OFFICE OF INSPECTOR GENERAL

Evaluation of DHS' Information Security Program for Fiscal Year 2016

Homeland Security

DHS OIG HIGHLIGHTS

Evaluation of
DHS' Information Security Program
for Fiscal Year 2016

Why We Did This Evaluation

We reviewed the Department of Homeland Security's (DHS) information security program in accordance with the *Federal Information Security Modernization Act of 2014*. Our objective was to determine whether DHS' information security program is adequate, effective, and complies with FISMA requirements.

What We Recommend

We recommended that DHS further strengthen its oversight of the Department's information security program in the areas of continuous monitoring, plan of action and milestones, security authorization, 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

DHS has taken actions to strengthen its information security program. For example, in January 2016, the Under Secretary for Management issued a memorandum requiring Components to enhance DHS' Cyber Defense by providing security training and exercises to employees and contractors, and implementing endpoint protection solutions and two-factor authentication on DHS' classified network. The Components have made significant progress in remediating security weaknesses identified, compared to the same period last year. Further, as of May 2016, all Components were reporting information security metrics to the Department, enabling DHS to better evaluate its security posture.

Despite the progress made, Components were not consistently following DHS' policies and procedures to maintain current or complete information on remediating security weaknesses timely. Components operated 79 unclassified systems with expired authorities to operate. Further, Components had not consolidated all internet traffic behind the Department's trusted internet connections and continued to use unsupported operating systems that may expose DHS data to unnecessary risks. We also identified deficiencies related to configuration management and continuous monitoring. Without addressing these deficiencies, the Department cannot ensure that its systems are adequately secured to protect the sensitive information stored and processed in them.

DHS Response

We made four recommendations to the Chief Information Security Officer. The Department concurred with all four recommendations.
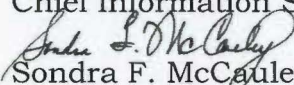
January 18, 2018

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 2016*

Attached for your action is our final report, *Evaluation of DHS' Information Security Program for Fiscal Year 2016*. We incorporated the formal comments from the Director, Departmental GAO-OIG Liaison Office, in the final report.

The report contains four recommendations aimed at improving the Department's information security program. The Department concurred with all four recommendations. Based on information provided in the Department's response to the draft report, we consider recommendations 1, 2, 3 and 4 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions. 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

Table of Contents

Appendixes

Abbreviations

ATO	authority to operate
CBP	Customs and Border Protection
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FLETC	Federal Law Enforcement Training Center
FY	fiscal year
ICE	Immigration and Customs Enforcement
ISCM	Information Security Continuous Monitoring
ISO	Information Security Office
IT	information technology
NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
OA	Ongoing Authorization
OCISO	Office of CISO
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	personal identity verification
POA&M	plan of action and milestones
S&T	Science and Technology
SA	security authorization
SOC	Security Operations Center
TSA	Transportation Security Administration
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Services
USGCB	United States Government Configuration Baseline
USSS	United States Secret Service

Background

Recognizing the importance of information security to the economic and national security interests of the United States, the Congress enacted the *Federal Information Security Modernization Act of 2014* (FISMA) to improve security within the Federal Government. Information security involves protecting information 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 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. As required by FISMA, each agency must develop, document, and implement an agency-wide security program. The security program should protect the information 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 security policies and procedures. FISMA requires that each agency Chief Information Officer, in coordination with senior agency officials, report annually to the agency head on the effectiveness of the information security program, including progress on remedial actions. The Office of Inspector General (OIG), or an independent external auditor designated by OIG, must independently evaluate the effectiveness of the agency's information security program and practices each year. Our report this year summarizes the results of our evaluation of the Department's information security program based on the FISMA reporting metrics dated September 26, 2016.[1]

The Chief Information Security Officer (CISO), who heads the Information Security Office (ISO), manages the DHS' information security program for its unclassified systems, as well as those classified as "Secret" and "Top Secret." To aid in managing the program, CISO developed the *Fiscal Year 2016 DHS Information Security Performance Plan.* CISO leverages operational efficiency to defend against evolving threats and maintains ongoing awareness of the Department's information security program, vulnerabilities, and potential threats through the execution of three programs: (1) Information Security Continuous Monitoring (ISCM) Data Feeds, (2) Ongoing Authorization (OA),

---

[1] *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, Version 1.1.3, September 26, 2016.

and (3) DHS Security Operations Center (DHS SOC). DHS relies on two enterprise management systems to create and maintain security authorization (SA) documentation and monitor plan of action and milestones (POA&M) activities for its unclassified and "Secret"-level systems.[2]

On July 22, 2015, in response to cyber-attacks on the Federal Government, the Under Secretary for Management issued a memorandum requiring DHS and its Components to strengthen their cyber defenses. Components were to implement the following cybersecurity infrastructure measures within 30 days:

- consolidate all of DHS' internet traffic behind the Department's trusted internet connections,
- implement strong authentication through the use of personal identity verification (PIV) cards for all privileged and unprivileged access accounts,
- achieve 100 percent SA compliance for systems identified by the Component as high value assets and 95 percent compliance for the remaining systems, and
- retire all discontinued operating systems and servers (e.g., Windows XP and Windows Server 2000/2003).

To further enhance the Department's cyber defense, the Under Secretary for Management issued a memorandum on January 13, 2016, requiring Components to take the following actions to protect their networks and educate their employees within 45 days: [3]

- establish the capability to perform searches for compromise indicators within 24 hours of detected suspicious network activity,
- remove users' administrative privileges on workstations connected to the networks, and
- require two-factor authentication for all users accessing the Department's Homeland Secure Data Network.[4]

---

[2] The National Institute of Standards and Technology (NIST) defines SA as the management decision by a senior organizational official to authorize operation of an information system and to explicitly 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.

[3] Under Secretary for Management Memorandum, *Continuous Improvement of Department of Homeland Security Cyber Defenses*, January 13, 2016.

[4] The Homeland Secure Data Network is a classified wide-area network for DHS and its Components, with specific and controlled interconnections to intelligence community and Federal law enforcement resources.

Components were further required to take the following actions within 60 days:

- provide additional instruction as part of the annual security awareness training to educate users on phishing and its prevention. Employees and contractors who had not completed the training within the required timeframe were to have their network accounts disabled,
- establish programs to raise employee awareness about the threat of social engineering. The programs were to include requirements to conduct semi-annual tests and spear-phishing exercises for all privileged users, all users of high-valued assets, and a representative sample of the remaining population, and
- implement technology (i.e., Initial Operational Capability) to prevent the activation of malicious links or attachments in phishing emails.

