OFFICE OF INSPECTOR GENERAL

Evaluation of DHS' Information Security Program for FY 2017

Homeland Security

March 1, 2018
OIG-18-56

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

March 1, 2018

MEMORANDUM FOR: Jeffrey Eisensmith
Chief Information Security Officer

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

SUBJECT: *Evaluation of DHS' Information Security Program for Fiscal Year 2017*

Attached for your action is our final report, *Evaluation of DHS' Information Security Program for Fiscal Year 2017*. We incorporated the formal comments from the Director, Departmental GAO-OIG Liaison Office, in the final report.

The report contains five recommendations aimed at improving the Department's information security program. The Department concurred with all five recommendations. Based on information provided in the response to the draft report, we consider recommendations 1, 2, 3, and 5 open and resolved. Recommendation 4 is resolved and closed. 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. Please send your response or closure request to OIGITAuditsFollowup@oig.dhs.gov.

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

Please call me with any questions, or your staff may contact Chiu-Tong Tsang, Director, Cybersecurity and Intelligence Division, at (202) 254-5472.

Attachment

DHS OIG HIGHLIGHTS

Evaluation of DHS' Information Security Program for Fiscal Year 2017

March 1, 2018

Why We Did This Evaluation

We reviewed DHS' information security program in accordance with the *Federal Information Security Modernization Act of 2014* (FISMA). Our objective was to determine whether DHS' information security program and practices were adequate and effective in protecting the information and information systems that supported DHS' operations and assets in fiscal year 2017.

What We Recommend

We are making five recommendations to the Chief Information Security Officer to enhance oversight of DHS' information security program in the areas of plans of action and milestones, security authorization, continuous monitoring, and configuration management.

For Further Information:
Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

The Department of Homeland Security could protect its information and systems more fully and effectively. DHS' information security program fell one level below the targeted "Level 4" in three of five areas listed in this year's FISMA reporting instructions. Specifically, DHS —

- met Level 4 in the ***identify*** area by managing identified cybersecurity risks through the systems security authorization process. However, 64 systems lacked valid authority to operate, and components did not remediate security weaknesses timely;
- did not implement all configuration settings required to ***protect*** component systems, continued using unsupported operating systems, and did not apply security patches timely to mitigate critical and high-risk security vulnerabilities on selected systems;
- did not monitor software licenses for unclassified systems and relied on data calls to monitor national security systems as part of its continuous monitoring process to ***detect*** potential incidents;
- met Level 4 through actions to ***respond*** to detected cybersecurity incidents; and
- did not test all system contingency plans, develop procedures for handling sensitive information, or identify alternate facilities to ***recover*** processing in the event of service disruptions.

Additional oversight is needed to address the identified deficiencies. Otherwise, DHS cannot ensure its systems adequately protect the sensitive data they store and process.

Management Response

DHS concurred with all five recommendations and had corrective actions underway to address the findings.

Table of Contents

Appendixes

Abbreviations

ATO	authority to operate
CBP	Customs and Border Protection
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
NPPD	National Protection and Programs Directorate
OIG	Office of Inspector General
PIV	Personal Identity Verification
POA&M	plan of action and milestones
S&T	Science and Technology
SA	security authorization
TSA	Transportation Security Administration
USCIS	United States Citizenship and Immigration Services
USGCB	United States Government Configuration Baseline

Background

The Congress enacted the *Federal Information Security Modernization Act of 2014* (FISMA) in recognition of the importance of information security to the economics and national security interests of the United States. Information security involves protecting data and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. FISMA provides a comprehensive framework to ensure the effectiveness of security controls over the information resources that support Federal operations and assets. In addition, the Act 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 that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or source. According to FISMA, agency heads 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 DHS Chief Information Security Officer, who heads the Information Security Office, manages the Department's information security program for its unclassified systems, as well as its national security systems classified as "Secret" and "Top Secret." The Chief Information Security Officer developed two separate performance plans to aid in managing the program for its unclassified and classified systems in fiscal year 2017. This official also maintains ongoing awareness of the Department's information security program, vulnerabilities, and potential threats through the execution of three programs:

- Information Security Continuous Monitoring (ISCM) Data Feeds
- Ongoing Authorization Program
- Security Operations Center

Further, DHS relies on two enterprise management systems to create and maintain security authorization (SA) documentation and monitor plans of

action and milestones (POA&M) for remediating information security weaknesses related to its unclassified and "Secret"-level systems.[1]

FY 2017 FISMA Reporting Instructions

Our report summarizes the results of our evaluation of the Department's information security program based on the FISMA reporting instructions dated April 14, 2017. The guidance aligns five functions from the NIST Cybersecurity Framework with eight domains for which metrics were established in the FISMA legislation.[2] The NIST Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides OIGs with instructions for assessing the maturity of information security controls to address those risks, 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**
		Contractor Systems
Protect	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	**Configuration Management**
		Identity and Access Management
		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 2017 FISMA Reporting Metrics

According to the FY 2017 reporting instructions, OIGs are well positioned to assess agency information security programs given their audit responsibilities and their awareness of each agency's unique mission, cybersecurity challenges, and resources to address those challenges. Each OIG is to evaluate the

[1] The National Institute of Standards and Technology (NIST) defines an SA 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.
[2] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014

agency's information security program based on 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. OIG will assign each of the agency's cybersecurity functions with a maturity level of 1 through 5 based on its evaluation. Following are the five possible maturity levels:

1. Ad-hoc
2. Defined
3. Consistently Implemented
4. Managed and Measurable
5. Optimized

Per the FY 2017 Reporting instructions, Level 4, "Managed and Measurable," represents an effective cybersecurity function. Where an agency achieves Level 4 in the majority of the five cybersecurity functions evaluated, its information security program may be considered effective overall.

