OFFICE OF INSPECTOR GENERAL

Evaluation of DHS' Information Security Program for Fiscal Year 2020

Homeland Security

September 30, 2021

OIG-21-72

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

September 30, 2021

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: 2021.09.30 09:25:08 -04'00'

SUBJECT: *Evaluation of DHS' Information Security Program for Fiscal Year 2020*

Attached is our final report, *Evaluation of DHS' Information Security Program for Fiscal Year 2020.* We incorporated the formal comments provided by the Department.

The report contains four recommendations aimed at improving the Department's information security program. The Department concurred with all four recommendations which, based on information provided in the Department's response to the draft report, we consider 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 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 B. Miller, Deputy Inspector General for Audits, at (202) 981-6000.

cc: Federal Emergency Management Agency, CIO
Science and Technology Directorate, CIO
Transportation Security Administration, CIO

DHS OIG HIGHLIGHTS

Evaluation of DHS' Information Security Program for Fiscal Year 2020

September 30, 2021

Why We Did This Evaluation

We reviewed Department of Homeland Security's information security program for compliance with *Federal Information Security Modernization Act of 2014* requirements. We conducted our evaluation according to fiscal year 2020 reporting instructions. Our objective was to determine whether DHS' information security program and practices adequately and effectively protected data and information systems supporting DHS' operations and assets for FY 2020.

What We Recommended

We made four 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

In May 2020, the Department of Homeland Security (DHS) formally documented its risk acceptance to allow the United States Coast Guard to meet *Federal Information Security Modernization Act of 2014* (FISMA) requirements according to Department of Defense, rather than DHS, reporting requirements. Therefore, when evaluating the overall effectiveness of the DHS information security program for FY 2020 FISMA, our rating does not include the Coast Guard. Also, our rating of DHS' program is contingent on the Department's completion of its corrective actions to our prior recommendations, such as revising its information security policies and procedures to reflect senior leadership's approval of Coast Guard's FISMA reporting to the Department of Defense and communicating the decision, in writing, to the Office of Management and Budget and selected congressional oversight committees.

DHS' information security program earned an overall rating of effective, with a maturity rating of "Managed and Measurable" (Level 4) in three of five functions. Specifically, we identified:

- systems operating without authority to operate;
- known information security weaknesses not promptly mitigated;
- security configuration settings not implemented for all systems; and
- use of an unsupported operating system and not applying security patches promptly.

DHS Response

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

Table of Contents

Appendixes

Abbreviations

ATO	Authority to Operate
CISA	Cybersecurity and Infrastructure Security Agency
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CBP	U.S. Customs and Border Protection
DISA	Defense Information Systems Agency
DoD	Department of Defense
ECD	Estimated Completion Date
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Modernization Act of 2014
HQ	Headquarters

ICE	U.S. Immigration and Customs Enforcement
ISCM	Information Security Continuous Monitoring
NIST	National Institute of Standards and Technology
NSS	National Security System
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
S&T	Science and Technology Directorate
TSA	Transportation Security Administration
U.S.C.	United States Code

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). Specifically, FISMA requires Federal agencies to develop, document, and implement agency-wide information security programs.[4] 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.[5] According to FISMA, agencies are responsible for conducting annual evaluations of information programs and systems under their purview, as well as assessing related information security policies and procedures. 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.[6] The Office of Inspector General (OIG) is responsible for conducting annual evaluations of information programs and systems under its purview.

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 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.[7]

The DHS Chief Information Security Officer (CISO) bears primary responsibility for protecting information and ensuring compliance with FISMA. Specifically, the DHS CISO heads the Information Security Office and manages the

[1] 44 U.S.C. § 3551 *et.seq.*
[2] *Id.* at § 3552(a)(3).
[3] *Id.* at § 3551(1).
[4] *Id.* at § 3554(b).
[5] *Id.*
[6] *Id.* at § 3554(a)(5).
[7] Cybersecurity is the process of protecting information by preventing, detecting, and responding to attacks.

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. 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 comprehensive framework to govern the information systems owned and operated across DHS.

Foremost to all DHS components is adhering to requirements set forth in the DHS security authorization process, which involves comprehensive testing and evaluation of security features of an information system before it becomes operational within the Department. This evaluation process results in an Authority to Operate (ATO) decision, whereby a senior organizational official authorizes the operation of an information system based on an agreed-upon set of security controls. Per DHS guidelines,[8] as part of the security authorization process, each component CISO is required to assess the effectiveness of controls implemented on all component information systems before authorizing the systems to operate, and periodically thereafter. The DHS CISO relies on two enterprise management systems to help administer the information security program and keep track of security authorization status. 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.[9]

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. Further, *FY 2020 Inspector General FISMA Reporting Metrics*[10] (FY 2020 FISMA Reporting Metrics) provide OIG with reporting requirements for addressing key areas identified during their independent evaluations of agency information security programs. Each agency Inspector General has discretion to determine both an overall

[8] DHS *FY20 Information Security Performance Plan*, Version 1.2, December 20, 2019.
[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] *FY 2020 Inspector General FISMA Reporting Metrics* (Version 4.0, April 17, 2020) were developed as a collaborative effort among the Office of Management and Budget (OMB), DHS, and the Council of the Inspectors General on Integrity and Efficiency, in consultation with the Federal Chief Information Officer Council.

effectiveness rating, as well as a rating for each of the Cybersecurity Framework functions (i.e., Identify, Protect, Detect, Respond, and Recover) at the maturity level of their choosing. Using this approach, the Inspector General 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.

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 and the advanced levels capture the extent to which agencies institutionalize those policies and procedures. Within the maturity model context, agencies should perform risk assessments and identify the optimal maturity levels that achieve cost-effective security based on their missions and risks faced, risk appetites, and risk tolerance levels.

This report summarizes the results of our evaluation of the Department's information security program based on the FY 2020 FISMA Reporting Metrics,[11] which align with five functions from the NIST Cybersecurity Framework.[12] The NIST Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise, as shown in Table 1.

[11] The results of our FY 2020 FISMA evaluation exclude the United States Coast Guard. In May 2020, the Department allowed the Coast Guard to meet FISMA requirements according to Department of Defense (DoD) reporting requirements, rather than DHS reporting requirements.
[12] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018.

Table 1. NIST Cybersecurity Functions and FISMA Domains

Cybersecurity Functions		FISMA Domains
Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	**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 2020 FISMA Reporting Metrics

According to the FY 2020 FISMA Reporting Metrics, OIGs are well positioned to assess agency information security programs, given their audit responsibilities and awareness of each agency's unique mission, cybersecurity challenges, and resources to address those challenges. Each OIG 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 within the NIST Cybersecurity Framework. Based on its evaluation, OIG assigns each of the agency's cybersecurity functions a maturity level of 1 through 5. Table 2 describes each maturity level.

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 2020 FISMA Reporting Metrics

Per the FY 2020 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.[13] Agencies should perform risk assessments on an ongoing basis (either as part of security authorization or continuous monitoring processes) to identify their information system maturity levels, based on cost-effectiveness, mission, and risk tolerance. Further, each OIG should apply a rating across the eight domains based on a simple majority. 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

We conducted an independent evaluation of the DHS information security program and practices based on the maturity model approach outlined in the FY 2020 FISMA Reporting Metrics and the NIST Cybersecurity Framework. We performed our fieldwork at the DHS Office of the CISO and at Cybersecurity and Infrastructure Security Agency (CISA), DHS Headquarters (HQ), U.S. Immigration and Customs Enforcement (ICE), Science and Technology Directorate (S&T), Transportation Security Administration (TSA), and United States Secret Service. 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. DHS defines

[13] *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics,* Version 4.0, April 17, 2020.

NSS as systems that collect, generate, process, store, display, transmit, or receive Unclassified, Confidential, Secret, and Top-Secret information.

