OFFICE OF INSPECTOR GENERAL

Evaluation of DHS' Information Security Program for Fiscal Year 2018

Homeland Security

September 19, 2019
OIG-19-60

DHS OIG HIGHLIGHTS

Evaluation of DHS' Information Security Program for Fiscal Year 2018

September 19, 2019

Why We Did This Evaluation

We reviewed DHS' information security program for compliance with *Federal Information Security Modernization Act* requirements. We conducted our evaluation according to this year's 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 Fiscal Year 2018.

What We Recommend

We are making three recommendations 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 was effective for fiscal year 2018 because the Department earned the targeted maturity rating, "Managed and Measurable" (Level 4) in four of five functions, as compared to last year's lower overall rating, "Consistently Implemented" (Level 3). We rated DHS' information security program according to five functions outlined in this year's reporting instructions:

Identify — Although some systems lacked authority to operate and security weaknesses were not remediated quickly, DHS achieved Level 4 by identifying cybersecurity risks through the systems security authorization process.
Protect — DHS achieved Level 4 by implementing a patch management program to mitigate vulnerabilities. However, DHS did not apply patches timely to mitigate vulnerabilities; did not implement all configuration settings, as required; and was using unsupported operating systems.
Detect — DHS was rated at Level 4 due to its process to detect potential incidents.
Respond — DHS earned Level 4 by taking sufficient actions to respond to detected cybersecurity incidents.
Recover — DHS received Level 3, its lowest rating, because it did not employ automated mechanisms to test all system contingency plans or identify alternate facilities to recover processing in the event of service disruptions.

We attributed DHS' progress to improvements in information security risk, configuration management practices, continuous monitoring, and more effective security training. By addressing the remaining deficiencies, DHS can further improve its security program ensuring its systems adequately protect the critical and sensitive data they store and process.

Management Response

DHS concurred with all three recommendations and initiated corrective actions.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

September 19, 2019

MEMORANDUM FOR: Paul Beckman
Chief Information Security Officer
Office of the Chief Information Officer

FROM: Sondra F. McCauley
Assistant Inspector General
Office of Audits

SUBJECT: *Evaluation of DHS' Information Security Program for Fiscal Year 2018*

Attached for your action is our final report, *Evaluation of DHS' Information Security Program for Fiscal Year 2018.* We incorporated the formal comments from the Department.

The report contains three recommendations aimed at improving the Department's Cybersecurity Workforce. The Department concurred with all three recommendations. Based on the supporting documentation provided and the results from our Fiscal Year 2019 evaluation, we consider recommendations 1, 2, and 3 resolved and closed.

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

Please call me with any questions, or your staff may contact Kristen Bernard, Deputy Assistant Inspector General for Information Technology, at (202) 981-6371.

Attachment

OIG *Project No.* 18-087-ITA-DHS

Table of Contents

Appendixes

Abbreviations

ATO	Authority to Operate
CBP	Customs and Border Protection
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
Coast Guard	United States Coast Guard
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FLETC	Federal Law Enforcement Training Center
ICE	Immigration and Customs Enforcement
ISCM	Information Security Continuous Monitoring

IT	information technology
NIST	National Institute of Standards and Technology
NSS	National Security Systems
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personal Identifiable Information
PIV	Personal Identity Verification
POA&M	plan of action and milestones
S&T	Science and Technology
Secret Service	United States Secret Service
TSA	Transportation Security Administration
USCIS	United States Citizenship and Immigration Services
USGCB	United States Government Configuration Baseline

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. FISMA provides a framework for ensuring effective security controls over the information resources that support Federal operations and assets.

FISMA focuses on program management, implementation, and evaluation of the security of unclassified and national security systems. Specifically, FISMA requires Federal agencies to develop, document, and implement agency-wide information security programs. 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. 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, 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. The Office of the Inspector General (OIG) is responsible for conducting annual evaluations of information programs and systems under its purview, as well as assessing related security policies and procedures.

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 and complex missions, DHS employs approximately 240,000 personnel, all of whom rely on information technology to perform their duties. As such, it is critical that DHS provide a high level of cybersecurity for the information and information systems supporting day-to-day operations.[2]

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

[1] Public Law 113-283 (December 18, 2014)
[2] Cybersecurity is the protection of internet-connected systems, including hardware, software, and data, from cyberattacks.

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. These programs provide a framework to govern the information systems owned and operated across DHS.

Foremost to all DHS components is adherence 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. Per DHS guidelines, each component CISO is required to assess the effectiveness of controls implemented on all component information systems as part of the security authorization process, and periodically thereafter. The DHS CISO relies on two enterprise management systems to help to administer its information security program and keep track of security authorization status. The enterprise management systems also provide a means to monitor plans of action for remediating information security weaknesses related to unclassified and Secret-level systems.[3]

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 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* provide OIGs with reporting requirements for addressing key areas identified during their independent evaluations of agency information security programs.[4]

This report summarizes the results of our evaluation of the Department's information security program based on the FY 2018 FISMA reporting metrics, Version 1.0.1, dated May 24, 2018. The metrics align five functions from the NIST Cybersecurity Framework with eight domains established in the *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.[5] The NIST framework provides agencies with a

[3] 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.
[4] The *FY 2018 Inspector General FISMA Reporting Metrics* 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.
[5] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018

common structure for identifying and managing cybersecurity across the enterprise, as shown in table 1.

Table1: 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 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*

According to the FY 2018 reporting instructions, 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 previously listed in table 1. The questions are derived from the maturity models outlined within the NIST Cybersecurity Framework. Based on its evaluation, the OIG assigns each of the agency's cybersecurity functions with a maturity level of 1 through 5. Table 2 describes each maturity level.