The President's Cybersecurity Executive Order

On May 11, 2017, the President issued Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, which outlines the various actions an agency must take to enhance its cybersecurity. The Executive Order states that known but unmitigated vulnerabilities are among the highest cybersecurity risks that agencies face. Known vulnerabilities include using operating systems or hardware beyond the vendors' support lifecycle, declining to implement the vendors' security patches, or failing to execute security-specific configuration guidance.

As such, the President plans to hold agency heads accountable for implementing risk management measures commensurate with the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information technology (IT) and data. In addition, agency heads will be accountable for aligning cybersecurity risk management processes with strategic, operational, and budgetary planning processes. Effective upon issuance of the Executive Order, each agency is required to use the NIST Cybersecurity Framework to manage the agency's cybersecurity risk. Each agency is also required to submit a risk management report to the Secretary of Homeland Security and the Director of the Office of Management and Budget within 90 days of the date of the Executive Order.

On May 19, 2017, the Office of Management and Budget issued a memorandum, "Reporting Guidance for Executive Order on Strengthening the

Cybersecurity Federal Networks and Critical Infrastructure" (M-17-25), which provides implementing guidance for the actions required in the Executive Order. DHS submitted the Department's plan for implementing actions outlined in the Executive Order on August 3, 2017. The Department identified "obsolete operating systems and hardware" and "cybersecurity workforce recruitment, retention, and training" as the top two risks it faced to implementing the President's Executive Order. Insufficient resources to ensure systems have current authority to operate (ATO) also pose a significant challenge.

We conducted this review to determine whether DHS' information security program and practices were adequate and effective in protecting the information and information systems that supported DHS' operations and assets in FY 2017.

Results of Evaluation

DHS could protect its information and systems more fully and effectively. DHS' overall information security program fell short of meeting the targeted "Level 4" for effectiveness in three of five areas listed in this year's FISMA reporting instructions. Specifically, DHS —

- met Level 4 in the ***identify*** area by managing identified cybersecurity risks through the systems security authorization process. However, 64 systems lacked valid authority to operate, and components did not remediate security weaknesses timely;
- did not implement all configuration settings required to ***protect*** component systems, continued using unsupported operating systems, and did not apply security patches timely to mitigate critical and high-risk security vulnerabilities on selected systems;
- did not monitor software licenses for unclassified systems and relied on data calls to monitor national security systems as part of its continuous monitoring process to ***detect*** potential incidents;
- met Level 4 through actions to ***respond*** to detected cybersecurity incidents; and
- did not test all system contingency plans, develop procedures for handling sensitive information, or identify alternate facilities to ***recover*** processing in the event of service disruptions.

Additional oversight is needed to address the identified deficiencies. Otherwise, DHS cannot ensure its systems adequately protect the sensitive data they store and process.

DHS' Information Security Program Could Be Improved

DHS has work to do to ensure the protection of the information and systems it uses to carry out its mission operations. DHS' overall information security program met the targeted Level 4 in two of five areas listed in this year's FISMA reporting instructions. Table 2 summarizes DHS' maturity level ratings for each cybersecurity function evaluated.

Table 2: DHS' Ratings for Each Cybersecurity Function Evaluated

Cybersecurity Function	Maturity Level
Identify	Level 4 - Managed and Measurable
Protect	Level 3 - Consistently Implemented
Detect	Level 3 - Consistently Implemented
Respond	Level 4 - Managed and Measurable
Recover	Level 3 - Consistently Implemented

Source: DHS OIG based on FY 2017 reporting instructions

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

Identify

The "Identify" function entails developing the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. We determined that DHS was operating effectively at the targeted "Level 4 – Managed and Measurable" in this area. We based this on our assessment that DHS was managing identified cybersecurity risks through its systems security authorization process. However, 48 unclassified and 16 national security systems lacked valid authority to operate. Components also did not maintain complete information to remediate security weaknesses timely.

Risk Management

Risk Management is a process that allows system owners to balance the operational and economic costs of implementing measures to protect the information systems and data that support the agency's mission activities. The

process is utilized whenever major modifications are introduced that have the potential to significantly impact sensitive information and systems, physical environments, interfaces, or user communities. It may also be needed to manage security risks during the system lifecycle.