As part of our review, we performed testing on four selected systems at U.S. Customs and Border Protection (CBP),[14] CISA, DHS HQ's Countering Weapons of Mass Destruction Office, and ICE, for compliance with applicable Defense Information Systems Agency (DISA) *Security Technical Implementation Guides* settings.[15] Specifically, we tested selected Windows 10 workstations, and we tested the effectiveness of controls implemented on selected databases and servers. We responded to the questions cited in the FY 2020 FISMA Reporting Metrics based on our evaluation of DHS' compliance with applicable FISMA requirements. Our responses were also based on our fieldwork performed at the DHS Office of the CISO, testing at CBP, CISA, DHS HQ, and ICE, and review of monthly FISMA Scorecards for unclassified systems and NSS.

To determine the effectiveness of components' implementation of their information security programs, our independent contractor performed work at S&T, TSA, and Secret Service. The contractor evaluated the components' procedures for identifying and managing cybersecurity risks based on applicable OMB and NIST guidance and the maturity approach outlined in the FY 2020 FISMA Reporting Metrics. We have incorporated the contractor's work as a part of our FY 2020 submission to OMB and into this report.

Results of Evaluation

In May 2020, the Department formally documented its risk acceptance to allow the Coast Guard to meet FISMA requirements according to Department of Defense (DoD), rather than DHS, reporting requirements. Therefore, when evaluating the overall effectiveness of DHS' information security program for FY 2020 FISMA, our rating does not include the Coast Guard. Also, our rating of DHS' program is contingent on the Department's completion of its corrective actions to our prior recommendations,[16] such as revising its information security policies and procedures to reflect senior leadership's approval of Coast Guard's FISMA reporting to the DoD and communicating the decision, in writing, to OMB and selected congressional oversight committees.
DHS' information security program earned an overall rating of effective, with a maturity rating of "Managed and Measurable" (Level 4) in three of five functions. Specifically, we identified:

[14] We included testing results from another FY 2020 OIG audit, which included vulnerability patch and configuration management assessments of selected Windows 10 workstations.
[15] DISA issues *Security Technical Implementation Guides* for Government agencies to implement for their computer systems to "harden" security settings.
[16] *Evaluation of DHS' Information Security Program for Fiscal Year 2019*, OIG-20-77, September 30, 2020.

- systems operating without authority to operate;
- known information security weaknesses not promptly mitigated;
- security configuration settings not implemented for all systems; and
- an unsupported operating system and not applying security patches promptly.

DHS Can Further Improve the Management of Its Information Security Program

DHS' information security program earned an overall rating of effective, with a maturity rating of "Managed and Measurable" (Level 4) in three of five functions. FY 2019 and FY 2020 ratings are summarized in Table 3.

Table 3. DHS' Maturity Level for Each Cybersecurity Function in FY 2019 Compared to FY 2020

Cybersecurity Function	Maturity Level	
	FY 2019	FY 2020
1. Identify	Level 1 – Ad Hoc	Level 4 – Managed and Measurable
2. Protect	Level 4 – Managed and Measurable	Level 4 – Managed and Measurable
3. Detect	Level 1 – Ad Hoc	Level 4 – Managed and Measurable
4. Respond	Level 1 – Ad Hoc	Level 3 – Consistently Implemented
5. Recover	Level 3 – Consistently Implemented	Level 1 – Ad Hoc

Source: DHS OIG analysis based on our FY 2019 report[17] and FY 2020 FISMA Reporting Metrics

Coast Guard's FISMA Reporting

We reported in September 2020[18] that, on June 11, 2019, the former DHS CIO[19] permitted the Coast Guard to change its cybersecurity reporting structure, allowing the Coast Guard to submit its cybersecurity and FISMA reports directly to DoD, while providing an information copy to DHS.[20] According to the former DHS CIO, he was not required to consult with the Deputy Under Secretary for Management due to a delegation of authority,

[17] *Id.*
[18] *Evaluation of DHS' Information Security Program for Fiscal Year 2019*, OIG-20-77, September 30, 2020.
[19] The DHS CIO departed from DHS on November 15, 2019.
[20] As one of the five Armed Services of the United States, the Coast Guard is the only military branch within DHS. The Coast Guard operates under DHS during peacetime, and can be transferred to the Department of the Navy within DoD by the President at any time, or by the U.S. Congress during times of war. Congressional authority transfers happened twice: in 1917, during World War I, and in 1941, during World War II.

per 44 United States Code (U.S.C.) § 3554(a)(3) and Delegation 04000, which gives the DHS CIO authority to implement FISMA responsibilities for the Department. As a result, unlike other DHS components, the Coast Guard does not:

1. provide to DHS for inclusion in its monthly information scorecard all required FISMA security metric data, such as information systems inventory, weakness remediation, security authorization, vulnerability management, security incident reports, and data feed; and

2. participate (by providing data) in DHS' Continuous Diagnostics and Mitigation Program, which is designed to increase visibility of department-wide cybersecurity vulnerabilities.

According to the former DHS CIO, his decision to allow the Coast Guard to no longer provide security metric data to DHS and to not participate in the Continuous Diagnostics and Mitigation Program was because:

- the Coast Guard uses or operates networks that are connected to, or operating under, DoD Information Networks to support its mission; and
- the DoD continuous monitoring tools that the Coast Guard uses, including reports the tools produce, are incompatible with DHS' continuous monitoring tools.

In a May 28, 2020 memorandum to the Acting Secretary, the Deputy Under Secretary for Management documented the Department's "risk acceptance that the Coast Guard will manage and defend its information systems under the direction" of DoD. According to the memorandum, the DHS CIO and the Coast Guard CIO agreed to this shift in responsibilities on June 7, 2019. This agreement, which DHS believed did not cause additional cybersecurity risks to the Department:

- allowed the Coast Guard to meet FISMA requirements through and in accordance with DoD architecture, implementation standards, and reporting requirements; and
- eliminated the need for the Coast Guard to use the civilian-focused Continuous Diagnostics and Mitigation in favor of DoD requirements.

Therefore, we excluded the Coast Guard when evaluating the overall effectiveness of DHS' information security program for FISMA, under the Council of the Inspectors General on Integrity and Efficiency's annual Inspector General reporting metrics that are based on NIST's Cybersecurity Framework. Our FY 2020 rating for the Department is also contingent on DHS' completion of its corrective actions to our prior recommendations, such as

revising its information security policies and procedures to reflect senior leadership's approval of the Coast Guard's FISMA reporting to DoD and communicating the decision, in writing, to OMB and selected congressional oversight committees.

DHS' FY 2020 FISMA Ratings

The following is a complete discussion of all progress and deficiencies we identified in each cybersecurity function we evaluated, based on the maturity model approach in the FY 2020 FISMA Reporting Metrics and the NIST Cybersecurity Framework.

1. Identify

The "Identify" function requires developing an organizational understanding to manage cybersecurity risks to systems, assets, data, and capabilities. Per the FY 2020 FISMA Reporting Metrics, we determined that DHS was operating at "Level 4 – Managed and Measurable" in this function. We based this rating on our conclusion that DHS was managing identified cybersecurity risks through its systems security authorization process.