Finally, Components were to implement solutions (i.e., Full Operational Capability) to prevent the activation of malicious links or attachments in phishing emails within 90 days of issuance of the Under Secretary for Management's memo.

Results of Evaluation

We conducted an independent evaluation of DHS' information security program and practices to comply with FISMA requirements. To determine DHS' progress in implementing its agency-wide information security program, we specifically assessed the Department's configuration management, POA&Ms, SA processes, and continuous monitoring programs.

In fiscal year (FY) 2016, DHS took steps to enhance its information security program. For example, the Department updated its enterprise-wide information security policies and procedures for its unclassified systems.[5] Further, the Under Secretary for Management issued a memorandum on January 13, 2016, requiring Components to improve network security through security training and exercises, endpoint protection solutions, and two-factor authentication on DHS' classified network.[6]

While improvements have been made, the Department can strengthen its oversight of its information security program. For example, DHS ISO did not issue the *Fiscal Year 2016 Information Security Performance Plan* until

---

[5] *DHS Sensitive Systems Policy Directive 4300A,* Version 12.01, dated February 12, 2016, *DHS 4300A Sensitive Systems Handbook,* Version 12.0, dated November 15, 2015.
[6] Under Secretary for Management Memorandum, *Continuous Improvement of Department of Homeland Security Cyber Defenses, January 13, 2016.*

June 2016, nearly 3 months before the end of the fiscal year. This plan, which serves as a roadmap for future initiatives, is needed to define performance requirements, priorities, and overall goals for the Department throughout the year. Further, while DHS began to collect system information and maintain monthly scorecards for its "Secret" systems in FY 2016, the Department has yet to issue a performance plan to establish the metrics, reporting requirements and the overall goals for these specific systems.

DHS Components are continuing to operate information systems without authorities to operate (ATO). Our review also identified deficiencies related to POA&Ms, configuration management, continuous monitoring, and contingency planning. Without addressing these deficiencies, the Department cannot ensure that its systems are properly secured to protect the sensitive information stored and processed in them.

Details

We focused on 10 key areas of DHS' information security program for its unclassified, "Secret", and "Top Secret" systems. Specifically, we reviewed the Department's:

- system inventory,
- risk management program,
- POA&Ms program,
- configuration management,
- incident response and reporting program,
- security training program,
- remote access program,
- identity and access management program,
- continuous monitoring program, and
- contingency planning program.

We identified the progress made in these key areas since our FY 2015 evaluation, along with issues DHS still needs to address.

System Inventory

DHS maintained and updated its FISMA system inventory, including agency and contractor systems, on an annual basis. In addition, DHS conducted site visits as part of its annual inventory refresh process to engage directly with

Component personnel, identify new systems, and resolve other inventory issues.

Progress

- DHS updated its *FISMA System Inventory Methodology* guidance in April 2016 to reflect the Department's latest guidance regarding systems inventory management.[7]

- DHS requires that Components identify and report their hardware assets monthly to establish a Department-wide inventory. As of August 2016, 11 of 12 Components had met or exceeded the Department's target of 95 percent for hardware asset reporting on DHS' monthly information security scorecard.

Issues To Be Addressed

- DHS required Components to report all software assets within their organizations as part of their ISCM programs. However, as of August 2016, 5 of 12 Components [Customs and Border Protection (CBP), National Protection and Programs Directorate (NPPD), Transportation Security Administration (TSA), United States Coast Guard (USCG), and United States Secret Service (USSS)] had not met the Department's target (95 percent) for software asset management.

See Appendix L, Status of Agency Program to Oversee Contractor Systems, for additional information.

Risk Management Program

The SA is a formal management decision by a senior official to authorize operation of an information system and 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.[8] The SA process provides an approach for assessing security controls (e.g., operational, technical, and management controls) to determine their overall effectiveness. DHS requires Components to use enterprise management systems to incorporate NIST security controls when performing SA on their systems. Enterprise-wide management systems enable Components to develop and

---

[7] *DHS FISMA System Inventory Methodology,* Version 13.6, April 29, 2016.
[8] *DHS Security Authorization Process Guide,* Version 11.1, March 16, 2015.

maintain system security documentation, as well as centralize documents supporting the ATO for each system.

Components use DHS enterprise management tools to create SA artifacts for monitoring and authorizing their systems. 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.

In October 2013, DHS began to allow Components to enroll in the Ongoing Authorization (OA) program. Each component is required to have a strong ISCM process, approved common controls, a designated OA manager, and a chartered operational risk management board for admission to the program. In addition, Components must maintain SA and weakness remediation metrics above 80 and 60 percent, respectively. Once a Component is accepted into the OA program, individual systems must meet the following requirements so that each system can also be entered into the program:

- Component OA program acceptance letter,
- OA system admission letter,
- OA recommendation letter,
- system ATO expiration more than 60 days beyond submission date,
- information system security officer with responsibilities primarily related to information assurance/security,
- information system security officer trained on OA processes, and
- an approved control allocation table.

Progress

- As of August 2016, 3 of 12 Components [Federal Law Enforcement Training Center (FLETC), OIG, and United States Citizenship and Immigration Services (USCIS)] had met the Department's SA target of 100 percent for high-value assets and mission-essential systems. In addition, 5 of 12 Components (Immigration and Customs Enforcement (ICE), OIG, Science and Technology (S&T),

TSA, and USCIS) had exceeded the Department's SA target of 95 percent for all other systems covered by FISMA.

Issues To Be Addressed

- DHS adopted two enterprise management systems to manage and track the SA process for its unclassified and "Secret" systems. During our evaluation, we identified the following inaccuracies associated with the unclassified enterprise management system:

  ➢ As of August 2016, NPPD and USSS were failing the Department's SA metrics for the components' unclassified systems for both high-value assets and remaining systems. DHS requires Components to achieve 100 percent and 95 percent compliance, respectively. We reported a similar finding for USSS in FY 2015. [9]

  ➢ As of July 2016, Headquarters had a failing SA score for its national security systems, which consisted of three different metrics: ATO, contingency plan tested, and POA&M management.

  ➢ As of June 2016, DHS had 79 unclassified systems operating without ATOs, compared to 203 in FY 2015. We reported similar findings for the same components in FY 2015.[10] Figure 1 illustrates the number of unclassified systems, by Component, operating without ATOs in June 2015 and June 2016.