Risk management encompasses the SA process. An SA is a formal management decision by a senior official to authorize an information system to operate, and to accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on implementation of an agreed-upon set of security controls. The SA process provides an approach for assessing the security controls (e.g., operational, technical, and management controls) to determine their overall effectiveness. DHS requires its components to use enterprise management systems to incorporate NIST security controls when performing SA on their systems. Enterprise management systems enable components to develop and maintain system security documentation, as well as centralize artifacts supporting the authority to operate for each system.

Components use DHS enterprise management tools to create SA artifacts for monitoring and authorizing each system. These artifacts include:

- privacy threshold analysis and, if required, privacy impact assessment;
- security plan;
- contingency plan;
- security assessment plan;
- contingency plan test results;
- security assessment report; and
- authorization decision letter.

Typically, system ATOs are granted for 3-year periods, based on NIST guidance. In October 2013, DHS began to allow components to enroll in an ongoing authorization program newly established by NIST. A component is required to have a strong ISCM process, approved common controls, a designated ongoing authorization manager, and a chartered operational risk management board for admission to the ongoing authorization program. In addition, components must maintain SA and weakness remediation metrics above 80 and 60 percent, respectively, on the monthly FISMA Scorecard. After a component has been accepted into the ongoing authorization program, an individual system must fulfill the following requirements to be entered into the program as well:

- component ongoing authorization program acceptance letter;
- system admission letter;
- ongoing authorization recommendation letter;
- System ATO expiration more than 60 days beyond the date of system submission to enter the program;

- information system security officer with responsibilities primarily related to information assurance/security;
- information system security officer trained on ongoing authorization processes; and
- an approved control allocation table listing the system security controls the component agrees to implement.

DHS has established an SA target of ensuring ATO for 100 percent of its high-value systems assets. The ATO target is 95 percent for other operational non-high value assets. However, our review of the August 2017 FISMA Scorecard for unclassified systems revealed that the following four components did not meet the SA target for high-value assets.

- Federal Emergency Management Agency (FEMA)
- Immigration and Customs Enforcement (ICE)
- National Protection and Programs Directorate (NPPD)
- United States Coast Guard (Coast Guard)

In addition, four components did not meet the SA target of 95 percent compliance for other operational non-high value assets.

- Headquarters
- Federal Law Enforcement Training Center (FLETC)
- ICE
- NPPD

Several components missed the SA target of 90 percent cited in the performance plan for national security systems. According to the Department's August 2017 FISMA Scorecard, three components (Headquarters, Coast Guard, and the Office of Chief Security Officer) failed based on not meeting ATO and contingency plan test metrics. Additionally, the Science and Technology Directorate (S&T) had a failing SA score for its stand-alone national security systems.

Our analysis of data from DHS' enterprise management systems showed that, as of June 30, 2017, 64 systems lacked ATOs. Specifically, 16 national security systems were operating without ATOs. In addition, 48 unclassified systems lacked ATOs—an improvement in comparison with 79 unclassified systems identified without ATOs in June 2016, and 203 reported for June 2015. Table 3 compares the number of unclassified systems, by component, operating without ATOs between June 2015 and 2017.

Table 3: Number of Unclassified Systems Operating without ATOs

Component	Number of Systems Operating Without ATO		
	FY 2015	FY 2016	FY 2017
Customs and Border Protection (CBP)	8	12	4
Headquarters	1	4	7
FEMA	111	15	15
FLETC	2	1	2
ICE	3	3	6
NPPD	15	10	6
S&T	12	3	2
Transportation Security Administration (TSA)	0	0	3
Coast Guard	35	6	2
United States Secret Service (Secret Service)	16	25	1
Total	203	79	48

Source: OIG-compiled based on our analysis of data obtained from DHS' unclassified enterprise management system

Our annual FISMA reports provide details regarding the number of DHS systems lacking ATOs in FYs 2015 and 2016.[3]

Our quality review of 10 SA packages at selected components identified the following deficiencies regarding component documentation to support ATO decisions.

- The Federal Information Processing Standards (FIPS) 199 security categorizations did not match information entered into the Department's enterprise management tool, security plan, and FIPS 199 worksheet.[4]

- Seven systems did not include the required appendices, such as incident response procedures, privacy handling was not within the defined timeframes.

[3] *Evaluation of DHS' Information Security Program for Fiscal Year 2015*, January 5, 2016, OIG-16-08 (Revised); and *Evaluation of DHS' Information Security Program for Fiscal Year 2016*, January 18, 2017, OIG-17-24.

[4] 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.

- Ten systems did not appropriately explain how controls were implemented in the security plan, including inherited and not applicable controls were not properly included or addressed in the security document.

- Six systems had issues where the security assessment results could not be tracked to the requirement traceability matrix of Security Assessment Plan.

- Ten systems did not have sufficient documentation to support controls that were tested.

According to its August 2017 action plan for implementing the NIST Cybersecurity Framework, DHS plans to enhance its SA process to obtain 100 percent ATO for high-value asset systems by December 2017. DHS cited a lack of qualified security engineers from the overall labor market as the foremost reason for components failing to meet the 95 percent SA metric for non-high value asset systems. DHS indicated this constraint may continue until cybersecurity becomes a common skillset across the Nation.