DHS can further improve in this function. For example, DHS needs to strengthen its oversight of the components' risk management, as more component systems are operating with expired ATOs. Without renewed and 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. 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]

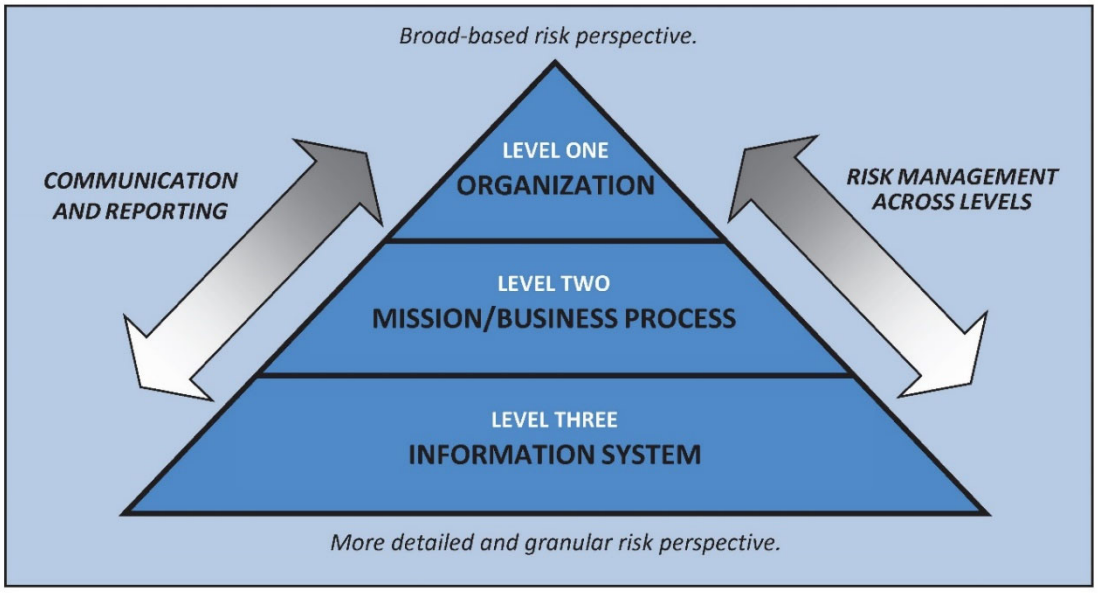
Risk Management

Managing risk is a complex, multifaceted activity that requires involvement of the entire organization — from senior leaders and executives providing the strategic vision and top-level goals and objectives for the organization to mid-level managers planning, executing, and managing projects and individual

[21] OMB Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001.

users operating information systems supporting the organization's missions and business functions. Risk management requires that organizations: (1) establish the framework for risk-based decisions; (2) assess risk; (3) respond to risk once determined; and (4) monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations. Therefore, risk management affects every aspect of the organization, including mission and business planning activities, the enterprise architecture, system development processes, and systems engineering activities integral to system life cycle management processes. Figure 1 illustrates a multi-level approach to risk management that addresses communication and reporting of security and privacy risk at the organization level, the mission/business process level, and the information system level.

Figure 1. Organization-Wide Risk Management Approach



Source: NIST Special Publication (SP) 800-37, Revision 2, December 2018

Risk management also encompasses the authorization process by which a senior management official (i.e., the authorizing official) reviews security and privacy information describing the current security and privacy posture of information systems.[22] The authorizing official uses this information to determine whether the mission/business risk of operating a system is acceptable and, if it is, explicitly accepts the risk by granting the system ATO. According to applicable DHS, OMB, and NIST policies, all systems must undergo the authorization process before they become operational.

[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.

Per DHS guidance,[23] DHS components are required to use enterprise management systems that incorporate NIST security controls when performing security assessments of their systems. Enterprise management systems enable centralized storage and tracking of all documentation required for the authorization package of each system. The security authorization package (also referred to as an ATO package) documents the results of the security control assessment and provides the authorizing official with essential information needed to make a risk-based decision whether to authorize operation of the information system. Seven artifacts must be included in the ATO package:

1. Privacy threshold analysis and, if required, privacy impact assessment
2. Security plan
3. Contingency plan
4. Security assessment plan
5. Contingency plan test
6. Security assessment report
7. Authorization decision letter

Based on OMB and NIST guidance,[24] system ATOs are typically granted for a specific period, in accordance with terms and conditions established by the authorizing official. However, in October 2013, DHS began allowing its components to enroll in an ongoing authorization program established by NIST. For each system to be admitted to the ongoing authorization program, a component must have approved common controls, a designated ongoing authorization manager, and a chartered organizational risk management board. In addition, DHS requires components to maintain security authorization and weakness remediation metrics above 95 and 90 percent, respectively, on the monthly FISMA Scorecard. After a component is accepted to the ongoing authorization program, system owners must fulfill the following requirements for each individual system:

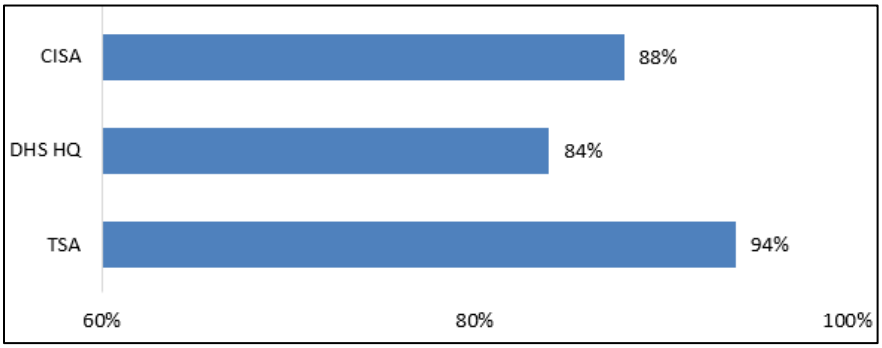
- ensure the component's enrollment in the ongoing authorization program is documented in the component's acceptance letter;
- submit an admission letter to enroll the system in the ongoing authorization program;
- receive an ongoing authorization recommendation letter from the Department to enroll the system in the ongoing authorization program;

[23] DHS *FY20 Information Security Performance Plan*, Version 1.2, December 20, 2019.
[24] 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.

- ensure the system's ATO does not expire for at least 60 days when applying to enter the program;
- assign the information system security officer with responsibilities primarily related to information assurance/security;
- provide the information system security officer with training about ongoing authorization processes; and
- maintain an approved control allocation table listing the system security controls the component agrees to implement.

DHS maintains a target goal of ensuring ATOs for 100 percent of its 138 high-value systems assets. The ATO target goal is 95 percent for its 406 operational non-high value assets. However, our independent review of DHS' August 2020 FISMA Scorecard for unclassified systems revealed that three components did not meet the required authorization target of 100 percent for high-value assets, as shown in Figure 2.

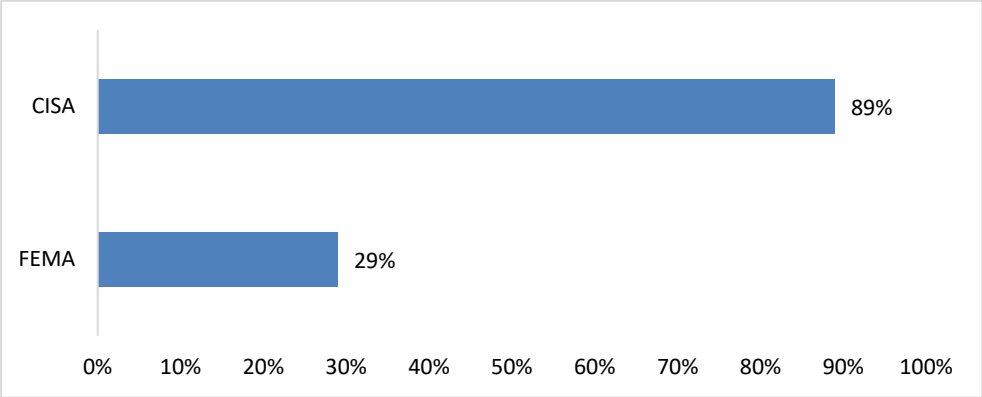
Figure 2. Selected Components' Performance in Meeting the ATO Goal for High-Value Systems Assets



Source: DHS OIG analysis of DHS' August 2020 FISMA Scorecard

In addition, according to DHS' August 2020 FISMA Scorecard, 2 (CISA and the Federal Emergency Management Agency (FEMA)) 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 3.

Figure 3. Selected Components' Performance in Meeting the ATO Goal for Non-High Value Systems Assets



Source: DHS OIG analysis of DHS' August 2020 FISMA Scorecard

To determine the components' compliance in meeting DHS' NSS security authorization target, we examined the Department's August 2020 NSS Scorecard. We found that one component (S&T) did not meet the ATO target of 95 percent for its NSS, compared to FY 2019 when all components met DHS' NSS ATO target.