Table 2 - IG Evaluation Maturity Levels

Maturity Level	Maturity Level Description
Level 1 – Ad-hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2 – Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3 – Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4 – Managed and Measureable	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 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*

Per the FY 2018 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.[6] 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 2018 Inspector General FISMA reporting metrics and NIST's Cybersecurity Framework. We performed our fieldwork at the DHS Office of the CISO and at select DHS components and offices.[7] As part of our review, we also performed

[6] *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics,* Version 1.0.1, May 24, 2018

[7] Customs and Border Protection (CBP), Cybersecurity and Infrastructure Security Agency (CISA), Federal Emergency Management Agency (FEMA), Headquarters, Immigration and Customs Enforcement (ICE), Science and Technology Directorate (S&T), Transportation

testing at three randomly selected components (ICE, TSA, Secret Service) to evaluate compliance with applicable United States Government Configuration Baseline (USGCB) settings on selected workstations, as well as the effectiveness of controls implemented on selected databases and servers.[8]

To determine whether security artifacts were developed according to applicable DHS, OMB, and NIST guidance, we performed quality reviews of 10 security authorization packages that included a mix of unclassified and classified systems at 9 components (CBP, Coast Guard, CISA, FEMA, Headquarters, ICE, S&T, TSA, and USCIS.) As part of the quality review, we also evaluated whether the same 9 components had implemented the required DHS baseline configuration settings on a randomly selected sample of 10 systems. To determine whether components effectively manage and secure their information systems, we reviewed DHS' monthly FISMA Scorecards for unclassified systems and national security systems (NSS).[9] DHS defines NSS as systems that collect, generate, process, store, display, transmit, or receive Unclassified, Confidential, Secret, and Top Secret information.

Results of Evaluation

DHS' information security program was effective for fiscal year 2018 because the Department earned the targeted maturity rating, "Managed and Measurable" (Level 4) in four of five functions, as compared to last year's lower overall rating, "Consistently Implemented" (Level 3). We rated DHS' information security program according to five functions outlined in this year's reporting instructions:

Identify — Although some systems lacked authority to operate and security weaknesses were not remediated quickly, DHS achieved Level 4 by identifying cybersecurity risks through the systems security authorization process.
Protect — DHS achieved Level 4 by implementing a patch management program to mitigate vulnerabilities. However, DHS did not apply patches timely to mitigate vulnerabilities; did not implement all configuration settings as required; and was using unsupported operating systems.
Detect — DHS was rated at Level 4 due to its process for detecting potential incidents.
Respond — DHS earned Level 4 by taking sufficient actions to respond to detected cybersecurity incidents.

Security Administration (TSA), United States Citizenship and Immigration Services (USCIS), United States Coast Guard (Coast Guard), and United States Secret Service (Secret Service).
[8] USGCB is a Federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain an effective configuration setting. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate.
[9] The 2018 FISMA scorecard includes all DHS components previously listed, as well as the Federal Law Enforcement Training Center (FLETC).

Recover — DHS received Level 3, its lowest rating, because it did not employ automated mechanisms to test all system contingency plans or identify alternate facilities to recover processing in the event of service disruptions.

We attributed DHS' progress to improvements in information security risk, configuration management practices, continuous monitoring, and more effective security training. By addressing remaining deficiencies, DHS can further improve its security program ensuring its systems adequately protect the critical and sensitive data they store and process.

DHS' Information Security Program Has Matured, but Additional Improvements Are Needed

DHS' overall information security program is effective because the Department achieved the targeted Level 4 in four of five areas listed in this year's FISMA reporting instructions. Specifically, the Department improved its level of maturity in two of the five cybersecurity functions we evaluated in FY 2017 and FY 2018, as summarized in Table 3.

Table 3: DHS' Maturity Levels for Each Cybersecurity Function in FY 2017 Compared to FY 2018

Cybersecurity Function	Maturity Level	
	FY 2017	FY 2018
1. Identify	Level 4 – Managed and Measureable	Level 4 – Managed and Measureable
2. Protect	Level 3 – Consistently Implemented	Level 4 – Managed and Measureable
3. Detect	Level 3 – Consistently Implemented	Level 4 – Managed and Measureable
4. Respond	Level 4 – Managed and Measureable	Level 4 – Managed and Measureable
5. Recover	Level 3 – Consistently Implemented	Level 3 – Consistently Implemented

Source: OIG analysis based on our FY 2017 report and *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* [10]

Following is a discussion of the progress and deficiencies identified in each cybersecurity function we evaluated.

[10] *Evaluation of DHS' Information Security Program for Fiscal Year 2017,* OIG-18-56, March 1, 2018

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 effectively at the targeted "Level 4 – Managed and Measureable" rating in this area. We based this rating on our conclusion that DHS was managing identified cybersecurity risks through its systems security authorization process. However, 7 NSS and 24 unclassified systems lacked valid authorities to operate (ATO) to provide a context for managing risk. We also identified deficiencies in remediation of security weaknesses, as several components did not effectively manage the plan of action and milestones (POA&M) process as required by DHS.

Risk Management

Risk Management is a process allowing system owners to balance operational and economic costs of protecting data and information systems supporting agency mission activities. It includes establishing the context for risk-related activities such as assessing risk, remediating security weaknesses and identified vulnerabilities, responding to risk, and monitoring risk over time. The risk management process is used whenever major modifications are made that may significantly affect sensitive information and systems, physical environments, interfaces, or system users.

Risk management is a key component of the security authorization process. Foremost, an information system must obtain an ATO before it becomes operational, according to DHS, OMB, and NIST guidance. The process to authorize an information system to operate is a formal decision by a senior official, or "Authorizing Official." The ATO process provides an overarching approach for assessing the effectiveness of operational, technical, and management security controls. DHS requires components to use enterprise management systems to incorporate NIST security controls when each component performs an assessment of its systems. Enterprise management systems enable centralized storage and tracking of all documentation required for the authorization package for each system. Specifically, seven artifacts must be included in the 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; and
7. authorization decision letter.