Weakness Remediation

FISMA mandates use of a POA&M as a corrective action plan for tracking and planning the resolution of information security weaknesses. The POA&M details resources required to accomplish the elements of the plan, any milestones for meeting the tasks, and scheduled completion dates for the milestones.[5]

We found that components did not effectively manage the POA&M process as required. For example, although components were required to update POA&Ms monthly, they did not always maintain complete and accurate information on progress in remediating security weaknesses. They did not timely resolve all POA&Ms within 6 months as required. They also did not always include estimates for resources needed to mitigate an identified weakness.

Our analysis of data from DHS' enterprise management system as of June 30, 2017, showed the following:

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

- Of the 5,228 open unclassified POA&Ms, 1,452 (28 percent) were past due. Moreover, 1,184 (82 percent) of the 1,452 past due POA&Ms were overdue by more than 90 days, while 531 (37 percent) were overdue by more than a year.

- Of the 1,452 overdue unclassified POA&Ms, 1,435 (99 percent) had weakness remediation estimated at less than $50, as required by DHS when costs could not be estimated due to the complexity of the task or other unknown factors.

Similarly, our quality review of 10 SA packages showed that all 10 systems had POA&Ms that were not mitigated within 30 days of the system obtaining ATO, and POA&Ms were not created for failed controls for 6 of the systems. Further, our analysis of the National Security Systems August 2017 FISMA Cybersecurity Scorecard revealed that Coast Guard and the Office of the Chief Security Officer had failing scores for weakness remediation through the POA&M process.

Protect

The "Protect" function entails developing and implementing the appropriate safeguards to ensure delivery of critical infrastructure services. We determined that DHS was operating at "Level 3 – Consistently Implemented" in this area, just below the targeted effective level. We based this rating on our assessment that DHS did not implement all configuration settings required to protect component systems, continued using unsupported operating systems, and did not apply security patches timely to mitigate critical and high-risk security vulnerabilities on selected systems.

Configuration Management

DHS requires that components configure their workstations according to United States Government Configuration Baseline (USGCB) settings. We tested three unclassified systems from FEMA, Headquarters, and Coast Guard for compliance with USGCB settings. Our testing revealed that components had not implemented all USGCB settings on all of the selected systems as required. The settings are necessary to secure the confidentiality, integrity, and availability of DHS' systems and the information they process and store. Table 4 summarizes components' compliance with USGCB settings for their Windows 7 workstations.

Table 4: USGCB Compliance by Component Systems

DHS Component	Windows 7 Workstations
Headquarters	98%
FEMA	98%
Coast Guard	99%

Source: OIG-compiled based on testing results

Some of the missing settings on the workstations tested related to the following:

- Exchange folders indexed in cache mode – This setting allows Microsoft Outlook to store a cached copy of a user's emails on the workstation. If the workstation is stolen or compromised, the user's emails could potentially be subject to unauthorized access.

- Registry auditing – This setting ensures that the Windows operating system maintains audit logs of when registry objects are accessed. Without this setting, changes may be made to the operating system configuration without proper attribution to a specific user.

- Anonymous access to the network shared drive – To prevent compromise of sensitive information, system administrators must disable this setting to restrict users from logging onto the network without credentials or passwords.

As part of our quality review of selected accreditation packages, we evaluated components' compliance with DHS Baseline Configuration settings on 10 judgmentally selected servers. We determined that components' compliance in implementing the required configuration settings on the servers ranged from:

- 80 to 94 percent on Windows 2008 servers,

- 91 to 96 percent on Windows 2012 servers, and

- 65 to 87 percent on UNIX/LINUX/AIX servers.

Unsupported Operating Systems

Known or new vulnerabilities can be exploited on operating systems for which vendors no longer provide service patches or technical support. DHS required that components discontinue the use of such unsupported operating systems

(e.g., Windows XP and Windows Server 2003). However, we identified the following instances where components continued to use unsupported operating systems, potentially exposing DHS data to unnecessary security risks:

- One Headquarters system still used an unsupported version of the Microsoft Windows 2003 server; Microsoft had stopped providing security updates and technical support for the server in July 2015. According to an official we interviewed, Headquarters was in the process of decommissioning the system.

- One Coast Guard system still used an unsupported version of the Windows 2003 server.

- One Secret Service system still used an unsupported version of the Windows 2003 server. According to an official, Secret Service had restricted system access to internal users only to reduce risks and planned to migrate the system to a different operating system.

Vulnerability Assessment Testing

Periodic scanning and assessment of critical systems is key to mitigating information security vulnerabilities. Per DHS Sensitive Systems Policy 4300A, components must manage systems to reduce vulnerabilities through testing, promptly installing patches, and eliminating or disabling unnecessary services. We performed vulnerability assessments on four selected systems to determine whether adequate security controls had been implemented. Table 5 summarizes by operating system the missing critical and high-risk patches we identified.

Table 5: Vulnerabilities Identified on Selected Operating Systems

Systems	Unique Critical Vulnerabilities	Unique High Vulnerabilities
DHS Headquarters Windows 7 Workstations	4	12
DHS Headquarters Windows 8.1 Workstations	5	0
FEMA Windows 7 Workstations	2	7
Coast Guard Windows 7 Workstations	0	4
Coast Guard Windows 2008/2012 Servers	2	4

Source: OIG-compiled based on system test results

Following are specific examples of the critical and high-risk vulnerabilities we detected.