The total number of unclassified systems operating without ATOs more than tripled when compared to FY 2018, even when DHS CIO did not include any Coast Guard security information in FY 2020 monthly scorecards.[25] Our analysis of June 30, 2020 data from DHS' unclassified enterprise management system revealed 75 of 536 systems across DHS did not have current ATOs. Table 4 outlines the number of unclassified systems operating without ATOs at selected components from FY 2018 to FY 2020.

[25] *Evaluation of DHS' Information Security Program for Fiscal Year 2018*, OIG-19-60, September 19, 2019; *Evaluation of DHS' Information Security Program for Fiscal Year 2019*, OIG-20-77, September 30, 2020.

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

Component	FY 2018	FY 2019	FY 2020
A	3	5	2
B	6	21	N/A
C	1	0	0
D	3	6	10
E	5	44	61
F	2	2	1
G	2	2	1
H	2	0	0
I	0	0	0
J	0	1	0
Total	**24**	**81**	**75**

Source: Evaluation of DHS' Information Security Program for Fiscal Year 2018, OIG 19-60, September 19, 2019; *Evaluation of DHS' Information Security Program for Fiscal Year 2019*, OIG-20-77, September 30, 2020.

Weakness Remediation

FISMA requires the use of 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.[26]

We found several components did not effectively manage the POA&M process as required by DHS. For example, although DHS requires components to update POA&Ms monthly, not all components consistently maintained complete and accurate information on progress in remediating security weaknesses. They also did not resolve all POA&Ms within 12 months as required, or consistently include estimates for resources needed to mitigate identified weaknesses. Our analysis of data from DHS' enterprise management system as of June 30, 2020, showed the following deficiencies:

- Of the 12,515 open unclassified POA&Ms, 2,343 (19 percent) were past due.
- Of the 2,343 past due unclassified POA&Ms, 463 (20 percent) were overdue by more than a year.

[26] OMB Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001.

- Of the 2,343 past due unclassified POA&Ms, 1,256 (54 percent) had weakness remediation costs estimated at less than $50. 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.

Our analysis of the August 2020 NSS FISMA Cybersecurity Scorecard revealed DHS HQ did not meet DHS' NSS weakness remediation metrics for POA&Ms.

According to FY 2020 FISMA Reporting Metrics, our independent contractor rated components' Identify function at "Level 4 - Managed and Measurable" for S&T and Secret Service, and "Level 5 – Optimized" for TSA.

2. Protect

The "Protect" function entails developing and implementing the appropriate safeguards to ensure delivery of critical services. It includes four FISMA domains: (1) Configuration Management, (2) Identity and Access Management, (3) Data Protection and Privacy, and (4) Security Training. We determined that, based the FY 2020 FISMA Reporting Metrics, DHS was operating at "Level 4 – Managed and Measurable." For example, DHS has implemented an enterprise-wide single sign-on solution and all the organization's systems interface with the solution.

However, we determined that DHS has not developed a DHS Cybersecurity Workforce Strategy to address gaps and requirements for planned actions identified in the FY 2017 Cybersecurity Workforce Assessment. Also, the Department did not provide documentation to support that it measures the effectiveness of its specialized security training program.

In addition, some components we reviewed did not replace or update an unsupported operating system on three servers and did not apply security patches and updates timely to mitigate critical and high-risk security vulnerabilities on selected systems. Components also did not always implement all configuration settings required to protect their systems. DHS should focus on improving these key configuration management activities to ensure components are replacing unsupported operating systems and implementing security patches in a timely manner.

Configuration Management

We determined DHS was operating at "Level 3 – Consistently Implemented" in the Configuration Management Domain. DHS requires components to

configure their Windows 10 workstations according to configuration settings set forth in DISA's *Security Technical Implementation Guides*. These settings are necessary to ensure confidentiality, integrity, and availability of DHS' systems and the information they process and store. To outline risk to information, DISA ranks each setting/control in the *Security Technical Implementation Guides* as either Category I, II, or III. For example, if a Category I control is not implemented or subverted, the risk to information is direct and immediate loss of confidentiality, integrity, or availability.

Our testing revealed that not all components we reviewed had implemented all required configuration settings. Specifically, we tested selected unclassified assets, including 675 workstations and 53 servers at selected components, for compliance with the required DISA *Security Technical Implementation Guides* Category I, II, and III settings. Table 5 summarizes the components' compliance.

Table 5. Selected Component Systems' Compliance with DISA's Security Technical Implementation Guides Categories I, II and III Settings

Component	Percentage of Compliance
A	70%
C	70%
D	93%
G	57%

Source: DHS OIG-compiled based on test results for four components

The missing settings on the workstations and servers we tested related to configuration of encryption algorithms, operating systems, and network communication. When these settings are not applied, unauthorized users can potentially access or exploit sensitive information. We found missing settings related to:

- Secure Boot – a security feature to ensure that Windows operating system is only using trusted software or drivers. When Secure Boot is turned off, there is an increased risk of software, malware, or drivers from untrusted sources being loaded into the operating system during system startup.
- Account Lockout Events not captured in audit logs on selected Windows servers – audit logs provide a trail of evidence in case a system or network is compromised and collecting audit logs is essential for detecting suspicious activities. Capturing account lockout events can be used to identify potentially malicious logon attempts.

- Data Execution Prevention – misconfiguration of this setting may allow harmful code to run in protected memory locations reserved for Windows and other programs.

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 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. DHS requires components to discontinue use of unsupported operating systems. However, we identified an unsupported version of an operating system, for which the manufacturer stopped providing technical support in January 2020, on three servers.

Vulnerability Assessment Testing

Periodic scanning and assessment of critical systems is key to mitigating information security vulnerabilities. Per DHS guidance, components must reduce system vulnerabilities through testing, prompt installation of software patches, and elimination or disabling of unnecessary services. We performed independent vulnerability assessments on selected workstations and servers at selected components. Table 6 summarizes the missing critical and high-risk software patches we identified.

Table 6. Software Patching Vulnerabilities Identified for Selected Operating Systems at Selected Components

Operating System	Component	Unique Critical Vulnerabilities	Unique High Vulnerabilities
Windows 10 Workstations	A	1	2
Windows 2016 Servers	A	0	1
Windows 10 Workstations	C	6	27
Windows 10 Workstations	D	4	39
Windows 2008 Servers	G	3	4
Windows 10 Workstations	G	3	7
Windows 2012 Servers	G	4	6
Windows 2016 Servers	G	5	6

Source: DHS OIG-compiled based on system test results

The following are examples of the critical and high-risk vulnerabilities we detected on the systems tested:

1. A security update for an anti-virus software was missing on 4 out of 13 (31 percent) Windows 2016 servers tested at Component G. As of September 2020, the four servers had outdated versions of the anti-virus software database.
2. Workstations at all components we tested did not have security software patches for Adobe products and a Microsoft Windows Defender patch. Failure to install these patches could allow an attacker who successfully exploited this vulnerability to elevate privileges on the system, and a remote attacker could exploit the systems to execute arbitrary code within the context of the user. Specifically, 281 (99 percent) of 283 workstations tested at Component D were missing current Adobe Acrobat security patches, which made these workstations vulnerable to multiple attacks.

If successfully exploited, these vulnerabilities could result in significant data loss or system disruption. Successful exploitation of critical and high-risk vulnerabilities may take the form of remote code execution, unauthorized modification or disclosure of information, or possible escalation of access rights and privileges. Ultimately, such exploitation could pose substantial risks to components' ability to carry out mission-critical DHS operations.

According to FY 2020 FISMA Reporting Metrics, our independent contractor rated components' Configuration Management Domain at "Level 3 - Consistently Implemented" for S&T, and "Level 4 - Managed and Measurable" for Secret Service and TSA.