Based on OMB and NIST guidance, system ATOs are typically granted for a specific period in accordance with terms and conditions established by the authorizing official.[11] In October 2013, DHS began allowing its components to enroll in an ongoing authorization program established by NIST. For each system to be admitted into the ongoing authorization program, a component must have a strong continuous monitoring process, 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 60 and 80 percent, respectively, on the monthly FISMA Scorecard. After a component is accepted into the ongoing authorization program, system owners must fulfill the following requirements for each individual system:

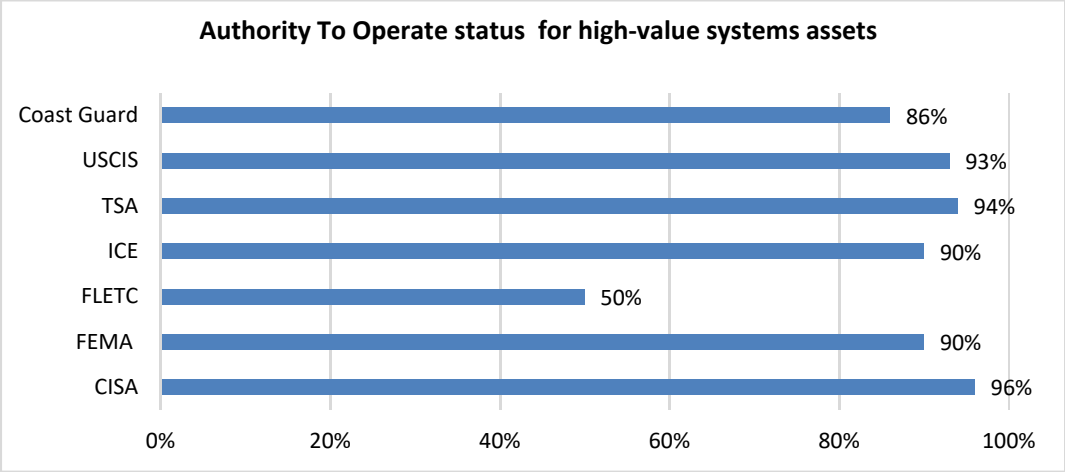
- Ensure the component's enrollment in the ongoing authorization program is documented in the component's acceptance letter.
- Submit an admission letter to enroll the system in the ongoing authorization program.
- Receive an ongoing authorization recommendation letter from the Department to enroll the system in the ongoing authorization program.
- 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.
- Maintain an approved control allocation table listing the system security controls the component agrees to implement.

DHS maintains a target goal to ensure ATOs for 100 percent of its 231 high-value systems assets.[12] The ATO target goal is 95 percent for the 348 operational non-high value assets. However, our review of DHS' August 2018 FISMA Scorecard for unclassified systems revealed that seven components did not meet the required authorization target of 100 percent for high-value assets, as shown in figure 1.

[11] 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

[12] High-value systems are those that may contain sensitive data used in DHS' critical operations or contain unique data that would make them of particular interest to attackers.

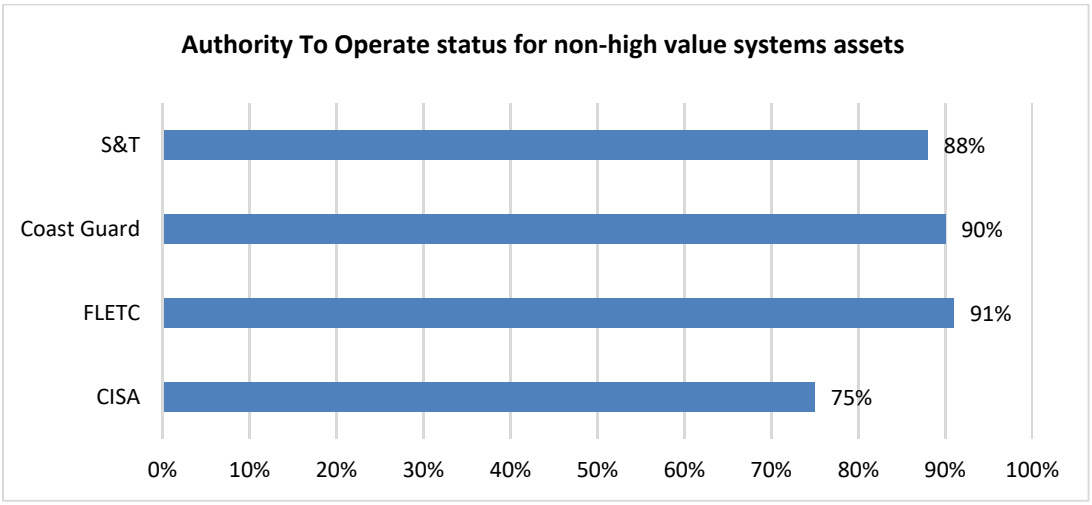
Figure 1. Components Not Meeting the Authority to Operate Goal for High-Value Systems Assets



Source: OIG analysis of DHS' August 2018 FISMA Scorecard

In addition, according to DHS' August 2018 FISMA scorecard, 4 of 12 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: Components Not Meeting the Authority to Operate Goal for Non-High Value Systems Assets



Source: DHS OIG Analysis of DHS' August 2018 FISMA Scorecard

To determine the components' compliance with meeting the Department's NSS security authorization target, we examined the Department's August 2018 NSS Scorecard. We found that neither DHS Headquarters nor the Coast Guard met the ATO target of 95 percent for their NSS systems. Rather, DHS scored 89 percent and Coast Guard scored 74 percent.