- Windows 2008 and 2012 operating systems were missing security patches for Oracle Java, an unsupported version of Internet Explorer, and a vulnerable version of Microsoft's Sidebar and Gadgets applications. Some of the missing security patches dated back to July 2013. We also found that DHS components had not applied some critical patches announced in July 2016 Microsoft security bulletins for these operating systems.

- Several Windows 8.1 and Windows 7 workstations were missing key security patches, including those to protect against WannaCry ransomware that infected tens of thousands of computers in over 150 countries in May 2017. Other examples of missing patches include those associated with internet browsers such as Mozilla and Firefox, and media players such as Flash player and Adobe Shockwave. We identified additional Adobe Acrobat vulnerabilities on these workstations as well.

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. Such exploitation can result in significant data loss and system disruption, which hampers 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 logical access, as required by *Homeland Security Presidential Directive-12*.[6] DHS requires that all privileged and unprivileged employees and contractors use the cards to log onto DHS systems. Based on the August 2017 FISMA Scorecard:

[6] *Homeland Security Presidential Directive-12,* dated August 27, 2004, required Federal agencies to begin using the standard form of identification by November 2006 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.

- DHS was 99.5 percent compliant with PIV implementation for privileged users, and 99.4 percent compliant with PIV implementation for unprivileged users.

- Eight components had met the 100 percent compliance target for required PIV card use by both privileged and unprivileged users.[7]

- Coast Guard did not meet the Department's compliance target as the component had implemented the use of PIV cards for 96.4 percent for privileged users.

According to the Department's August 2017 action plan for implementing the NIST Cybersecurity Framework, the 100 percent target for compliance in using the PIV card for logical access was not efficient for DHS business operations. As such, DHS indicated the need to revise the PIV-compliant metric to make it more achievable.

Security Training Program

Educating employees on acceptable practices and rules of behavior is critical for an effective information security program. DHS' multi-tiered Security Training program is collaboratively managed by Headquarters, the Office of the Chief Human Capital Officer, and the components. The Department's Performance and Learning Management System tracks employee completion of training, including security awareness training. Components are required to ensure that all employees and contractors annually receive IT security awareness training, including specialized training for employees with significant responsibilities.

However, neither DHS nor its components obtain feedback to ensure adequacy of the IT security awareness training provided. In May 2016, the DHS Chief Information Security Officer established the DHS Information Security Training Working Group, comprising representatives from the Department and components, to promote security awareness by sharing information on training activities, and developing and updating course material. DHS uses the Working Group as a means of obtaining feedback from its members on the effectiveness of its security awareness training material; however, it does not obtain feedback directly from course participants through such means as a training questionnaire. Obtaining feedback from the larger user audience would allow

[7] The eight components that were 100 percent compliant were Headquarters, FEMA, ICE, NPPD, OIG, S&T, TSA, and Secret Service.

DHS to gather more in-depth suggestions and ideas for improving and enhancing the course materials.

According to program officials that we interviewed, DHS also has not assessed the knowledge, skills, and abilities of its cyber workforce. Lacking such an assessment, DHS cannot assure that its employees possess the knowledge and skills necessary to perform their various job functions, or that qualified personnel are hired to fill cybersecurity-related positions. As previously stated, DHS cited a lack of qualified security engineers from the overall labor market as the foremost reason for components failing to meet its SA metric.

Detect

The "Detect" function entails developing and implementing the appropriate activities to identify the occurrence of a cybersecurity event. We determined that DHS 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 maintain software licenses for unclassified systems, and relied on data calls to monitor national security systems as part of its continuous monitoring process to detect potential incidents.

ISCM is a principal means for DHS program officials to gain visibility into network resources, maintain knowledge and awareness of security threats and vulnerabilities, and ensure effectiveness of implemented controls. DHS implemented the ISCM strategy for its unclassified systems, emphasizing FISMA reporting through direct data feeds from a security management tool. The ISCM strategy supports visibility into assets, and program officials' awareness of threats, vulnerabilities, and mission/business impacts through the DHS Monthly Executive Scorecard and daily ISCM reports. However, the current ISCM Strategy is dated May 2014 and does not address the monitoring of software licenses. Further, DHS has not updated its ISCM Strategy to address evolving cybersecurity risks since it was issued in May 2014. DHS also lacks an automated process to maintain software license information, including license expiration dates. Because the components individually maintain software license information, DHS obtains this information through annual data calls or when the software licenses are close to expiration.