Figure 1: Number of Systems Operating without ATOs

Component	Number of Systems Operating Without ATO	
	FY 2015	**FY 2016**
CBP	8	12
Headquarters	1	4
FEMA	111	15
FLETC	2	1
ICE	3	3
NPPD	15	10
S&T	12	3
USCG	35	6
USSS	16	25
Total	**203**	**79**

Source: OIG-compiled based on data from DHS' enterprise management systems.

---

[9] Under Secretary for Management Memorandum, *Strengthening DHS Cyber Defenses*, July 22, 2015.
[10] *Evaluation of DHS' Information Security Program for Fiscal Year 2015*, January 5, 2016, OIG-16-08 (Revised).

- Based on our quality review of 10 SA packages at selected Components, we identified the following deficiencies:

  ➢ NIST 800-53 annual self-assessments had not been completed for six systems.
  ➢ System security plans for six systems did not include all required security controls based on their systems categorization.
  ➢ System security plans for five systems did not describe the process for emergency configuration management changes.
  ➢ FIPS 199 artifacts for three systems were either improperly categorized or had missing information.

Appendix C, Status of Risk Management Program, provides summary information.

Plan of Action and Milestones Program

DHS requires the creation and maintenance of POA&Ms for all known information security weaknesses. A POA&M must detail the resources required to accomplish the elements of the plan, any milestones for meeting the tasks, and the scheduled completion dates for the milestones. DHS ISO tracks POA&M remediation as part of the monthly FISMA Scorecard, which measures key aspects of POA&M effectiveness. In addition, DHS ISO assists Components through POA&M reviews and site visits. Despite these efforts, Components did not enter and track all information security weaknesses in DHS' unclassified and classified enterprise management systems as required.

Progress

- Components had made significant progress in remediating POA&Ms compared to the previous year. For example, as of June 2016, DHS had 6,427 open unclassified POA&Ms, as compared with 22,294 POA&Ms in the same period in FY 2015.

Issues To Be Addressed

- Components did not maintain current or complete information on progress in remediating security weaknesses and did not resolve all POA&Ms in a timely manner. DHS requires Components to complete POA&M remediation within 6 months. Without adequate POA&M information, authorizing officials lacked the most current

information on their systems and could not determine whether known weaknesses were properly remediated. As of June 2016, we identified the following deficiencies in the Department's unclassified enterprise management system:

> ➢ Of 6,427 open unclassified POA&Ms, 2,895 (45 percent) were overdue. Moreover, 2,484 of these open POA&Ms were at least 3 months late while 1,728 POA&Ms were more than a year past due.
> ➢ Of the 2,895 open overdue unclassified POA&Ms, 2,669 (92 percent) had weakness remediation estimates less than $50. DHS requires that Components provide a nominal estimate of $50 to mitigate known weaknesses where a cost could not be estimated due to the complexity of the task or unknown factors.

- DHS ISO was not tracking the quality of POA&Ms for its national security systems.

Appendix G, Status of Plan of Action and Milestones Program, provides summary information.

Configuration Management

We selected eight general support systems from CBP, Federal Emergency Management Agency (FEMA), NPPD, TSA, USCG, and USSS to evaluate the Components' compliance with United States Government Configuration Baseline (USGCB) and DHS baseline configuration settings. We included a mix of unclassified and "Secret" systems in our testing.

Progress

- Three specialized equipment used Windows XP at TSA. Microsoft had stopped providing security updates and technical support for Windows XP in April 2014, which could lead to unidentified and unpatched vulnerabilities for these older operating systems. Subsequent to our testing, TSA personnel informed us that they had removed the equipment from the Component's network.

- Our test results revealed that Components had made improvements in implementing USGCB settings, which is the core set of security related configuration settings that all agencies must

implement or document any deviations. Figure 2 summarizes Components' Windows 7 workstation USGCB compliance.

Figure 2: USGCB Compliance for Windows 7 Operating Systems

Component/System	Windows 7
CBP System #1	98%
CBP System #2	94%
FEMA System #1	95%
FEMA System #2	100%
NPPD	95%
TSA	97%
USCG	91%
USSS	97%

Source: OIG-compiled based on testing results.

Issues To Be Addressed

- The results of our testing revealed that Components had implemented all USGCB settings on only one of eight systems tested. When fully implemented, these settings help secure the confidentiality, integrity, and availability of DHS' information and systems.

- DHS requires that Components discontinue the use of unsupported operating systems (e.g., Windows XP and Windows Server 2000/2003).[11] We identified the following instances, in which Components continued to use unsupported operating systems, potentially exposing DHS data to unnecessary security risks:
  - ➢ One Headquarters classified server still used a Windows Server 2003, for which Microsoft had stopped providing security updates in July 2015. According to a program official, Headquarters was in the process of migrating the server to a different operating system.

---

[11] Under Secretary for Management Memorandum, *Strengthening DHS Cyber Defenses*, July 22, 2015.

Server Compliance with DHS Baseline Configuration Settings

- We evaluated approximately 300 configuration settings on Windows 2008 servers. Overall, Components had implemented about 74 percent of the DHS baseline configuration settings on the servers tested.

- We evaluated 100 configuration settings on Unix servers. Our testing revealed that only 65 percent of the configuration settings evaluated met the DHS baseline requirements.

Vulnerability Assessments of Selected Systems

We performed vulnerability assessments on eight systems at six Components to determine whether adequate security controls had been implemented on these systems. Our assessments revealed the following deficiencies.

- Several servers running Windows 2008 and 2012 operating systems were missing security patches for Oracle Java, antivirus software, an unsupported version of Internet Explorer, and Microsoft XML Parser and Core Services that Microsoft no longer supported since April 2014. Microsoft considers some of the missing patches to be high-risk and should have been fixed dating back to August 2012, while other missing critical patches should have been mitigated dated back to January 2014.

- Some of the Windows 8.1 and 7 workstations tested were missing security patches for Internet browsers (e.g., Internet Explorer, Firefox), media players (e.g., Flash Player, QuickTime), and Microsoft Office products. Some of the missing high-risk patches dated back to March 2011, while missing critical patches dated back to February 2013. We found additional vulnerabilities regarding Adobe Acrobat, Adobe Reader, and Oracle Java software on Windows 7 workstations. If exploited, these vulnerabilities could allow unauthorized access to DHS data.

See Appendix D, Status of Configuration Management Program, for more information.