Identity and Access Management

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 (PIV) cards for access, pursuant to Homeland Security Presidential Directive-12.[27] DHS requires all privileged and unprivileged employees and contractors to use the PIV cards to log onto DHS systems.

DHS did not provide documentation to support that its identity, credential, and access management program was properly resourced as required by FY 2020

[27] *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.

FISMA reporting metrics. DHS also did not have automatic mechanisms to manage its systems' user accounts.

According to FY 2020 FISMA Reporting Metrics, our independent contractor rated components' Identity and Access Management Domain at "Level 1 – Ad-Hoc" for S&T, "Level 2 – Defined" for Secret Service, and "Level 5 – Optimized" for TSA.

Data Protection and Privacy

DHS developed a data privacy policy in 2011 to protect personally identifiable information stored and processed by its information systems. The DHS Privacy Office is responsible for privacy compliance across the Department, including ensuring the technologies used sustain and do not erode privacy protections for personal and departmental information. However, we reported in November 2020 that the DHS Privacy Office had not effectively monitored the completion of annual privacy training.[28] Specifically, more than 50 percent of DHS HQ staff did not complete the training in 2019. Across all components, including DHS HQ, 12 percent of employees did not complete the annual privacy training.

Per the FY 2020 FISMA Reporting Metrics, DHS did not have qualitative and quantitative measures in place to gauge the performance of its network defenses against unauthorized transfer of information from a system, known as data exfiltration. DHS did not conduct regular exfiltration exercises to measure the effectiveness of its data exfiltration or enhanced network defenses, as required by applicable NIST guidance. In addition, the Department did not provide documentation that it uses qualitative and quantitative performance measures to monitor and analyze the effectiveness of its Data Breach Response Plan.

According to FY 2020 FISMA Reporting Metrics, our independent contractor rated components' Data Protection and Privacy Domain at "Level 3 - Consistently Implemented" for S&T and Secret Service, and "Level 5 – Optimized" for TSA.

Security Training Program

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

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

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.

However, DHS did not provide documentation to support that its security awareness and training program was properly resourced per the FY 2020 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 Assessment. 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;
- establishing qualitative and quantitative measures to monitor data exfiltration or enhanced network defenses; and
- finalizing a strategy to address identified gaps outlined in its Cybersecurity Workforce Assessment.

According to FY 2020 FISMA Reporting Metrics, our independent contractor rated components' Security Training Domain at "Level 1 - Ad-hoc" for S&T and Secret Service, and "Level 5 – Optimized" for TSA.

3. Detect

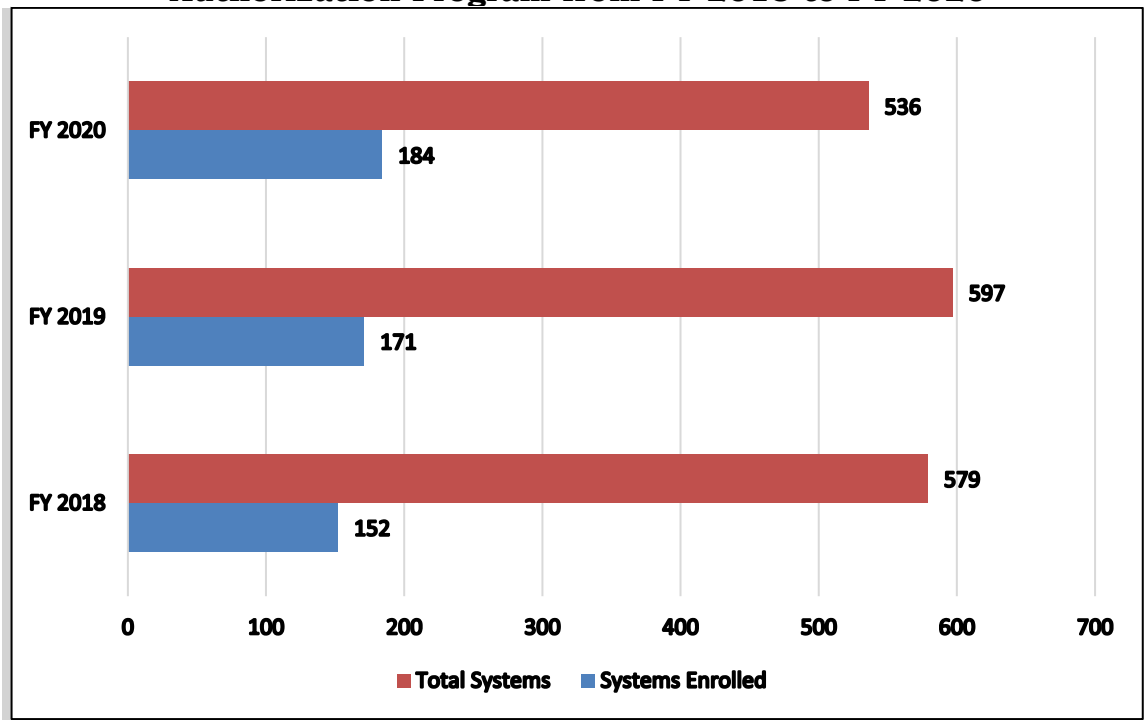
The "Detect" function entails developing and implementing appropriate activities, including ongoing systems authorization and continuous monitoring, to identify any irregular system activity. Per the FY 2020 FISMA Reporting Metrics, we determined that DHS was operating at "Level 4 – Managed and Measurable" in this function. We based this rating on our conclusion that DHS monitors and analyzes performance measures on the effectiveness of its ISCM strategy and makes updates as appropriate.

However, the Department did not provide documentation to support that it had integrated metrics on the effectiveness of the ISCM program to deliver continuous situational awareness across the organization. DHS also did not establish an ongoing authorization program for its NSS.

According to NIST, an effective ISCM program should begin with developing a comprehensive strategy that addresses 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. However, DHS 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 June 2020, eight components were enrolled in the Department's ongoing authorization program. The Department had increased the number of systems enrolled in the program from FY 2018 to FY 2020, as shown in Figure 4.

Figure 4. DHS Systems Enrolled in the Ongoing Authorization Program from FY 2018 to FY 2020