DHS also relies on data calls to components for visibility into its national security systems, instead of using the enterprise management tool that creates SA artifacts for monitoring and authorizing each system. Using the data call information, DHS prepares monthly scorecards for its national security systems. Our analysis of the data obtained from the enterprise management tool revealed that components did not include in the tool estimated resource requirements for mitigating security weaknesses through POA&Ms, as required

by applicable Office of Management and Budget and DHS policy. In addition, the tool lacked the capability to determine whether system contingency plans were tested as required. Nonetheless, three components (FEMA, OIG, and TSA) received 100 percent scores for contingency plan testing, and five components (Headquarters, FEMA, TSA, S&T, and OIG) received perfect scores for weakness remediation in DHS' June 2017 national security systems scorecard. The discrepancies are indicators that the classified enterprise management tool and the national security systems scorecard may not contain the most accurate information for management officials to make credible risk-based decisions.

On September 9, 2017, DHS updated its Ongoing Authorization program methodology to include a requirement that components participating in the program utilize the unclassified enterprise management tool to store all security documentation. The Department had increased the number of systems participating in the Ongoing Authorization program, from 82 systems in FY 2015, to 96 systems in FY 2016, and to 130 systems from eight components in August 2017. The eight components were Headquarters, CBP, FLETC, ICE, OIG, S&T, TSA, and USCIS.

Respond

The "Respond" function entails developing and implementing the appropriate activities to take action regarding a detected cybersecurity event. We determined that DHS was operating effectively at the targeted "Level 4 – Managed and Measurable" in this area. We based this rating on Security Operations Center actions to address cybersecurity incidents according to DHS policy.

Given agencies' increased reliance on computer resources to accomplish their missions, incident response has become a vital part of an effective information security program. 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 has 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 that components comply with applicable Federal and DHS security policy and corresponding controls. The DHS Security Operations Centers provide situational awareness, serve as central data repositories, and facilitate reporting and coordination regarding computer security incidents across the Department.

The "Respond" function supports agencies' ability to contain the impact of a potential cybersecurity event, as well as coordinate response activities with internal and external stakeholders, including support from external law enforcement agencies. Specifically, FISMA requires agencies to develop procedures for detecting, reporting, and responding to security incidents. For major security incidents, agencies are required to submit reports to the Congress within the required timeframe.

From our review of 10 selected accreditation packages, we determined that DHS components did not report all security incidents to the Security Operations Centers as required. Specifically, we identified three systems that had each experienced a security event that was not reported within 48 hours as required.[8] When reporting is delayed, the Security Operations Centers may not have all the information needed to address suspicious activity or security event as quickly as possible and thereby minimize potential impact.

Recover

The "Recover" function entails developing and implementing plans for resiliency and restoration of any capabilities or services impaired due to a cybersecurity event. Because information systems and resources are so vital to agencies to accomplish their missions, it is critical that DHS minimize the impacts of interruptions to its operations without extensive outages, in the event of emergencies. We determined that DHS' Identify 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 test all system contingency plans, develop procedures for handling sensitive information, or identify alternate facilities to recover processing in the event of service disruptions.

The Department maintained an entity-wide business continuity and disaster recovery program. As part of this program, DHS implemented a Reconstitution Requirements Functions Worksheet to collect components' key business requirements and capabilities needed in the event of an attack or disaster. DHS used this information to develop a Reconstitution Plan that outlines procedures at a macro level for all of the Department's senior leadership, staff, and components to follow to resume normal operations as quickly as possible in the event of an emergency. The procedures for resuming operations may involve both manual and automated processing at alternate locations as appropriate.

[8] Per *Government Auditing Standards*, we do not report on OIG operations; however, for the sake of full disclosure, an OIG data breach was identified in 2017 as part of an ongoing investigation. OIG reported the breach to Congress according to FISMA requirements.

DHS components are responsible for developing and periodically testing corresponding contingency plans that outline backup and disaster recovery procedures for their respective information systems.

Our analysis of DHS' unclassified enterprise management tool revealed that components had not tested contingency plans for 19 systems. Further, as part of our quality of review of accreditation packages for 10 selected systems, we determined the following:

- For two systems with FIPS-199 high or moderate availability, components did not include disaster recovery procedures for managing sensitive information at alternate or offsite facilities in their contingency plans, as required.

- For two systems with FIPS-199 high availability, data backup, data recovery, and notification tests had not been performed for more than a year. Components are required to conduct such tests every 12 months.

Conclusion

In three of five areas, DHS fell one level below the targeted "Level 4" defined in the FY 2017 FISMA reporting guidance as achieving effectiveness in information security. The DHS Chief Information Security Officer is centrally responsible for coordinating with other senior agency officials to manage the Department's information security program for its unclassified and national security systems. Based on this year's FISMA results, additional oversight is needed for the Department to improve in ensuring that components comply with Federal and DHS information security policy.

Specifically, since the Department's inception in 2003, components have not effectively managed and secured their information systems. Components have continued to operate systems without ATOs, used unsupported operating systems that expose DHS data to unnecessary risks, ineffectively managed the POA&M process to mitigate identified security weaknesses, and failed to apply security patches timely. Such repeated deficiencies are contrary to the President's Cybersecurity Executive Order and clear indicators that departmental oversight of the enterprise-wide information security program needs to be strengthened. Until DHS overcomes challenges to addressing its systemic information security weaknesses, it will remain unable to ensure that its information systems adequately protect the sensitive data they store and process.