Incident Response and Reporting Program

The Department operates the DHS SOC and the Homeland Secure Data Network SOC to ensure that unclassified and "Secret" information technology (IT) resources are secure. SOCs are also responsible for ensuring compliance with security policy and controls Department-wide. DHS SOC provides situational awareness, serves as a central data repository, and facilitates reporting and coordination regarding computer security incidents across the Department.

> Appendix E, Status of Incident Response and Reporting Program, provides additional information.

Security Training Program

Components are required to maintain and provide IT security training to all employees as part of their respective training programs. IT training consists of annual IT security awareness and specialized training for privileged users. In January 2016, the Undersecretary for Management directed all Components to include anti-phishing prevention as part of annual DHS IT security awareness training. In addition, Components must also conduct semi-annual social engineering exercises for both unprivileged and privileged users.

Progress

- As of September 2016, CBP, FEMA, FLETC, ICE, NPPD, OIG, S&T, TSA, USCG, and USCIS had provided the mandatory security awareness training to all users.

- As of September 2016, CBP, FEMA, FLETC, Headquarters, ICE, NPPD, OIG, S&T, TSA, and USCIS had conducted the required semi-annual social engineering exercises for both unprivileged and privileged users.

Issues To Be Addressed

- As of August 2016, four Components (CBP, FEMA, NPPD, and S&T) had not submitted reports on privileged user training completed during the year. As a result, ISO could not effectively monitor and report on whether all DHS employees and contractors with significant security responsibilities had received the required specialized training.

See Appendix F, Status of Security Training Program, for additional information.

Remote Access Program

DHS has established policies and procedures to mitigate the risks associated with remote access and dial-in capabilities. Components are responsible for managing all remote access and dial-in connections to their systems by using two-factor authentication, enabling audit logs, and implementing encryption mechanisms to protect transmission of sensitive information. Components developed policies and procedures to protect remote connections and implemented various mitigating security controls (i.e., multi-factor authentication, firewalls, virtual private network concentrators, etc.) to protect DHS systems and data from external threats.

Issues To Be Addressed

- As of August 2016, FEMA, Headquarters, TSA, and USSS had not consolidated multiple connections behind trusted Internet connections, as required.[12]

See Appendix H, Status of Remote Access Program, for more information.

Identity and Access Management Program

DHS' identity and access management program was decentralized, with its Components individually responsible for issuing PIV cards to their employees and contractors for logical access as required by *Homeland Security Presidential Directive-12*. Each Component used account management software (e.g., Active Directory) to enforce access policies consistent with DHS procedures and guidance.

Progress

- As of July 2016, CBP, FLETC, ICE, NPPD, OIG, S&T, and USSS had met the 100 percent compliance target for required PIV card use by privileged users.

---

[12] Under Secretary for Management Memorandum, *Strengthening DHS Cyber Defenses*, July 22, 2015.

Issues To Be Addressed.

- As of August 2016, CBP, ICE, TSA, USCG, and USCIS had not met the PIV card compliance target for unprivileged users. Further, Headquarters, TSA, USCG, and USCIS had not met the compliance target for required PIV card use by privileged users. DHS requires the use of PIV cards by all privileged and unprivileged users for logical access.[13]

See Appendix I, Status of Identity and Access Management Program, for summary information.

Continuous Monitoring Program

DHS had taken steps to strengthen its continuous monitoring program. For example, as of May 2016, USCG and USSS were reporting information security metrics, which allowed DHS to better evaluate the Department's security posture. ISO established the monthly FISMA Scorecard for national security systems to track and report information security metrics for "Secret" systems. Further, in an effort to bolster the Department's cyber defense, DHS required Components to develop the capability to prevent activation of malicious links or attachments in phishing emails. This was to be accomplished within 60 days of the issuance of the Undersecretary for Management's January 13, 2016 memorandum.

Progress

- DHS increased the number of systems participating in the OA program. As of July 2016, 96 systems from 7 Components (CBP, Headquarters, ICE, FLETC, OIG, TSA, and USCIS) were enrolled in the OA program, as compared with 82 systems in FY 2015.

- DHS ISO established the monthly FISMA scorecard for national security systems to track SA and ISCM metrics for most of its "Secret" systems.

Issues To Be Addressed

- As of July 2016, DHS was not collecting ISCM metrics for its stand-alone "Secret" systems.

---

[13] Under Secretary for Management Memorandum, *Strengthening DHS Cyber Defenses*, July 22, 2015.

- DHS had not issued a FY16 performance plan to outline requirements, priorities, and overall goals for reporting on its national security systems.

- As of September 2016, DHS and its Components had implemented only about 25 percent of the technology solution (i.e., Initial Operational Capability) to prevent activation of malicious links or attachments in phishing emails. Two Components (FEMA and TSA) had not begun their deployment efforts. DHS required that Components achieve Full Operational Capability within 90 days of the issuance of the Under Secretary for Management's January 13, 2016 memorandum.

- We interviewed selected CISOs and senior information security personnel at seven Components to discuss their continuous monitoring programs. We identified the following deficiencies, which may restrict Components from protecting their systems or preventing unauthorized software or hardware from being installed on their IT assets:

  ➢ Four Components did not perform network penetration testing.
  ➢ Two components did not have the technical capability to block unauthorized network devices, two components had not implemented the technical solution to block unauthorized hardware, and two components did not have the capability to block unauthorized software from being introduced to the network.

See Appendix J, Status of Continuous Monitoring Program, for more information.

Contingency Planning Program

DHS maintained an entity-wide business continuity and contingency planning program. However, the Department could take additional steps to strengthen its business continuity and disaster recovery programs.

Progress

- DHS had developed approaches for testing its business continuity and disaster recovery capabilities. In FY 2016, DHS participated

in Eagle Horizon, a mandatory, national-level exercise to test its continuity and reconstitution plans. The exercise also helped participants determine communications requirements and critical infrastructure support needed to execute mission-essential functions.

- The Department finalized *DHS Directive Number 008-03, Continuity Programs*, on June 10, 2015, to establish and further clarify its business continuity program policy, responsibilities, and requirements.

Issues To Be Addressed

- Nine Components (CBP, Headquarters, FEMA, FLETC, ICE, NPPD, S&T, USCG, and USSS) had not tested the contingency plans within the past 12 months for 41 operational systems with an overall FIPS 199 security categorization of moderate or high. When contingency plans are not tested, DHS and its Components cannot ensure operational restoration or recovery in the event of system failures or service disruptions.