To obtain a tally of NSS and unclassified systems lacking ATOs, we analyzed data from DHS' unclassified enterprise management system. Our analysis showed, as of June 30, 2018, 31 systems across DHS lacked ATOs. Specifically, 7 NSS and 24 unclassified systems lacked ATOs. For NSS, this is an improvement over the 16 classified systems that lacked ATOs in 2017. For unclassified systems, the data shows steady improvement compared to prior reviews, which identified 79 unclassified systems operating without ATOs in 2016, and 48 in 2017.[13] Table 4 outlines each component's progress in reducing its number of unclassified systems operating without ATOs from FY 2016 to FY 2018.

Table 4: Number of Unclassified Systems Operating without ATOs

Component	Number of Systems Operating Without ATO		
	FY 2016	FY 2017	FY 2018
CISA	10	6	3
Coast Guard	6	2	6
CBP	12	4	1
FEMA	15	15	5
FLETC	1	2	2
Headquarters	4	7	3
ICE	3	6	2
Secret Service	25	1	0
S&T	3	2	2
TSA	0	3	0
Total	**79**	**48**	**24**

Source: OIG-compiled based on our analysis of data obtained from DHS' unclassified enterprise management system and the *Evaluation of DHS' Information Security Program for Fiscal Year 2017*

The security authorization package documents the results of the security control assessment and provides the authorizing official with essential information needed to make a risk-based decision on whether to authorize operation of an information system. Our quality review of a sample of 10 ATO packages from select components identified the following deficiencies in documentation to support ATO decisions:[14]

- Security plans for seven systems did not identify how security controls were implemented for each system.
- Individual system categorizations did not match data entered in the Department's enterprise management system, security plan, and Federal

[13] *Evaluation of DHS' Information Security Program for Fiscal Year 2016*, OIG-17-24, January 18, 2017; and *Evaluation of DHS' Information Security Program for Fiscal Year 2017*, OIG-18-56, March 1, 2018

[14] We based our review of ATO packages on the requirements in DHS, NIST, and OMB policies.

Information Processing Standards (FIPS) 199 worksheet for six systems.[15]
- Security assessment results for six systems could not be traced back to the traceability matrix documents to ensure they were appropriately implemented and operational.
- Components could not provide sufficient documentation to support selected controls were tested as part of the annual self-assessment for three systems.

Weakness Remediation

FISMA requires the use of POA&Ms to track and plan the resolution of information security weaknesses. The POA&M details the resources required to accomplish elements of the plan, any milestones for meeting tasks, and scheduled completion dates for milestones.[16]

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 6 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, 2018, showed the following deficiencies:

- Of the 6,855 open unclassified POA&Ms, 1,390 (20 percent) were past due. Moreover, of the 1,390 past due POA&Ms, 1,172 (84 percent) were overdue by more than 90 days, while 537 (38 percent) were overdue by more than a year.
- Of the 1,390 past due unclassified POA&Ms, 1,073 (77 percent) had weakness remediation costs estimated at less than $50. 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.

[15] FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). Security categorization, the first step of NIST Risk Management Framework, is essential for selecting an initial set of baseline security controls for a system.
[16] OMB Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001

Similarly, our quality review of 10 security authorization packages showed 6 systems had POA&Ms that were not mitigated within 30 days of each system obtaining ATO. Additionally, POA&Ms were not created to address inadequate controls for the same six systems. Our analysis of the August 2018 *NSS FISMA Cybersecurity Scorecard* revealed both the Coast Guard and TSA did not meet DHS' NSS weakness remediation metrics through the POA&M process.

2. Protect

The "Protect" function entails developing and implementing the appropriate safeguards to ensure delivery of critical services. It includes four FISMA domains: Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training. We determined that, overall, DHS was operating at the target "Level 4 – Managed and Measureable" rating in this function. DHS can further improve its focus on key configuration management activities, such as replacing unsupported operating systems and timely application of security patches. Specifically, we concluded that select components did not replace or update two unsupported operating systems, and did not apply security patches and updates timely to mitigate critical and high-risk security vulnerabilities on selected systems.[17] In addition, the components did not implement all configuration settings required to protect their systems.

DHS generally had effective practices to manage the four domains essential to the "Protect" function. DHS components' compliance in each domain is described in the following sections.

Configuration Management

DHS requires components configure their workstations according to configuration settings set forth in the USGCB, which is the core set of security-related configuration settings that all agencies must implement. These settings are necessary to secure the confidentiality, integrity, and availability of DHS' systems and the information they process and store. Where agencies do not comply with the settings, they must document any deviations. Once deviations are documented and all USGCB settings are fully implemented, the compliance rate should be 100 percent.

Our testing revealed that not all components we reviewed had implemented all required configuration settings. Specifically, we tested selected unclassified Windows 7 workstations at ICE, TSA, and Secret Service to determine

[17] One operating system included the Microsoft Windows Server 2003 that was no longer supported as of July 2015; the other included a Red Hat Enterprise Linux that was not supported after July 2014.

compliance with the required settings. Table 5 summarizes the components' compliance.

Table 5: Compliance Rate of Selected Component Systems with USGCB

Component	Percentage of Compliance
ICE	97%
TSA	98%
Secret Service	98%

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

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

- System cryptography – This setting ensures that the operating system uses the strongest algorithms for encryption and digital signature. Using weak algorithms increases the risk of compromise.
- Remote Assistance – Enabling this setting can restrict a user from accepting unsolicited remote assistance requests from malicious users.
- Smart card removal behavior – This setting determines what happens when an authenticated user removes the smart card from its reader. When this setting is not configured properly, it increases the risks that malicious users can gain unauthorized access to the workstation.
- Network Client Communications – When the setting is enabled, specific network packets must be digitally signed to maintain the integrity of communication between a workstation and server. Not signing communications digitally increases the risk of service disruption or unauthorized access to information.