Recommendations

We recommend that the DHS Chief Information Security Officer:

Recommendation #1: Pursue with the Under Secretary for Management alternate strategies for ensuring that components accomplish planned actions to address deficiencies in areas such as security authorization, weakness remediation, and continuous monitoring that have consistently lagged behind in key performance metrics on the monthly information scorecard.

DHS Comments to Recommendation 1

DHS concurred with recommendation 1. The Chief Information Security Officer had already implemented the Deputy Under Secretary for Management's quarterly cybersecurity review process to receive updates from the Department's senior executives regarding remedial actions to improve components' information security programs. The quarterly review process remains ongoing in FY 2018. The Chief Information Security Officer will pursue additional strategies for ensuring compliance with planned actions to address deficiencies in areas such as security authorization, weakness remediation, and continuous monitoring. The estimated completion date for these actions is September 30, 2018.

OIG Analysis of DHS Comments

We believe that the steps DHS has taken satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

Recommendation #2: Enforce the requirements for components to obtain authority to operate, test contingency plans, and apply sufficient resources to mitigate security weakness for national security systems according to applicable policies.

DHS Comments to Recommendation 2

DHS concurred with recommendation 2. In 2017, the Chief Information Security Officer published the annual "National Security Systems Cybersecurity Performance Plan" to communicate requirements, priorities, and overall DHS information security goals for national security systems. The Chief Information Security Officer will continue to enforce ATO requirements, test contingency plan requirements, and apply sufficient resources to mitigate

weaknesses for the national security systems. The estimated completion date for these actions is September 30, 2018.

OIG Analysis of DHS Comments

We believe that the steps DHS has taken satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

Recommendation #3: Revise the information systems continuous monitoring strategy to include an up-to-date inventory of software assets and licenses used within the Department.

DHS Comments to Recommendation 3

DHS concurred with recommendation 3. The Chief Information Security Officer is in the process of updating the Department's "Information Systems Continuous Monitoring Strategy." As part of the strategy, DHS is implementing the continuous diagnostics and mitigation solution across the enterprise. Once fully implemented, the solution will continuously and systemically inventory assets on DHS' network and track software licenses. The Department will monitor each software asset identified until its ultimate disposal. The estimated completion date for these actions is September 30, 2018.

OIG Analysis of DHS Comments

We believe that the steps DHS has taken satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

Recommendation #4: Implement controls and perform quality reviews to validate that information security data input to DHS' enterprise management systems is complete and accurate.

DHS Comments to Recommendation 4

DHS concurred with recommendation 4. DHS agreed that internal controls and quality reviews must be in place to ensure that the data in enterprise management systems are complete and accurate. The Department has already implemented actions to achieve this outcome based on similar findings from prior OIG reports.

OIG Analysis of DHS Comments

We believe that the steps that DHS has taken satisfy the intent of this recommendation. We consider this recommendation resolved and closed.

Recommendation #5: Expedite the process for discontinuing the use of unsupported operating systems within the Department.

DHS Comments to Recommendation 5

DHS concurred with recommendation 5. The Chief Information Security Officer has published a policy requiring components to discontinue the use of unsupported operating systems; however, there are complicating factors regarding discontinuing the use of some of these systems. Using a risk-based approach and mitigating controls, the Chief Information Security Officer will continue working with DHS components to discontinue use of the unsupported operating systems, as appropriate. The Chief Information Security Officer also tracks the removal of unsupported operating systems and reports the results on the monthly FISMA scorecards. The Chief Information Security Officer will continue to provide status reports to the Deputy Under Secretary for Management and component leadership at quarterly meetings. The estimated completion date for these actions is September 30, 2018.

OIG Analysis of DHS Comments

We believe that the steps DHS has taken satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

Appendix A
Objective, Scope, and Methodology

DHS 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 are adequate and effective. Our independent evaluation focused on DHS' information security program based on the requirements outlined in FY 2017 IG FISMA Reporting Metrics. Specifically, we evaluated DHS' Information Security Programs' compliance with applicable requirements outlined in the five NIST Cybersecurity Functions.

We performed our fieldwork at the DHS Office of the Chief Information Officer and at organizational components and offices, including Headquarters, CBP, FEMA, ICE, NPPD, TSA, Coast Guard, USCIS, and Secret Service. To conduct our evaluation, we interviewed selected 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 2016 FISMA evaluation as a baseline for the FY 2017 evaluation;
- evaluated policies, procedures, and practices that 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 to evaluate the effectiveness of controls implemented on four systems. We also tested DHS' compliance with applicable USGCB settings on selected workstations.

Further, we performed quality reviews on 10 SA packages at Headquarters, CBP, FEMA, USCIS, NPPD, S&T, TSA, and Coast Guard 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 DHS' baseline configuration settings were implemented as required. We also evaluated whether components performed continuous monitoring on their systems and networks, including systems operated by contractors or other entities on DHS' behalf.

We conducted this review between March and October 2017 under the authority of the *Inspector General Act of 1978*, as amended, and in accordance with 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. We included OIG data for informational and comparison purposes only.