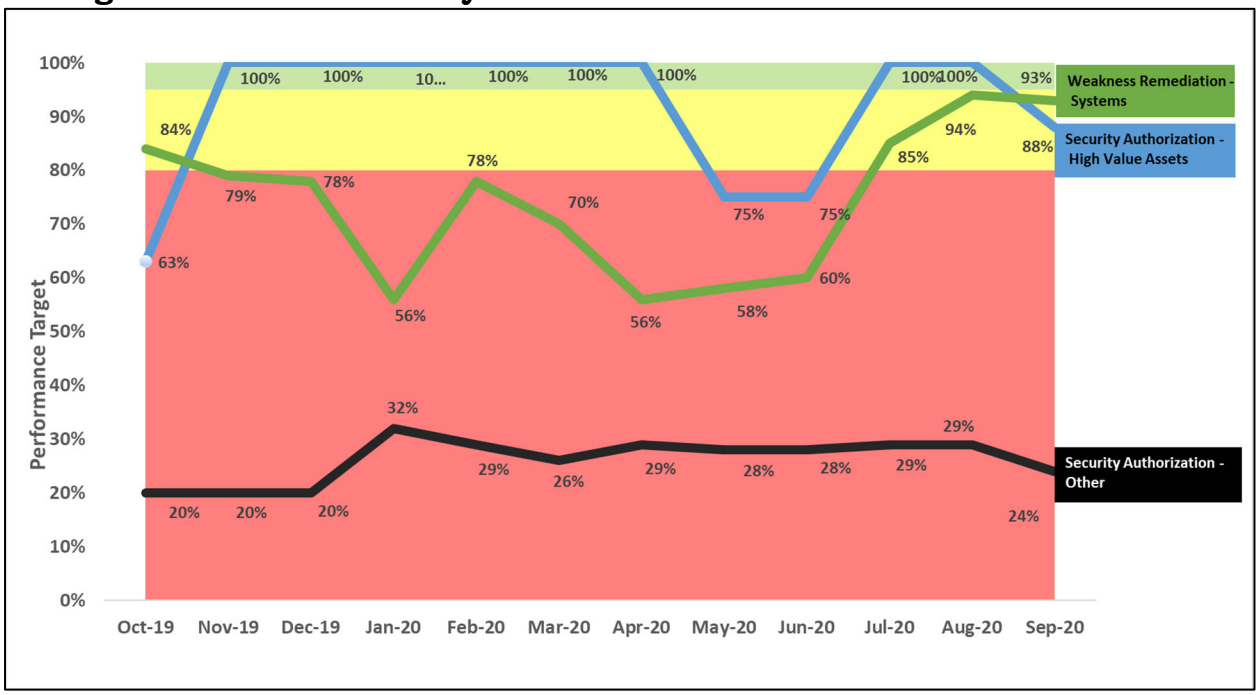


Source: DHS OIG-compiled based on DHS Office of the CISO data

However, not all components sustained their information security programs on a year-round, continuous basis by maintaining Security Authorization and

POA&M remediation status. For example, our review of the Department's monthly FISMA Scorecards revealed that FEMA did not always maintain its information security programs on a year-round, continuous basis or consistently achieve the Department's Security Authorization and POA&M (i.e., weakness remediation) performance metrics from October 2019 to September 2020. Figure 5 depicts FEMA's overall score for all three metrics (i.e., Security Authorization – High Value Assets, Security Authorization – Other, and Weakness Remediation – Systems), which peaked during the months of components' annual FISMA reporting (around July–August) and subsequently dropped.

Figure 5. FEMA Security Authorization and Weakness Remediation



Source: DHS OIG-compiled based on available DHS monthly information security scorecards

We identified a similar issue in 2009[29] and 2015.[30] This trend is an indication that FEMA is not complying with requirements to update and maintain its information security program and systems' Security Authorizations and POA&M documentation on a continuous basis. It also indicates that the Department's oversight of components' information security programs needs strengthening. Specifically, FEMA could not achieve better than 32 percent in

[29] *Evaluation of DHS' Information Security Program for Fiscal Year 2009*, OIG-09-109, September 2009.
[30] *Evaluation of DHS' Information Security Program for Fiscal Year 2015*, OIG-16-08, November 13, 2015.

the "Security Authorization – Other" metric from October 2019 to September 2020.

According to FY 2020 FISMA Reporting Metrics, our independent contractor rated components' Detect function at "Level 4 - Managed and Measurable" for S&T and Secret Service, and "Level 5 – Optimized" for TSA.

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 provide evidence to support that the Department (1) has qualitative and quantitative performance measures to assess the effectiveness of its incident response policies and procedures, (2) applies profiling techniques to measure the characteristics of expected activities on its networks, and (3) uses profiling techniques to measure the characteristics of expected activities on its networks and systems.

Incident Response

In FY 2020, DHS reported two major incidents. According to applicable FISMA major incident reporting requirements, the Department notified selected congressional oversight committees of the following:

(1) February 25, 2020: FEMA potentially shared more disaster survivors' personally identifiable information than required with two of its vendors to execute their service contracts.[31] In December 2019, according to FEMA, 6.8 million disaster survivors' personally identifiable information was discovered on one vendor's systems. FEMA did not comply with applicable cyber security policies to allow the vendors to transmit and store FEMA data on non-FEMA information technology systems between 2007 and 2020. In addition, since about 2007, a third vendor received information from FEMA without all the appropriate cyber security safeguards.

(2) March 25, 2020: For a contract awarded in June 2018, a FEMA vendor did not provide adequate user access controls to a system containing

[31] On November 9, 2018, OIG issued a draft management alert to notify FEMA about the incident. Subsequently, OIG issued the final management alert, *Management Alert – FEMA Did Not Safeguard Disaster Survivors' Sensitive Personally Identifiable Information (REDACTED),* (OIG-19-32), on March 15, 2019. Following the release of this management alert, FEMA identified two additional major incidents in 2019.

personally identifiable information of approximately 2.5 million individuals who had contacted FEMA requesting changes in flood maps.

According to FY 2020 FISMA Reporting Metrics, our independent contractor rated components' Respond function at "Level 1 - Ad-hoc" for S&T and Secret Service, and "Level 4 - Managed and Measurable" for TSA.

5. Recover

DHS' approximately 240,000 employees rely heavily on information technology to perform their duties. Because information systems and resources are so vital to DHS' accomplishment of its mission operations, it is critical to minimize the effect of service interruptions and avoid extensive outages in the event of an emergency. 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 1 – Ad Hoc." DHS did not achieve "Level 2 – Defined" because there was no delegation of authority as the Department's Information System Contingency Planning Manager position was vacant in FY 2020.

DHS defined its policies, procedures, and strategies for information contingency planning. However, as of June 2020, 29 unclassified systems and 2 NSS contingency plans had not been tested. Further, DHS did not provide documentation to support that (1) the Department had integrated metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans; and (2) information system contingency plan testing and exercises are consistently implemented, and information system contingency plan testing and exercises are integrated, to the extent practicable, with testing of related plans, such as incident response plan/Continuity of Operations Planning/Business Continuity Planning.

Contingency Planning

DHS has a department-wide business continuity program to react 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. However, as of June 30, 2020, we identified the following deficiencies:

- Our review of the June 2020 NSS Scorecard revealed that DHS HQ did not meet DHS' NSS compliance target for contingency plan testing.
- CISA, DHS HQ, and FEMA had not tested contingency plans for 29 of 536 unclassified systems, based on our analysis data from DHS' enterprise management system as of June 30, 2020.

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.

According to FY 2020 FISMA Reporting Metrics, our independent contractor rated components' "Recover" function at "Level 3 - Consistently Implemented" for S&T and TSA, and "Level 2 – Defined" for Secret Service.

Summary of Selected Components' Implementation of Information Security Programs

According to FY 2020 FISMA Reporting Metrics, our independent contractor rated component information security programs effective for TSA by achieving "Level 4 – Managed and Measurable" or higher in four of the five functions. S&T's and Secret Service's overall information security programs were not effective because they were rated below "Level 4 – Managed and Measurable" in three of five functions. Because the Department performs several security functions on S&T's and Secret Service's behalf, these components have not yet developed component-specific policies, procedures, and business processes, as required by DHS policy. Table 7 summarizes the implementation of information security programs by S&T, TSA, and Secret Service.

Table 7. Summary Status of S&T, TSA, and Secret Service Information Security Programs for FY 2020

Function / Component	S&T	TSA	Secret Service
Identify	Level 4 - Managed and Measurable	Level 5 - Optimized	Level 4 - Managed and Measurable
Protect	Level 1 - Ad-hoc	Level 5 - Optimized	Level 3 - Consistently Implemented
Detect	Level 4 - Managed and Measurable	Level 5 - Optimized	Level 4 - Managed and Measurable
Respond	Level 1 - Ad-hoc	Level 4 - Managed and Measurable	Level 1 - Ad-hoc
Recover	Level 3 - Consistently Implemented	Level 3 - Consistently Implemented	Level 2 - Defined
Overall Rating	**Ineffective**	**Effective**	**Ineffective**

Source: DHS OIG contractor

Since 2019, our independent contractor has performed fieldwork at six selected components and rated three components' information security programs as "ineffective" because the components achieved below "Level 4 – Managed and Measurable" in three of five functions, under the FY 2020 FISMA Reporting Metrics.

Recommendations

Recommendation #1: We recommend the DHS Chief Information Officer enforce requirements for components to obtain authority to operate and resolve critical and high-risk vulnerabilities, implement required configuration settings, and apply sufficient resources to mitigate security weaknesses for both their unclassified systems and national security systems.