In addition, as part of our quality review of the 10 security authorization packages, we evaluated components' compliance with DHS Baseline Configuration settings on 10 judgmentally selected servers.[18] We determined components' compliance implementing required configuration settings on the servers ranged from:

[18] DHS developed Baseline Configuration guides to establish a clear, concise set of procedures to ensure a minimum baseline of security in the installation and configuration of the hardware and software.

- 85 to 97 percent on Windows 2008 servers,
- 89 to 97 percent on Windows 2012 servers, and
- 33 to 81 percent on UNIX/Linux/AIX servers.[19]

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

Unsupported Operating Systems

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 discontinue the use of such unsupported operating systems (e.g., Windows XP and Windows Server 2003). However, we identified the following unsupported operating systems still in use:

- Windows Server 2003 on one ICE system, and
- Red Hat Enterprise Linux on one Secret Service system.

Vulnerability Assessment Testing

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

Table 6: Software Patching Vulnerabilities Identified on Selected Operating Systems at ICE, Secret Service, and TSA

Operating System	Component	Unique Critical Vulnerabilities	Unique High Vulnerabilities
Windows 7 Workstations	ICE	2	5
Linux Servers	ICE	0	1
Windows 7 Workstations	TSA	3	4
Windows 7 Workstations	Secret Service	1	4
Windows Servers	Secret Service	1	6
Linux Servers	Secret Service	13	61

Source: OIG-compiled based on system test results

[19] Through the years, the UNIX operating system has been developed and evolved through a number of different versions and environments. For example, Linux and IBM's AIX are variants of the UNIX operating system and have their own unique elements and foundations.

Following are five specific examples of the critical and high-risk vulnerabilities we detected on the systems tested:

1. ICE Windows 7 workstations were missing security updates for Microsoft XML core services and various unsupported Microsoft Office Suite functions. The workstations also lacked security software patches for VMware Horizon; Microsoft Access, Excel, and other Office products; and a library loading capability.
2. An ICE Linux server was missing a patch to address one unique high-risk vulnerability that could allow remote attackers to launch a denial of service attack.
3. TSA's Windows 7 workstations lacked operating system security updates for Microsoft Skype/Lync/Live meeting and Internet Explorer.
4. Secret Service's Windows servers were missing security updates for Internet Explorer, Microsoft Security Bulletin, and Oracle Java. They also had out-of-date antivirus definitions and an insecure library loading vulnerability.
5. Several Secret Service's Linux servers had 13 critical and 61 high-risk vulnerabilities. These vulnerabilities were attributed to the servers running an unsupported version of the Red Hat Enterprise Linux operating system.

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.

Identity and Access Management

Identity and Access Management is critical to ensure that 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.[20] DHS requires all privileged and unprivileged employees and contractors use the cards to log onto DHS systems. Based on the August 2018 FISMA Scorecard, DHS was 99 percent compliant with PIV implementation for both privileged and unprivileged

[20] *Homeland Security Presidential Directive-12: Policy for a Common Identification Standard for Federal Employees and Contractors*, dated August 27, 2004, required Federal agencies to begin using a standard form of identification to gain physical and logical access to federally controlled facilities and information systems. It also called for interoperable mechanisms for authenticating employee identity and permissions at graduated levels of security, depending on the agency environment and the sensitivity of facilities and data accessed.

users. Specifically,

- Nine DHS components had met the 100 percent compliance target for required PIV card use for both privileged and unprivileged users.[21]
- Coast Guard did not meet the Department's compliance target because it had implemented PIV card use for 97 percent of its privileged users and 99 percent of its unprivileged users.

Data Protection and Privacy

DHS developed a data privacy policy in 2011 for the protection of personally identifiable information (PII) stored on 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, 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. In addition, 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.

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 in place that is collaboratively managed by Headquarters, 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 information technology (IT) security awareness training, as well as specialized training for employees with significant responsibilities.

According to the program officials, while DHS assessed the knowledge, skills, and abilities of its cyber workforce, DHS has not finalized a strategy to address the identified gaps outlined in its Cybersecurity Workforce Assessment. Without a workforce strategy, DHS cannot assure that its employees possess the knowledge and skills necessary to perform job functions, or that qualified personnel are hired to fill cybersecurity-related positions.

[21] CISA, Headquarters, FEMA, Federal Law Enforcement Training Center, ICE, OIG, Secret Service, S&T, and TSA

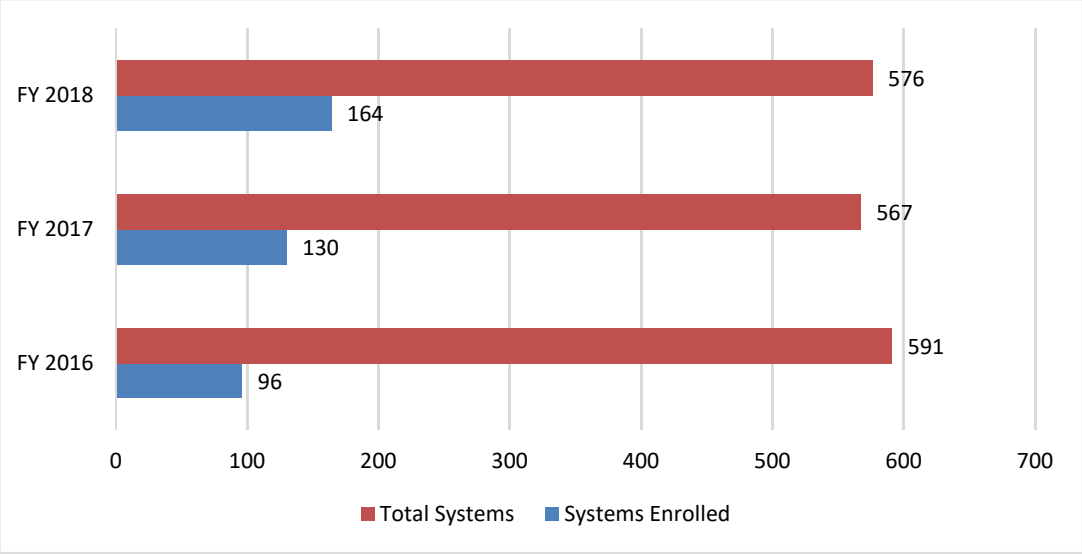
Although the Department has made overall progress in the "Protect" function, DHS components can further safeguard the Department's information systems and sensitive data by:

- implementing all required USGCB and DHS Baseline 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 Cybersecurity Workforce strategy for addressing identified gaps outlined in its assessment.

3. Detect

The "Detect" function entails developing and implementing appropriate activities, including ongoing systems authorization and continuous monitoring, to identify the occurrence of irregular system activity. We determined the Department had increased the number of systems enrolled in the program from FY 2016 to FY 2018, as shown in figure 3. As of September 2018, eight components were enrolled in the Department's ongoing authorization program.

Figure 3: Total DHS Systems Enrolled in the Ongoing Authorization Program FY 2016 to FY 2018



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

Based on our analysis, we determined DHS was operating effectively, at "Level 4 – Managed and Measureable," in monitoring its unclassified systems. However, DHS' authorization program for its NSS was not equally effective.

Information Security Continuous Monitoring (ISCM)

As part of the Detect function, DHS established its continuous monitoring, or ISCM, program, which allows officials to gain visibility into network resources, maintain awareness of security threats and vulnerabilities, and ensure effectiveness of implemented controls. In 2011, DHS developed an initial ISCM strategy by implementing tools and metrics at each layer in the architecture. DHS' current ISCM program for its unclassified systems includes monthly data feeds from automated system scans performed across component networks and systems. The current continuous monitoring program provides officials with awareness of threats and vulnerabilities, as well as mission and business effects, for unclassified systems.

However, DHS did not have an equivalent process for automated monitoring and scanning of NSS department-wide. Instead, DHS officials relied on data calls to components to monitor their NSS performance metrics regarding system authorization, weakness remediation, vulnerability management, and contingency plan testing. DHS officials manually prepared monthly scorecards for NSS. Our analysis of performance data from DHS' classified enterprise management system, as of June 30, 2018, revealed the following issues:

- Components with open or unresolved NSS actions did not include resource estimates for mitigating security weaknesses through POA&Ms, as required by OMB and DHS policy.
- There was no capability to determine whether system contingency plans are tested as required.
- There was a lack of evidence that components periodically reviewed the remediation status of all open POA&Ms.

Nonetheless, our analysis of the June 2018 NSS scorecard revealed that four components — CISA, FEMA, S&T, and TSA — received 100 percent scores for contingency plan testing. Additionally, four components — CISA, Headquarters, FEMA, and S&T — received perfect scores for weakness remediation in the same NSS scorecard. The discrepancies we identified in the performance data from the classified enterprise management system, and the high score reported here in the NSS scorecard, are indicators that management officials may not have the most accurate information to make credible risk-based decisions.

4. Respond

The "Respond" function entails developing and implementing appropriate responses to detected cybersecurity events. We determined DHS was operating effectively at the targeted "Level 4 – Managed and Measurable" rating in this

area. Given agencies' increased reliance on computer resources to accomplish their missions, incident response has become a vital part of an effective information security program.

Incident Response

According to FISMA 2014, an "incident" is defined as an occurrence that jeopardizes or may jeopardize the integrity, confidentiality, or availability of information or an information system without legal consent. It may also constitute a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. Although agencies can reduce the frequency of incidents by taking actions and instituting controls to secure their networks and systems, they have no assurance of preventing all incidents.

The Department established two Security Operation Centers to monitor and respond to suspicious activities — one for unclassified systems and the other for classified systems. These Security Operations Centers are responsible for ensuring components comply with applicable Federal and DHS security policy and corresponding controls. DHS Security Operations Centers provide situational awareness, serve as central data repositories, and facilitate reporting and coordination regarding computer security incidents across the Department. In addition, DHS personnel are required to follow DHS Security Operations Center procedures for detecting, reporting, and responding to information security incidents.[22]

The "Respond" function supports agencies' ability to contain the impact of a potential cybersecurity event. As such, the function not only requires that agencies develop procedures for detecting, reporting, and responding to security incidents; it also requires coordinating response activities with internal and external stakeholders. Specifically, FISMA 2014 requires agencies to:

- notify and consult with law enforcement agencies and relevant Offices of Inspector General and General Counsel, as appropriate; and
- inform selected congressional oversight committees of major incidents within the required timeframe.

In 2017, DHS developed procedures to notify OIG, the Office of General Counsel, and selected congressional oversight committees about major PII incidents. However, we determined that DHS has not yet developed detailed procedures for notifying OIG about the details regarding other types of security incidents, including major incidents, not involving PII.

[22] DHS' incident response procedures are outlined in 4300A, 4300B, and 4300C.

We identified instances where components did not comply with security incident reporting requirements. Specifically, as part of our review of 10 security authorization packages, we determined that 4 of 9 components reviewed had at least 1 incident that was not reported within required timeframes.[23] Two components had at least one lost/stolen device incident not reported timely. Additionally, 4 of the 9 components, experienced incidents from penetration testing activities that were not identified through Security Operations Center incident monitoring.

When security incidents are not reported to the Security Operations Centers, the Department cannot take appropriate corrective actions to contain their potential impact and protect against a potential cybersecurity event. Moreover, the Security Operations Centers may lack the information they need to address suspicious activity as quickly as possible.