Appendix B
Management Comments to the Draft Report

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

Homeland Security

February 1, 2018

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

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

SUBJECT: Management's Response to OIG Draft Report: "Evaluation of DHS' Information Security Program for Fiscal Year 2017" (Project No. 17-061-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 report documents significant and continued improvements in the DHS Chief Information Security Officer's (CISO) efforts to improve the Information Security Program. For example, the CISO has reduced the number of unclassified systems operating without a current authority to operate by nearly 75 percent since FY 2015. DHS remains committed to ensuring its information systems adequately protect the sensitive data they store and process.

The draft report contained five 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. 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 17-061-ITA-DHS

The OIG recommended that the DHS Chief Information Security Officer:

Recommendation 1: Pursue with the Under Secretary for Management [USM] alternate strategies for ensuring that components accomplish planned actions to address deficiencies in areas such as security authorization, weakness remediation, and continuous monitoring that have consistently lagged behind in key performance metrics on the monthly information scorecard.

Response: Concur. In 2016, DHS Office of the Chief Information Officer's (OCIO) Office of the Chief Information Security Officer (OCISO) implemented the Quarterly Deputy Under Secretary for Management (DUSM) Cybersecurity Review process to receive updates from the Department's senior executives regarding remedial actions and resolve impediments to improving Components' information security programs. The Quarterly DUSM Cybersecurity Review process continued through FY 2017 and is ongoing in FY 2018. This process is working well and has driven rapid improvement. OCISO will pursue, with the USM, additional strategies for ensuring compliance with planned remedial actions to address deficiencies in areas such as security authorization, weakness remediation, and continuous monitoring. Estimated Completion Date (ECD): September 30, 2018.

Recommendation 2: Enforce the requirements for components to obtain authority to operate [ATO], test contingency plans, and apply sufficient resources to mitigate security weakness for national security systems according to applicable policies.

Response: Concur. In 2017, The DHS OCISO published the annual DHS National Security Systems Cybersecurity Performance Plan to communicate requirements, priorities and overall Departmental Information Security goals for national security systems. OCISO will continue to enforce ATO requirements, test contingency plan requirements, as well as apply sufficient resources to mitigate weaknesses for NSS systems. ECD: September 30, 2018.

Recommendation 3: Revise the information systems continuous monitoring strategy to include an up-to-date inventory of software assets and licenses used within the Department.

Response: Concur. OCISO is in the process of updating its Information Systems Continuous Monitoring strategy. As part of its ISCM strategy, DHS is implementing the Continuous Diagnostics and Mitigation (CDM) solution across the enterprise with the expectation that CDM will be fully functional within all Components by September 30, 2018. This is a collaborative effort being carried out by the system owner (DHS CISO), the implementer (DHS Program Management Office), and each DHS Component CISO. As the CDM solution comes online, it will continuously and systematically inventory assets in the DHS environment and track software licensing within the governance module of the CDM tool suite. Each software asset identified will have an assigned individual responsible for maintaining its status and disposition. After successful implementation of the DHS CDM program OCISO also will be able to expedite the scan results frequency from the components and report any violations to the DUSM, as needed. ECD: September 30, 2018.

2

Recommendation 4: Implement controls and perform quality reviews to validate that information security data input to DHS' enterprise management systems is complete and accurate.

Response: Concur. The DHS CIO agrees that internal controls and quality reviews must be in place to ensure that data in enterprise management systems is complete and accurate. DHS OCIO has already implemented actions to achieve this outcome, in response to a similar recommendation (Recommendation 5) contained in OIG-16-08 Revised, "Evaluation of DHS' Information Security Program for Fiscal Year 2015," dated January 5, 2016. On January 18, 2018, OIG formally advised that it considered this recommendation "resolved and closed" based on the actions that the Department had taken to address the recommendation and the results of testing conducted during this FY 2017 review. Therefore, we request that OIG consider this recommendation resolved and closed.

Recommendation 5: Expedite the process for discontinuing the use of unsupported operating systems within the Department.

Response: Concur. The OCISO has published policy that requires components to discontinue the use of unsupported Operating Systems (OS). The DHS 4300A, "Sensitive Systems Policy Handbook" states, "only licensed and approved operating systems and applications may be used on DHS workstations." However, there are complicating factors around discontinuing the use of some of these systems. Using our risk-based approach and mitigating controls, OCISO will continue working with the Components to discontinue unsupported OS for both the mission and security needs, as appropriate. The DHS OCISO also tracks the removal of unsupported OS and reports the results on the monthly Federal Information Security Management Act Scorecard. OCISO will continue to report the status to the DUSM and Component leadership at quarterly meetings. ECD: September 30, 2018.

3

Appendix C
Office of Information Technology Audits Major Contributors to This Report

Chiu-Tong Tsang, Director
Brandon Barbee, IT Audit Manager
Thomas Rohrback, Chief, Information Assurance and Testing
Jasmine Raeford, IT Specialist
Ann Brooks, IT Auditor
Mahfuza Khanam, IT Auditor
Dave Bunning, IT Specialist
Hoa Do, IT Specialist
Beverly Dale, 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, USCIS, NPPD, S&T, TSA, USCG, 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