- Our review of 10 SA packages disclosed the following deficiencies related to system contingency planning documentation:

  ➢ Contingency plans for two systems were not tested at the level required by DHS guidance.
  ➢ Procedures were not in place for four systems to restore operations for handling sensitive information to alternate sites.

See Appendix K, Status of Contingency Planning Program, for additional information.

Recommendations

We recommend that the CISO:

Recommendation #1: Maintain the process for informing the Department's senior executives on planned remedial actions to improve Components' information security programs that consistently lagged behind in key performance metrics (e.g., security authorization, weakness remediation, and continuous monitoring) on the FY 2016 information scorecard.

Recommendation #2: Institute an annual performance plan to communicate requirements, priorities, and overall goals for national security systems (e.g., "Secret" and "Top Secret" systems).

Recommendation #3: Expedite the implementation of strong authentication by ensuring the use of PIV cards by all privileged access account holders.

Recommendation #4: Strengthen ISO oversight to ensure that Components track and maintain POA&Ms in the Department's classified and unclassified enterprise management systems as required.

Management Comments and OIG Analysis

Management Comments to Recommendation #1

DHS concurred with recommendation 1. The Office of CISO (OCISO) plans to actively maintain the Quarterly Deputy Under Secretary for Management Cybersecurity Review process to keep the Department's senior executives informed of planned remedial actions and resolve impediments to improving Components' information security programs. Additionally, OCISO will issue the Information Security Performance Plans and monthly FISMA Scorecards for unclassified and national security systems. The scorecards document the Department's information security goals, progress towards the goals, and leverage the monthly CISO Council meetings to address specific information security challenges. Estimated Completion Date: December 31, 2016.

OIG Analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation is resolved and will remain open until DHS provides documentation to support that all planned corrective actions are completed.

Management Comments to Recommendation #2

DHS concurred with recommendation 2. OCISO is developing an annual Information Security Performance Plan specifically for National Security Systems to communicate requirements, priorities, and overall Departmental Information security goals. Estimated Completion Date: March 31, 2017.

OIG Analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation is resolved and will remain open until DHS provides documentation to support that all planned corrective actions are completed.

Management Comments to Recommendation #3

DHS concurred with recommendation 3. DHS has now achieved 99.4% privileged mandatory PIV logon compliance as of November 30, 2016 with 10 out of 12 Components reporting 100% compliance. DHS rapidly improved its Privileged Access Management practices as part of the 30-Day Cyber Security Sprint, with most Components implementing a password vaulting solution. Components yet to reach 100% compliance are Headquarters (3 users) and USCG (56 users). DHS Headquarters is currently implementing a solution for three mainframe privileged users at DC1 to be completed within the next several months. USCG is following Department of Defense guidance for Privileged Access Management (separate two-factor tokens and workstations) and is currently migrating the remaining 56 users to that prescribed solution.

In FY 2018, DHS will continue to strengthen its Privileged Access Management practices by participating in Continuous Diagnostic and Mitigation Phase II Privileged Management. Estimated Completion Dates: April 30, 2017 (Headquarters users); September 30, 2017 (all Components).

OIG Analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation is resolved and will remain open until DHS provides documentation to support that all planned corrective actions are completed.

Management Comments to Recommendation #4

DHS concurred with recommendation 4. OCISO will continue to improve and strengthen its oversight of Component developed POA&Ms in the Department's classified and unclassified enterprise information assurance and compliance systems. OCISO completed a formal IT Weakness Remediation Project of its classified systems in January 2016 and for its unclassified systems in November 2016. OCISO has been working with Components to (1) develop

effective weakness remediation plans, (2) improve POA&M status reporting, and (3) review Component POA&M progress on a bi-weekly basis.

In the area of POA&M oversight for National Security Systems, OCISO will ensure that POA&M quality measures are described in the Annual Information Security Performance Plan for DHS National Security Systems, are reviewed on a monthly basis by OCISO/ National Security Systems division and are reflected in the Monthly FISMA/Information Security Continuous Monitoring Scorecard. Estimated Completion Date: December 31, 2016.

OIG Analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation is resolved and 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 economy, efficiency, and effectiveness within the Department.

The objective of this review was to determine whether DHS had developed adequate and effective information security policies, procedures, and practices in FY 2016, in compliance with FISMA. In addition, we evaluated DHS' progress in developing, managing, and implementing its information security program for its unclassified, "Secret" and "Top Secret" systems.

Our independent evaluation focused on DHS' information security program based on the requirements outlined in FY 2016 reporting metrics. We performed our fieldwork at DHS Office of the Chief Information Officer (CIO) and at organizational Components and offices, including CBP, FEMA, Headquarters, ICE, NPPD, TSA, USCG, USCIS, and USSS.

To conduct our evaluation, we assessed compliance by DHS and its Components' with mandatory FISMA requirements and other applicable Federal information security policies, procedures, standards, and guidelines. Specifically, we (1) used last year's FISMA evaluation as a baseline for this year's evaluation; (2) reviewed policies, procedures, and practices that DHS had implemented at the program and component levels; (3) reviewed DHS' POA&M process to ensure all security weaknesses were identified, tracked, and addressed; (4) reviewed processes and the status of the department-wide information security program as reported in DHS' monthly information security scorecards, including system inventory, risk management, configuration management, incident response and reporting, security training, remote access, identity and access management, continuous monitoring, and contingency planning; and (5) developed our independent assessment of DHS' information security program.

We performed quality reviews of 10 SA packages at Headquarters, FEMA, ICE, NPPD, TSA, USCG, and USCIS for compliance with applicable DHS, OMB, and

NIST guidance. As part of the quality reviews, we also evaluated these 10 systems' compliance with DHS' baseline configuration settings. Finally, we determined the effectiveness of controls and compliance with USGCB settings for eight systems at CBP, FEMA NPPD, TSA, USCG, and USSS. Our evaluation did not include a comprehensive review of the Department's OA program.

We conducted this review between April and September 2016 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 the 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
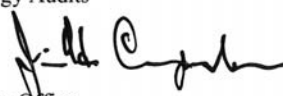
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

December 12, 2016

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 2016"
                  (Project No.16-052-ITA-MGMT)

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 significant progress in
remediating security weaknesses identified. DHS remains committed to strengthening its
information security program. For example, during fiscal year (FY) 2016, the
Department nearly completed numerous initiatives as directed by the Under Secretary for
Management (USM) in two cybersecurity memorandums. The initiatives enhanced
DHS's cyber defenses by holding department-wide information security awareness re-
training, conducting spear-phishing exercises, implementing endpoint protection
solutions, and enabling two-factor authentication on DHS's classified network. And, as
OIG's report highlights, as of May 2016, all Components were reporting information
security metrics to the Department, enabling DHS to better evaluate its security posture.