Recommendation #2: We recommend S&T Chief Information Officer strengthen the component's information security program by establishing necessary policies and procedures according to the NIST Cybersecurity Framework.

Recommendation #3: We recommend Secret Service Chief Information Officer strengthen the component's information security program by establishing necessary policies and procedures according to the NIST Cybersecurity Framework.

Recommendation #4: We recommend FEMA Chief Information Officer strengthen the component's oversight to sustain its information security program on a year-round, continuous basis and maintain Security Authorization and Plan of Action and Milestones remediation status current.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Department. In its comments, the Department stated it appreciates the work of OIG in planning and conducting its review and issuing this report.

We have reviewed the Department's comments, as well as the technical comments previously submitted under separate cover and updated the report as appropriate. The following is our evaluation of the Department's general comments, as well as a response to each recommendation in the draft report provided for Department review and comment.

OIG Response to General Comments:

The Department stated that "by statute, the authority to accept cybersecurity risk for the Department resides solely with the DHS CIO." This assertion is inconsistent with FISMA requirements, as agency heads are ultimately responsible for ensuring that their respective agencies maintain protections commensurate with the risk of harm of a compromise.[32] Each agency's 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.[33] Agency heads must maintain awareness of their agency's information security programs and direct CIOs and CISOs to implement appropriate security measures and, where necessary, take remedial actions to address known vulnerabilities and threats. Further, in an effort to verify the agency head's awareness and to validate the agency's FISMA report, OMB requires a signed letter from agency heads to the OMB Director as part of their annual reporting package to OMB.[34]

With regard to the statement that "DHS leadership is perplexed with OIG's statement in the draft report that the FY 2020 rating of DHS's program is 'contingent' on the Department's completion of corrective actions to prior recommendations…" We maintain this arrangement was intended to give the

[32] 44 U.S.C. § 3554(a)(1)(A).
[33] *Id.* at § 3554(a)(5).
[34] OMB M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*, dated November 9, 2020.

Department time to pursue completion of agreed-upon corrective actions issued in our FY 2019 FISMA report.[35] This includes taking steps to revise information security policy and procedures and communicating senior leadership's approval of Coast Guard FISMA reporting to DoD in writing to OMB and selected congressional oversight committees. Although the Department concurred with and agreed to implement these two corrective actions, the Department has yet to provide documentation to support that all corrective actions have been completed or met the estimated scheduled completion date.

Response to Report Recommendations:

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

DHS Comments to Recommendation #1: Concur. The Department stated that the DHS CIO holds monthly meetings with component CIOs to discuss remedial actions and resolve impediments to improving components' information security program metrics. DHS CIO will continue to work with component CIOs in this forum to develop additional strategies for compliance with planned remedial actions addressing areas such as security authorization and weakness remediation. In addition, DHS CIO will work with component CIOs to reduce high-risk vulnerabilities, ensure prompt installation of software patches, and eliminate unnecessary services for unclassified and national security systems. Estimated Completion Date (ECD): June 30, 2022.

OIG Analysis of DHS Comments

DHS' actions are responsive to this recommendation. This recommendation will remain open and resolved until DHS provides documentation to support that all planned corrective actions are completed.

DHS Comments to Recommendation #2: Concur. The Department stated that the S&T CIO recognizes the value of the NIST Cybersecurity Framework in helping to strengthen the cybersecurity program. As such, the S&T CIO is in the process of establishing the recommended policies and procedures. Further, the S&T CIO is working to add three other policies from the NIST Cybersecurity Framework to enhance and support the S&T Cybersecurity efforts. Specifically: (1) S&T 1 ID.RM-001, *Information Security Policy*, (2) S&T 1 ID.RM-002, *Information Security Risk Management Policy*, and (3) S&T 1 ID.RM-003, *Risk Assessment Policy*. ECD: September 30, 2021.

[35] *Evaluation of DHS' Information Security Program for Fiscal Year 2019,* (OIG-20-77, September 30, 2020). Recommendations 2 and 4 remain open and unresolved.

OIG Analysis of DHS Comments

S&T's actions are responsive to this recommendation. This recommendation will remain open and resolved until S&T provides documentation to support that all planned corrective actions are completed.

DHS Comments to Recommendation #3: Concur. Since the first quarter of FY 2021, the Secret Service's Office of the Chief Information Officer (OCIO) staff have undertaken significant efforts to formally review, update, and create enterprise policies and standard operating procedures and ensure they align to Federal statute and regulation, Department policy, and NIST guidelines, as appropriate. For example, the OCIO has updated 9 of 44 of the OCIO policies. During FY 2022, the OCIO will evaluate the remaining 35 policies and determine which ones should be removed as no longer applicable to the Secret Service's operations, require substantial updates, or require minor updates. The Secret Service's leadership believes that policies and procedures benefit from continuous improvement and is committed to periodically review this guidance, as appropriate. ECD: September 30, 2023.

OIG Analysis of DHS Comments:

The Secret Service's actions are responsive to this recommendation. This recommendation will remain open and resolved until the Secret Service provides documentation to support that all planned corrective actions are completed.

DHS Comments to Recommendation #4: Concur. Throughout the past year, FEMA's OCIO staff took action to improve the information security program, security authorization status for high value assets, non-high value assets, and related POA&Ms remediation efforts. For example, while all FEMA's high value assets currently have an ATO, the FEMA CIO is targeting an ATO goal of 100 percent for all systems by the end of the second quarter of FY 2022. FEMA OCIO's POA&M remediation efforts have also drastically improved the quality of POA&M development and reduced the number of expired POA&Ms. FEMA's goal is to reduce expired POA&MS to zero and maintain a status of green for the Weakness Remediation metric. FEMA is taking the necessary actions to improve its information security program and cybersecurity risk posture for the agency. ECD: March 31, 2022.

OIG Analysis of DHS Comments

FEMA's actions are responsive to this recommendation. This recommendation will remain open and resolved until FEMA provides documentation to support 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 adequately and effectively protect the information and information systems supporting DHS' operations and assets for FY 2020. Our independent evaluation focused on assessing DHS' information security program against requirements outlined in the *FY 2020 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: CISA, DHS HQ, ICE, S&T, 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:

- referenced our FY 2018 and FY 2019 FISMA evaluations as a baseline for the FY 2020 evaluation;
- evaluated policies, procedures, and practices DHS had 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 four components. The specialists tested DHS' compliance with applicable DISA *Security Technical Implementation Guides* on selected Windows 10 workstations. In addition to technical testing

conducted for this evaluation, we also included results from a select OIG audit conducted during the same fiscal year. 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 S&T, TSA, and Secret Service to support our evaluation.

We conducted this review between July and November 2020 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

September 2, 2021

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: 2021.09.02 10:07:50 -04'00'

SUBJECT: Management Response to Draft Report: "Evaluation of DHS' Information Security Program for Fiscal Year 2020" (Project No. 20-045-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.

Department leadership is pleased that DHS OIG's fiscal year (FY) 2020 Federal Information Security Modernization Act (FISMA) review did not include the United States Coast Guard (Coast Guard), which as the DHS Chief Information Officer (CIO) has repeatedly communicated to the OIG during the last two years is more appropriately reviewed by the Department of Defense (DOD) OIG.[1] Leadership also notes the FY 2020 maturity ratings in the functional areas of "Identify," "Protect," "Detect," and "Respond," improved from the FY 2019 ratings, however, still believes the FY 2019 ratings were misinformed and lower than they should have been because of the DHS-OIG disagreement concerning Coast Guard inclusion in the FY 2019 review.

