significant update to better align with applicable Federal mandates, DHS Management Directive standards, and industry common practices, to include the documents mentioned in this recommendation. In FY 2021, the intensity of the response to the SW breach, and the pace of procedural changes afterward, hindered this update and integration of new policies with the revision of existing policies in 4300A. However, DHS OCIO is simplifying the 4300A policy process and procedures, eliminating the Sensitive Systems Handbook, shortening the 4300A Policy Directive from several hundred pages to 84 pages, and socializing the updated policies with DHS Components. This CISO effort will culminate in a full update to DHS 4300A, and all dependent policies, by the end of FY 2022.

ECD: September 30, 2022.

5

Appendix C
Major Contributors to This Report

Chiu-Tong Tsang, Director
Shawn Hatch, Audit Manager
Sonya Davis, Auditor-in-charge
Brendan Burke, Auditor
Samantha Stout, Program Analyst
Bridgette OgunMokun, Program Analyst
Thomas Rohrback, Branch Director, Cybersecurity Risk Assessment Division
Rashedul Romel, Supervisory IT Cybersecurity Specialist
Jason Dominguez, Supervisory IT Cybersecurity Specialist
Taurean McKenzie, IT Cybersecurity Specialist
Thomas Hamlin, Communications Analyst
Garrick Greer, Referencer

Appendix D
Committee on Oversight and Reform Questions and Responses

On June 2, 2021, the Committee on Oversight and Reform asked that several questions be addressed as part of the FISMA FY 2021 effort. Specifically, we were asked to include an assessment of any vulnerabilities created or exacerbated by the Department's use of remote-access software to facilitate telework during the coronavirus pandemic and whether any such vulnerabilities were effectively mitigated.

Our independent contractor collected the responses from FEMA, FLETC, and Coast Guard to the Committee's questions. The questions and responses are summarized below:

1. **Examine the acquisition, deployment, management, and security of remote connections to Department networks, including those facilitated by Virtual Private Network (VPN)s and/or virtual network controllers.**

Components used applications that were already in place prior to the pandemic, such as Microsoft TEAMS, the Department VPN, and Virtual Desktop Infrastructure. Due to increased telework use, all three components took measures to increase bandwidth to provide better audio and video content when using collaboration platforms such as Microsoft TEAMS, Zoom, Adobe Connect, and Commercial Virtual Remote (decommissioned June 2021). In addition, components increased software licenses and purchased more laptops to allow more people to telework.

2. **Examine the acquisition, deployment, management, and security of collaboration platforms such as Microsoft Teams, Zoom, Slack, and Cisco WebEx.**

FEMA continued to use Microsoft TEAMS, Zoom, and Adobe Connect during the pandemic. FLETC made no adjustments to its telework arrangement and continued to use Microsoft TEAMS. Coast Guard used the *Coronavirus Aid, Relief, and Economic Security Act* funding to purchase Microsoft Office 365 licenses. Additionally, Coast Guard continued to use Commercial Virtual Remote collaborative tool, which is paid for by DoD. Coast Guard also used Zoom. Components worked with DHS to increase bandwidth due to increased telework use during the pandemic. FEMA made no changes and continued to use Adobe Connect during the pandemic. As a part of its services, DHS performed security management and monitoring for FLETC. Lastly, Coast

Guard's use of Zoom was managed by the General Services Administration, while DoD managed Commercial Virtual Remote.

3. Examine whether the Department, and all components, has implemented security controls to prevent the unauthorized dissemination of controlled unclassified information, personally identifiable information, or sensitive but unclassified information via third-party collaboration platforms.

FEMA only allows access to its internal networks for its users and implemented technical configurations to prevent its internal users from inviting an external user to Microsoft TEAMS meetings. FLETC has no other technical controls on sharing sensitive information other than educating its users through annual cyber awareness training and issued guidance on handling personally identifiable information and handling of sensitive information. Lastly, Coast Guard stated the same policies are already in place for the protection and disclosure of information.

4. Examine whether the identity, credential, and access management of users that permit remote access to Department networks, including the extent to which the Department has enabled multi-factor authentication and implemented procedures to disable inactive and potentially unauthorized user accounts.

Components use multi-factor authentication, Personal Identity Verification cards, and Common Access Cards for remote access. Prior to teleworking, personnel must sign telework agreements. This requirement has continued during the pandemic. DHS monitors VPN and telework for components. Specific to the pandemic, FEMA added monitoring for remote access from outside the Continental United States to trigger alerts for tracking and investigation. For Coast Guard, it monitors all users' access using Common Access Cards[44] and personal identification numbers. Coast Guard has account lockout procedures in place if users' accounts are locked from failed login attempts. In addition, Coast Guard already had remote user inactivity timing set by Active Directory Group Policy.

[44] A Common Access Card is similar to a Personal Identity Verification card used by Coast Guard personnel.

5. Examine the distribution and management of virtual and physical assets that facilitate telework, including laptop computers, smartphones, and RSA tokens.

One component mailed laptops and smartphones to telework eligible employees. If employees had to meet at the component locations to pick up their equipment, they had to schedule appointments with their respective IT Office, have a negative COVID test result, wear a face mask, and follow social distancing rules when in the facility. Components also offered staggered appointment times due to the pandemic. Component Human Resources also staggered appointments for benefit paperwork and meetings with sponsors.

FEMA's IT Property Management Branch team is responsible for handling and distributing all government furnished equipment. During the pandemic, if an employee picked up the equipment in person, he or she hand-signed a receipt. If an employee received the equipment via United Postal Service delivery, he or she digitally signed a receipt. All receipts were uploaded into the Sunflower Asset Management System. Coast Guard and FLETC followed the same procedures established prior to the pandemic to manage equipment.

6. Examine the Department's adherence to Trusted Internet Connection 3.0 guidance.

FEMA uses existing DHS Trusted Internet Connection for cloud environments and internet traffic. There have been no changes as a result of the pandemic. FLETC's internet traffic goes through OneNet and did not implement changes as a result of the pandemic. Lastly, Coast Guard does not subscribe to the Trusted Internet Connection and follows DoD requirements using a similar solution.

7. Examine whether the Department's CIO and all component CIOs implemented additional security policies in response to coronavirus-related telework and how they are enforcing those policies.

Because telework was already in place prior to the pandemic, FEMA and FLETC did not implement additional security policies. Due to the pandemic, Coast Guard emailed the telework policy to all personnel informing on their roles and responsibilities.

8. Determine whether the Department has implemented continuous monitoring and scanning of networks to identify vulnerabilities.

Due to the pandemic, FEMA has conducted additional monitoring of alerts on travel outside of the United States to ensure its remote workforce works inside

the country. FEMA made no change to its vulnerability scanning policy despite the increase in its remote workforce during the pandemic. FLETC uses the Department's VPN to allow telework, and officials stated that no changes were made to its vulnerability scanning schedules in response to the pandemic.

Lastly, Coast Guard ensured its existing continuous monitoring tools worked as designed while using remote VPN or Virtual Desktop Infrastructure connections and completed work to ensure that VPN device scanning was enabled. Coast Guard did not add any new tools for its remote workforce.

Appendix E
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
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, FEMA, ICE, I&A, USCIS, CISA, S&T, TSA, 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 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" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, 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