The draft report contained four recommendations with which the Department concurs.
Attached find our detailed response to the recommendations.

Again, thank you for the opportunity to review and comment on this draft report.
Technical comments were previously provided under separate cover. Please feel free to
contact me if you have any questions. We look forward to working with you in the
future.

Attachment

Attachment: DHS Management Response to Recommendations Contained in OIG Draft Report 16-052-ITA-MGMT

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

Recommendation 1: Maintain the process for informing the Department's senior executives on planned remedial actions to improve Components' information security programs that consistently lagged behind in key performance metrics (e.g., security authorization, weakness remediation, and continuous monitoring) on the FY 2016 information scorecard.

Response: Concur. The DHS Office of the Chief Information Security Officer (OCISO) plans to actively maintain the Quarterly Deputy Under Secretary for Management (DUSM) Cybersecurity Review process to keep the Department's senior executives informed of planned remedial actions and resolve impediments to improving Components' information security programs. Additionally, OCISO will issue the Information Security Performance Plans and monthly Federal Information Security Modernization Act of 2014 (FISMA) Scorecards for unclassified and national security systems. The scorecards document the department's information security goals, progress towards the goals, and leverage the monthly CISO Council meetings to address specific information security challenges. Estimated Completion Date (ECD): December 31, 2016

Recommendation 2: Institute an annual performance plan to communicate requirements, priorities, and overall goals for national security systems (e.g., "Secret" and "Top Secret" systems).

Response: Concur. OCISO is developing an annual Information Security Performance Plan specifically for National Security Systems to communicate requirements, priorities, and overall Departmental information security goals. ECD: March 31, 2017.

Recommendation 3: Expedite the implementation of strong authentication by ensuring the use of [personal identity verification] PIV cards by all privileged access account holders.

Response: Concur. DHS has now achieved 99.4 percent privileged mandatory PIV logon compliance as of November 30, 2016 with 10 out of 12 Components reporting 100 percent compliance. DHS rapidly improved its Privileged Access Management practices as part of the 30-Day Cyber Security Sprint, with most Components implementing *Xceedium* as a password vaulting solution. Components yet to reach 100 percent compliance are DHS Headquarters (HQ) (3 users) and USCG (56 users). DHS OCIO is currently implementing a solution for three mainframe privileged users at DC1 to be

2

completed within the next several months. USCG OCIO is following Department of Defense guidance for Privileged Access Management (separate two-factor tokens and workstations) and is currently migrating the remaining 56 users to that prescribed solution.

In FY 2018, DHS will continue to strengthen its Privileged Access Management practices and compliance reporting by participating in the Continuous Diagnostic and Mitigation (CDM) Phase II Privileged Management. ECDs: April 30, 2017 (HQ users); September 30, 2017 (all Components)

Recommendation 4: Strengthen [Information Security Office] ISO oversight to ensure that Components track and maintain [plan of action and milestones] POA&Ms in the Department's classified and unclassified enterprise management systems as required.

Response: Concur. OCISO will continue to improve and strengthen its oversight of Component developed POA&Ms in the Department's classified and unclassified enterprise information assurance and compliance systems (CIACS and IACS, respectively). OCISO completed a formal IT Weakness Remediation Project of its classified systems during January 2016 and the project concluded over its unclassified systems in November 2016. OCISO has been working directly with Components to: (1) develop effective weakness remediation plans, (2) improve POA&M status reporting, and (3) review Component POA&M progress on a bi-weekly basis.

In the area of POA&M oversight for National Security Systems, OCISO will ensure that POA&M quality measures are described in the Annual Information Security Performance Plan for DHS National Security Systems, are reviewed on a monthly basis by OCISO/ National Security Systems division and are reflected in the Monthly FISMA/Information Security Continuous Monitoring Scorecard. ECD: December 31, 2016.

3

Appendix C
Status of Risk Management Program

Status of Risk Management Program		
Has the organization established a risk management program that includes comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?		
1.	Identifies and maintains an up-to-date system inventory, including organization- and contractor-operated systems, hosting environments, and systems residing in the public, hybrid, or private cloud. (2016 CIO FISMA Metrics, 1.1; NIST Cybersecurity Framework (CF) ID.AM.1, NIST 800-53: PM-5)	**Yes**
2.	Develops a risk management function that is demonstrated through the development, implementation, and maintenance of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1. (NIST SP 800-39)	**Yes**
3.	Incorporates mission and business process-related risks into risk-based decisions at the organizational perspective, as described in NIST SP 800-37, Rev. 1. (NIST SP 800-39)	**Yes**
4.	Conducts information system-level risk assessments that integrate risk decisions from the organizational and mission/business process perspectives and take into account threats, vulnerabilities, likelihood, impact, and risks from external parties and common control providers. (NIST SP 800-37, Rev. 1, NIST SP 800-39, NIST SP 800-53: RA-3)	**Yes**
5.	Provides timely communication of specific risks at the information system, mission/business, and organization-level to appropriate levels of the organization.	**Yes**
6.	Performs comprehensive assessments to categorize information systems in accordance with Federal standards and applicable guidance. (FIPS 199, FIPS 200, FISMA, Cybersecurity Sprint, OMB M-16-04, President's Management Council cybersecurity assessments)	**Yes**
7.	Selects an appropriately tailored set of baseline security controls based on mission/business requirements and policies and develops procedures to employ controls within the information system and its operational environment.	**Yes**
8.	Implements the tailored set of baseline security controls described in Question 7.	**Yes**
9.	Identifies and manages risks with system interconnections, including authorizing system interconnections, documenting interface characteristics and security requirements, and maintaining interconnection security agreements. (NIST SP 800-53: CA-3)	**Yes**