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 3 – Consistently Implemented," just below the targeted level for effectiveness. We based this rating on our assessment that DHS did not employ automated mechanisms to test system contingency plans, did not develop procedures for handling sensitive information, and did not identify alternate facilities to recover processing in the event of service disruptions. Although contingency planning is vital to agency recovery from a cybersecurity event, DHS' progress in this area was minimal from 2017 to 2018.

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

[23] DHS' incident response procedures are outlined in 4300A.

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 corresponding contingency plans that outline backup and disaster recovery procedures for their respective information systems.

However, we identified the following four deficiencies:

1. Two components (Coast Guard and Headquarters) did not meet DHS' NSS compliance target for contingency plan testing.
2. Four components (CISA, Coast Guard, FEMA, and ICE) had not tested contingency plans for 8 of 576 unclassified systems.
3. For two systems with high or moderate availability per their FIPS-199 security categorizations, components did not include disaster recovery procedures for managing sensitive information at alternate or offsite facilities in their contingency plans, as required.
4. Four systems, with high availability per their FIPS-199 security categorizations, did not have data backup, data recovery, or notification tests performed for more than a year. Components are required to conduct these tests annually.

DHS has made little progress, maintaining a "Level 3 – Consistently Implemented" rating in the "Recover" function for the past 2 years. 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 the inability to recover operations in a timely manner.

Recommendations

We recommend the DHS CISO:

Recommendation #1: Enforce requirements for components to obtain authority to operate; test contingency plans; and apply sufficient resources to mitigate security weaknesses for both their unclassified systems and NSS.

Recommendation #2: Establish detailed procedures to notify relevant stakeholders, including the Office of Inspector General and the Office of General Counsel, of non-PII related major incidents.

Recommendation #3: Implement internal controls and perform quality reviews to validate that information security data input to DHS' classified enterprise management system is complete and accurate.

Management Comments and OIG Analysis

DHS concurred with our three recommendations and is taking steps or has implemented actions to address them. Appendix B contains DHS' management comments in their entirety. We also received technical comments to the draft report and revised the report as appropriate. We consider all recommendations resolved and closed. A summary of DHS' responses and our analysis follow.

DHS' Comments to Recommendation 1: Concur. The Department already has a process in place to enforce requirements for components to obtain ATOs, test contingency plans, and apply sufficient resources to mitigate security weaknesses. On June 21, 2019, the Office of the CISO updated DHS 4300A with the following policies for unclassified systems:

- Security Assessment and Authorization Policy,
- Contingency Planning Policy, and
- DHS Plan of Action and Milestones Process Guide.

The Office of the CISO monitors Security Authorization and POA&M remediation progress continuously and reports the results in the monthly information security scorecards. To ensure its effectiveness, the CISO implemented processes for escalating any areas of concern related to the Department's unclassified systems through the DHS CISO Council and Deputy Under Secretary for Management meetings.

For NSS, DHS 4300B (4300B.102) provides guidance for assigning senior personnel as authorizing officials and educating them on the Security Authorization process. The Office of the CISO monitors components' security programs for compliance with DHS policies. Components are responsible for applying sufficient resources to mitigate their specific weaknesses and conducting contingency plan tests, which were completed on November 21, 2018.

The Office of the CISO provided separately to the OIG documentation to support completion of these corrective actions. The Office of the CISO requests that the OIG consider this recommendation resolved and closed as implemented.

OIG Analysis of DHS' Comments: We believe that the steps the Office of the CISO has taken satisfy the intent of this recommendation. After reviewing the supporting documents DHS provided and the results from our FY 2019 evaluation, this recommendation is now resolved and closed.

DHS' Comments to Recommendation 2: Concur. The Department has implemented procedures in the *DHS Major Cybersecurity Incident Response Guide*. This guide outlines procedures for notifying the OIG, General Counsel, and other relevant stakeholders regarding major incidents. The roles of the Major Cybersecurity Incident Response Team, including the OIG and General Counsel, are discussed in the guide.

The Office of the CISO provided separately to the OIG documentation to support the completion of these corrective actions. The Office of the CISO requested that the OIG consider this recommendation resolved and closed as implemented.

OIG Analysis of DHS' Comments: We believe that the steps the Office of the CISO has taken satisfy the intent of this recommendation. After reviewing the supporting documents DHS provided and the results from our FY 2019 evaluation, this recommendation is now resolved and closed.

DHS' Comments to Recommendation 3: Concur. The Office of the CISO has established a process to validate information security data input to DHS' classified enterprise management system. For example, DHS has strengthened its oversight of the classified enterprise management system by establishing the document inventory team and risk executive function to approve and monitor components' compliance with DHS 4300B. Given recent changes in the way components report, the CISO expects NSS scores to improve in the near future.

The Office of the CISO provided separately to the OIG documentation to support the completion of these corrective actions. The Office of the CISO requested that the OIG consider this recommendation resolved and closed as implemented.

OIG Analysis of DHS' Comments: We believe that the steps the Office of the CISO has taken satisfy the intent of this recommendation. After reviewing the supporting documents DHS provided and the results from our FY 2019 evaluation, this recommendation is now resolved and closed.

Appendix A
Objective, Scope, and Methodology

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107–296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote efficiency and effectiveness within the Department.

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 fiscal year 2018. Our independent evaluation focused on assessing DHS' information security program against requirements outlined in the *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*. Specifically, we evaluated DHS' Information Security Programs' compliance with requirements outlined in five NIST Cybersecurity Functions.