DHS leadership also adamantly disagrees with OIG's draft report statements that the Deputy Under Secretary for Management (DUSM) in anyway impeded OIG's ability to evaluate the Department's enterprise-wide information program under the FY 2020 reporting metrics. As repeatedly communicated to the OIG, all actions taken by both the DUSM and DHS CIO related to the Coast Guard were completely within their authority. It is also important to note that Coast Guard systems operating on the DOD Information Network do not pose any significant cybersecurity risks to DHS. While Coast Guard cybersecurity is absolutely relevant to the Department, the OIG's concerns clearly do not

[1] On May 20, 2021, the DOD OIG and DHS OIG announced a joint audit of security controls over Coast Guard systems used and operated on the DOD Information Network.

fully consider the measures DHS has in place to provide visibility into and confidence in Coast Guard cybersecurity practices, as appropriate.

For example, the DHS CIO had the necessary ability to receive data and supporting documentation from DOD to perform statutory responsibilities for oversight of Coast Guard systems and capabilities throughout FY 2019 and FY 2020. While this ability was not completely outlined in writing—nor was it required to be—it was functioning. To help allay OIG concerns in this regard, DHS and DOD are currently working to update an already agreed-upon DHS-DOD Memorandum of Agreement with a new Annex that will further clarify respective roles and responsibilities regarding cybersecurity reporting requirements and information sharing between DHS and DOD. The requirements documented in the Annex will formally effectuate prior agreements that allow the Coast Guard to eliminate wasteful duplicative dual reporting while continuing to deliver compliance information to DHS and maintaining readiness and interoperability with DOD.

In addition, DHS leadership is perplexed with OIG's statement in the draft report that the FY 2020 rating of DHS's program is "contingent" on the Department's completion of corrective actions to prior recommendations, such as revising information security policy and procedures to reflect senior leadership's approval of Coast Guard FISMA reporting to DOD and communicating this in writing to the Office of Management and Budget (OMB) and selected congressional oversight committees. First, it is unclear how a point-in-time program rating can be contingent on future actions which may or may not occur, especially considering that two of the five recommendations in OIG's FY 2019 report remain open and unresolved (i.e., in disagreement). Second, it is also important to reiterate that by statute, the authority to accept cybersecurity risk for the Department resides solely with the DHS CIO. As previously discussed with OIG's review team, the CIO acted appropriately to accept risk, and confirmed this decision with OMB, and Federal Chief Information Security Office officials; and no requirement exists to report matters like this to Congress. The CIO provided evidence of this to the OIG during numerous discussions with Department officials, Component program officials, subject matter experts, and others, which also included sharing corroborating documentation.

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 four recommendations with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, sensitivity, 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.

Attachment

Attachment: Management Response to Recommendations Contained in Project No. 20-045-AUD-DHS

OIG recommended that the DHS CIO:

Recommendation 1: Enforce requirements for components to obtain authority to operate and resolve critical and high-risk vulnerabilities, implement required configuration settings, and apply sufficient resources to mitigate security weaknesses for both their unclassified systems and national security systems.

Response: Concur. The DHS CIO holds monthly meetings with component CIOs to discuss remedial actions and resolve impediments to improving Components' information security program metrics. The DHS CIO will continue to work with component CIOs in this forum to develop additional strategies for compliance with planned remedial actions addressing areas such as security authorization and weakness remediation. In addition, the CIO will work with component CIOs to reduce high-risk vulnerabilities, ensure prompt installation of software patches, and eliminate unnecessary services for unclassified and national security systems. Estimated Completion Date (ECD): June 30, 2022.

OIG recommended that the Science and Technology Directorate (S&T) CIO:

Recommendation 2: Strengthen the component's information security program by establishing necessary policies and procedures according to the NIST [National Institute of Standards and Technology] Cybersecurity Framework.

Response: Concur. The S&T CIO recognizes the value of the NIST Cybersecurity Framework in helping to strengthen the cybersecurity program. As such, the CIO is in the process of establishing the recommended policies and procedures. For example, the recently published SAT 1 NCF-001, "S&T Security Awareness and Training Policy," dated May 27, 2021, provides guidance for new and current user groups and identifies the cyber training requirements for all privileged users, including cyclical re-training requirements. In addition, the SAT 4 NCF (RS.CO-2-4)-005, "Incident Response Plan," dated June 1, 2020, addresses a variety of possible incident scenarios and provides an incident response template that will assist the members with protocols and procedures. Furthermore, beyond the documents mentioned above, S&T CIO is working to add three other policies from the NIST Cybersecurity Framework to enhance and support the S&T Cybersecurity efforts, specifically: (1) S&T 1 ID.RM-001, "Information Security Policy," (2) S&T 1 ID.RM-002, "Information Security Risk Management Policy, and (3) S&T 1 ID.RM-003, "Risk Assessment Policy. ECD: September 30, 2021.

4

OIG recommended that the United States Secret Service (USSS) CIO:

Recommendation 3: Strengthen the component's information security program by establishing necessary policies and procedures according to the NIST Cybersecurity Framework.

Response: Concur. Since the first quarter of FY 2021, USSS Office of the Chief Information Officer (OCIO) staff have undertaken significant efforts to formally review, update and create enterprise policies and standard operating procedures and ensure they align to Federal statute and regulation, Department policy, and NIST guidelines, as appropriate. For example, during the third quarter of FY 2021, the USSS OCIO updated six Agency directives including directives governing security authorizations for information systems, vulnerability management, and patch management. From December 2020 through July 2021, the Cyber Security Program also completed 37 standard operating procedures (SOP) corresponding to the first NIST security control in a security control family. These controls, commonly referred to as dash-1 controls, generate requirements for specific policies and procedures that are needed for the effective implementation of the other security controls in the family. The SOPs included but were not limited to policies and procedures for security assessments and authorizations, access control, and incident response. Furthermore, the OCIO has updated 9 of 44 of the Office of the Chief Information Security Officer policies by the way of deletion or rewrite. During FY 2022, the OCIO will evaluate the remaining 35 policies and determine which ones should be removed as no longer applicable to USSS operations, require substantial updates, or require minor updates. USSS leadership believes that policies and procedures benefit from continuous improvement and is committed to periodically review this guidance, as appropriate. ECD: September 30, 2023.

OIG recommended that the Federal Emergency Management Agency (FEMA) CIO:

Recommendation 4: Strengthen the Component's oversight to sustain its information security program on a year-round, continuous basis and maintain Security Authorization and Plan of Action and Milestones remediation status current.

Response: Concur. Throughout the past year, FEMA OCIO staff took action to improve the information security program, security authorization status for High Valued Assets (HVA), Non-HVAs, and related Plan of Action and Milestones (POA&M) remediation efforts. For example, while all FEMA HVAs currently have an Authority to Operate (ATO), FEMA OCIO recently increased the security authorization status for Non-HVAs by 33 percent. In addition, the FEMA CIO is targeting an ATO goal of 100 percent for all systems by the end of the second quarter of FY 2022.

5

The FEMA OCIO's POA&M remediation efforts have also drastically improved the quality of POA&M development and reduced the number of expired POA&Ms. For example, in May 2020, 58 percent of POA&Ms were current, and 42 percent were expired. However, by June 2021, 76 percent of POA&Ms were current and only 24 percent expired. FEMA has reached stability in the Weakness Remediation - Systems performance metric on the FISMA scorecard and is also compliant with a grade of 96 percent. FEMA's goal is to reduce expired POA&MS to zero and maintain a status of green for the Weakness Remediation metric. Visible improvements in all performance metrics indicate that FEMA is taking the necessary actions to improve its information security program and cybersecurity risk posture for the agency. ECD: March 31, 2022.

6

Appendix C
Major Contributors to This Report

Chiu-Tong Tsang, Director
Shawn Hatch, Manager
Stefanie Holloway, IT Auditor
Thomas Rohrback, Branch Chief, Information Assurance and Testing
Brenden Burke, Program Analyst
Samantha Stout, Program Analyst
Bridgette OgunMokun, Program Analyst
Jason Dominguez, IT Specialist
Rashedul Romel, IT Specialist
Taurean McKenzie, IT Specialist
Kevin Dolloson, Communications Analyst
Garrick Greer, Referencer

Appendix D
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 USSS

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