10.	Continuously assesses security controls, including hybrid and shared controls, using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to meeting the security requirements for the system.	**Yes**
11.	Maintains ongoing information system authorizations based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable (OMB M-14-03, NIST Supplemental Guidance on Ongoing Authorization).	**Yes**
12.	Maintains security authorization packages containing system security plans, security assessment reports, and POA&Ms that are prepared and maintained in accordance with government policies. (SP 800-18, SP 800-37)	**Yes**
13.	Maintains and reviews POA&Ms to ensure they are effective for correcting security weaknesses.	**Yes**
14.	Centrally tracks and maintains and independently reviews/validates POA&M activities at least quarterly. (NIST SP 800-53:CA-5; OMB M-04-25)	**Yes**
15.	Prescribes the active involvement of information system owners, common control providers, chief information officers, senior information security officers, authorizing officials, and others as applicable in the ongoing management of information system-related security risks.	**Yes**
16.	Implements an insider threat detection and prevention program, including the development of comprehensive policies, procedures, guidance, and governance structures, in accordance with Executive Order 13587 and the National Insider Threat Policy. (President's Management Council; NIST SP 800-53: PM-12)	**Yes**
17.	Provides any additional information on the effectiveness (positive or negative) of the organization's Risk Management program that was not noted in the questions above. Based on all testing performed, is the Risk Management program effective?	**Yes**
Comments:	• As of June 2016, DHS had 79 unclassified systems operating without ATO.	

Appendix D
Status of Configuration Management Program

Status of Configuration Management Program		
Has the organization established a configuration management program that is inclusive of comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?		
1.	Develops and maintains an up-to-date inventory of the hardware assets (i.e., endpoints, mobile assets, network devices, input/output assets, and SMART/NEST devices) connected to the organization's network with the detailed information necessary for tracking and reporting. (NIST CF ID.AM-1; 2016 CIO FISMA Metrics 1.5, 3.17; NIST 800-53: CM-8)	**Yes**
2.	Develops and maintains an up-to-date inventory of software platforms and applications used within the organization and with the detailed information necessary for tracking and reporting. (NIST 800-53: CM-8, NIST CF ID.AM-2)	**Yes**
3.	Implements baseline configurations for IT systems that are developed and maintained in accordance with documented procedures. (NIST SP 800-53: CM-2; NIST CF PR.IP-1)	**Yes**
4.	Implements and maintains standard security settings (also referred to as security configuration checklists or hardening guides) for IT systems in accordance with documented procedures. (NIST SP 800-53: CM-6; CIO 2016 FISMA Metrics, 2.3)	**Yes**
5.	Assesses configuration change control processes, including processes to manage configuration deviations across the enterprise that are implemented and maintained. (NIST SP 800-53: CM-3, NIST CF PR.IP-3)	**Yes**
6.	Identifies and documents deviations from configuration settings. Acceptable deviations are approved with business justification and risk acceptance. Where appropriate, automated means that enforce and redeploy configuration settings to systems at regularly scheduled intervals are deployed, while evidence of deviations is also maintained. (NIST SP 800-53: CM-6, Center for Internet Security Controls (CIS) 3.7)	**Yes**
7.	Implemented SCAP certified software assessing (scanning) capabilities against all systems on the network to assess both code-based and configuration-based vulnerabilities in accordance with risk management decisions. (NIST SP 800-53: RA-5, SI- 2; CIO 2016 FISMA Metrics 2.2, CIS 4.1)	**Yes**
8.	Remediates configuration-related vulnerabilities, including scan findings, in a timely manner as specified in organization policy or	**Yes**

	standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2)	
9.	Develops and implements a patch management process in accordance with organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3, SI-2, OMB M-16-04, DHS Binding Operational Directive 15-01)	**Yes**
10.	Provides any additional information on the effectiveness (positive or negative) of the organization's Configuration Management Program that was not noted in the questions above. Based on all testing performed, is the Configuration Management Program effective?	**Yes**
Comments:	• Our testing results revealed that Components had made improvements in implementing USCGB settings. However, Components had implemented all USGCB settings on only one of eight systems tested. • Components had implemented about 74 percent of the DHS Baseline configuration settings on the Windows 2008 servers tested, and only 65 percent of the configuration settings on Linux servers tested. • We also identified missing security patches on Windows Server 2008/2012, as well as Windows 8.1 and 7 workstations tested. • Components continued to use unsupported operating systems (e.g., Windows XP, Windows Server 2003).	

Appendix E
Status of Incident Response and Reporting Program

Status of Incident and Response and Reporting Program		
Incident response program is not formalized and incident response activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16 03, OMB M 16-04, and US-CERT Federal Incident Notification Guidelines).		
1.	Please provide the Department/Agency ISCM maturity level for the People domain.	**Defined (Level 2)**
2.	Please provide the Department/Agency ISCM maturity level for the Processes domain.	**Defined (Level 2)**
3.	Please provide the Department/Agency ISCM maturity level for the Technology domain	**Defined (Level 2)**
4.	Please provide the Department/Agency ISCM maturity level for the ISCM Program Overall.	**Defined (Level 2)**
Comments:	None.	

Appendix F
Status of Security Training Program

Status of Security Training Program		
Has the organization established a security and privacy awareness and training program, including comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?		
1.	Develops training materials for security and privacy awareness training containing appropriate content for the organization, including anti-phishing, malware defense, social engineering, and insider threat topics. (NIST SP 80050, 80053: AR5, OMB M1501, 2016 CIO Metrics, President's Management Council, National Insider Threat Policy)	**Yes**
2.	Evaluates the skills of individuals with significant security and privacy responsibilities and provides additional security and privacy training content or implements human capital strategies to close identified gaps. (NIST SP 80050)	**No**
3.	Identifies and tracks status of security and privacy awareness training for all information system users (including employees, contractors, and other organization users) requiring security awareness training with appropriate internal processes to detect and correct deficiencies. (NIST 80053: AT2)	**Yes**
4.	Identifies and tracks status of specialized security and privacy training for all personnel (including employees, contractors, and other organization users) with significant information security and privacy responsibilities requiring specialized training.	**Yes**
5.	Measures the effectiveness of security and privacy awareness and training programs, including the use of social engineering and phishing exercises. (President's Management Council, 2016 CIO FISMA Metrics 2.19, NIST SP 80050, NIST SP 80055)	**Yes**
6.	Provides any additional information on the effectiveness (positive or negative) of the organization's Security and Privacy Training Program that was not noted in the questions above. Based on all testing performed, is the Security and Privacy Training Program effective?	**Yes**
Comments:	• Some Components did not report the numbers of employees who had received privileged training monthly. As of August 2016, four Components had not submitted a report on privileged user training completed during the year. • DHS had not established a central repository or administrator for tracking IT security awareness training and specialized training for privileged users.	