We performed our fieldwork at the DHS Office of the CISO and at organizational components and offices, including CISA, Coast Guard, Headquarters, CBP, FEMA, ICE, S&T, Secret Service, TSA, and USCIS. To conduct our evaluation, we interviewed select DHS Headquarters 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 2017 FISMA evaluation as a baseline for the FY 2018 evaluation;
- evaluated policies, procedures, and practices DHS had implemented at the program and component levels;
- reviewed DHS' POA&Ms and ongoing authorization procedures to ensure all 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, contingency planning; and
- developed an independent assessment of DHS' information security program.

Using scanning tools, we conducted vulnerability assessments of controls implemented at three components. We also tested DHS' compliance with applicable USGCB settings on selected workstations.

OIG's contractors performed quality reviews of security authorization packages at CBP, CISA, Coast Guard, FEMA, Headquarters, ICE, USCIS, S&T, and TSA for compliance with applicable DHS, Office of Management and Budget, and NIST guidance. As part of the quality reviews, we executed automated scripts on sampled systems to determine whether baseline configuration settings were implemented as required. We also reviewed information from DHS' enterprise management systems to determine data reliability and accuracy. We found no discrepancies or errors with the data.

We conducted this review between May and October 2018 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

August 26, 2019

MEMORANDUM FOR: Sondra F. McCauley
Assistant Inspector General for Audits
Office of Inspector General

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

SUBJECT: Management Response to Draft Report: "Evaluation of DHS' Information Security Program for Fiscal Year 2018" (Project No. OIG-18-087-ITA-DHS)

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

The Department is pleased to note OIG's positive recognition of the DHS information security program for Fiscal Year (FY) 2018, specifically noting the Department' improved targeted maturity rating of "Managed and Measurable" (Level 4) in four of five functions from an overall rating of "Consistently Implemented" (Level 3) from FY 2017. DHS remains committed to ensuring its information systems adequately protect the sensitive data they store and process.

The draft report contained three recommendations with which the Department concurs. Attached find our detailed response to each recommendation. Technical comments were previously provided under separate cover.

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.

Attachment

Attachment: Management Response to Recommendations Contained in OIG-18-087-ITA-DHS

OIG recommended that the DHS Chief Information Security Officer (CISO):

Recommendation 1: Enforce requirements for components to obtain authority to operate; test contingency plans; and apply sufficient resources to mitigate security weaknesses for both their unclassified systems and NSS [National Security System].

Response: Concur. DHS already has a process in place to enforce requirements for components to obtain authority to operate; test contingency plans; and apply sufficient resources to mitigate security weaknesses. Specifically, the DHS Office of the Chief Information Officer (OCIO) has established these processes for unclassified systems and NSS in DHS 4300A "Sensitive Systems Policy Directive" and DHS 4300B "NSS Policy Directive."

The DHS 4300A, updated on June 21, 2019, contains the following policies for unclassified systems:

- Security Assessment and Authorization Policy for Unclassified systems,
- Contingency Planning policy, and
- DHS Plan of Action and Milestones Process Guide.

In addition, Security Authorization and Weakness Remediation checks are tracked continuously and reported monthly via the Federal Information Security Modernization Act scorecard, and components are responsible for applying sufficient resources to mitigate their specific weaknesses and to conduct contingency plan tests. To ensure effectiveness, on June 21, 2019, the DHS Office of the Chief Information Security Officer (OCISO) implemented escalation processes through the DHS CISO council and Deputy Under Secretary for Management (DUSM) meetings for areas of concern to the DHS Chief Information Officer and DUSM related to Sensitive But Unclassified issues.

For NSS, the DHS 4300B (4300B.102) provides guidance for assigning senior personnel as authorizing officials and educating them on the process. The OCISO reviews for compliance and components are responsible for applying sufficient resources to mitigate their specific weaknesses and to conduct contingency plan tests which were completed on November 21, 2018.

Documentation corroborating the completion of these actions is in the process of being provided to the OIG under separate cover. We request that the OIG consider this recommendation resolved and closed as implemented.

2

Recommendation 2: Establish detailed procedures to notify relevant stakeholders, including the Office of Inspector General and the Office of General Counsel [OGC], of non-PII related major incidents.

Response: Concur. The DHS OCISO has implemented procedures like this, which are documented in the "DHS Major Cybersecurity Incident Response Guide" (Version 1.0), dated August 29, 2018 (Attachment A). This guide outlines procedures for notifying the OIG, OGC, and other relevant stakeholders regarding major incidents. The roles of the Major Cybersecurity Incident Response Team, includes OIG and OGC as members of the team, is discussed in the Guide.

Documentation corroborating the completion of these actions is in the process of being provided to the OIG under separate cover. We request that the OIG consider this recommendation resolved and closed as implemented.

Recommendation 3: Implement internal controls and perform quality reviews to validate that information security data input to DHS' classified enterprise management system is complete and accurate.

Response: Concur. The DHS OCISO has established a process to validate information security data input to DHS' classified enterprise management system. Specifically, within the NSS enterprise management system, there is a document inventory team and risk executive function role that approves and monitors the risk management framework steps in accordance with DHS 4300B. Given recent changes to the way components report, the DHS OCIO expects NSS scores to improve in the near future.

Documentation corroborating the completion of these actions is in the process of being provided to the OIG under separate cover. We request that the OIG consider this recommendation resolved and closed as implemented.

3

Appendix C
Office of Audits Major Contributors to This Report

Chiu-Tong Tsang, Director
Marcie McIsaac, IT Audit Manager
Brandon Barbee, IT Audit Manager
Thomas Rohrback, Chief, Information Assurance and Testing
Yusuf Lane, IT Auditor
Raheem Wilson, Program Analyst
Jason Dominguez, IT Specialist
Rashedul Romel, IT Specialist
Taurean McKenzie, IT Specialist
John Kohler, Referencer
Michael Thorgersen, Referencer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
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