Appendix G
Status of Plan of Action and Milestones Program

Status of Plan of Action and Milestones Program		
Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines, and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		
1.	Documents policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation.	**Yes**
2.	Tracks, prioritizes, and remediates weaknesses.	**Yes**
3.	Ensures remediation plans are effective for correcting weaknesses.	**Yes**
4.	Establishes and adheres to milestone remediation dates and provides adequate justification for missed remediation dates.	**Yes**
5.	Ensures resources and ownership are provided for correcting weaknesses.	**Yes**
6.	Ensures POA&Ms include security weaknesses discovered during assessments of security controls that require remediation (do not need to include security weakness due to a risk-based decision to not implement a security control) (OMB M-04-25).	**Yes**
7.	Identifies costs associated with remediating weaknesses in terms of dollars (NIST SP 800-53, Control PM-3; OMB M-04-25).	**Yes**
8.	Ensures program officials report remediation progress to Chief Information Officer on a regular basis, at least quarterly, and the Chief Information Officer centrally tracks, maintains, and independently reviews/validates POA&M activities at least quarterly (NIST SP 800-53: CA-5; OMB M-04-25).	**Yes**

Comments:	• As of June 2016, DHS had 6,427 open unclassified POA&Ms in the Department's unclassified enterprise management system:
	  ➢ Of the 6,427 open unclassified POA&Ms, 2,895 (45 percent) were overdue. Moreover, 2,484 of these open POA&Ms were at least 3 months late while 1,728 POA&Ms were more than a year past due. DHS requires Components to complete POA&M remediation within 6 months.
	  ➢ Of the 2,895 open unclassified POA&Ms, 2,669 (92 percent) had weakness remediation estimates less than $50. DHS requires that Components provide reasonable resource estimates of at least $50 to mitigate known weaknesses.
	• DHS ISO was not tracking the quality of POA&Ms for its national security systems.	

Appendix H
Status of Remote Access Program

Status of Remote Access Program		
Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		
1.	Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST SP 800-53: AC-1, AC-17).	**Yes**
2.	Protection against unauthorized connections or subversion of authorized connections.	**Yes**
3.	Users uniquely identified and authenticated for all access (NIST SP 800-46, Section 4.2, Section 5.1).	**Yes**
4.	A fully developed telecommuting policy (NIST SP 800-46, Section 5.1).	**Yes**
5.	Authentication mechanisms meeting NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms.	**Yes**
6.	Defined and implemented encryption requirements for information transmitted across public networks.	**Yes**
7.	Remote access sessions, in accordance with OMB M-07-16, timed-out after 30 minutes of inactivity, after which re-authentication is required.	**Yes**
8.	Lost or stolen devices disabled and appropriately reported (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines).	**Yes**
9.	Adequate remote access rules of behavior in accordance with government policies (NIST SP 800-53, PL-4).	**Yes**
10.	Adequate remote-access user agreements in accordance with government policies (NIST SP 800-46, Section 5.1; NIST SP 800-53, PS-6).	**Yes**
11.	Policy to detect and remove unauthorized (rogue) connections?	**Yes**
Comments:	• As of August 2016, FEMA, Headquarters, TSA, and USSS have not consolidated multiple connections behind a trusted Internet connection, as required.	

Appendix I
Status of Identity and Access Management Program

Status of Identity and Access Management Program		
Has the organization established an identity and access management program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?		
1.	Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements, participate in required training prior to being granted access, and recertify access agreements on a predetermined interval. (NIST 800-53: PL-4, PS-6)	**Yes**
2.	Ensures that all users are only granted access based on least privilege and separation-of-duties principles.	**Yes**
3.	Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. networking devices such as load balancers and intrusion detection/prevention systems, and other input/output devices such as faxes and internet protocol phones).	**Yes**
4.	Implements PIV for physical access in accordance with government policies. (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11)	**Yes**
5.	Implements PIV or a NIST Level of Assurance 4 credential for logical access by all privileged users (system, network, database administrators, and others responsible for system/application control, monitoring, or administration functions). (Cybersecurity Sprint, OMB M-16-04, President's Management Council, 2016 CIO FISMA Metrics 2.5.1)	**Yes**
6.	Enforces PIV or a NIST Level of Assurance 4 credential for logical access for at least 85 percent of non-privileged users. (Cybersecurity Sprint, OMB M-16-04, President's Management Council, 2016 CIO FISMA Metrics 2.4.1)	**Yes**
7.	Tracks and controls the use of administrative privileges and ensures that these privileges are periodically reviewed and adjusted in accordance with organizationally defined timeframes. (2016 CIO FISMA Metrics 2.9, 2.10; OMB M-16-04, CIS 5.2)	**Yes**
8.	Ensures that accounts are terminated or deactivated once access is no longer required or after a period of inactivity, according to organizational policy.	**Yes**
9.	Identifies, limits, and controls the use of shared accounts. (NIST SP 800-53: AC-2)	**Yes**

10.	Uniquely identifies and authenticates all users for remote access using strong authentication (multi-factor), including PIV. (NIST SP 800-46, Section 4.2, Section 5.1, NIST SP 800-63)	**Yes**
11.	Protects against and detects unauthorized remote access connections or subversion of authorized remote access connections, including remote scanning of host devices. (CIS 12.7, 12.8, FY 2016 CIO FISMA metrics 2.17.3, 2.17.4, 3.11, 3.11.1)	**Yes**
12.	Times out remote access sessions after 30 minutes of inactivity, requiring user re-authentication, consistent with OMB M-07-16.	**Yes**
13.	Enforces a limited number of consecutive invalid remote access logon attempts and automatically locks the account or delays the next logon prompt. (NIST 800-53: AC-7)	**Yes**
14.	Implements a risk-based approach to ensure that all agency public websites and services are accessible through secure connections through the use and enforcement of https and strict transport security. (OMB M-15-13)	**Yes**
15.	Provides any additional information on the effectiveness (positive or negative) of the organization's Identity and Access Management Program that was not noted in the questions above. Based on all testing performed, is the Identity and Access Management Program effective?	**Yes**
Comments:	• As of August 2016, DHS Headquarters, TSA, USCG, and USCIS had not met the compliance target to require PIV card use by privileged users. DHS requires mandatory PIV card use by all privileged and unprivileged users.	

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix J
Status of Continuous Monitoring Program

Status of Continuous Monitoring Program		
ISCM program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800 53, SP 800 137, OMB M-14-03, and the CIO ISCM CONOPS.		
1.	Please provide the Department/Agency ISCM maturity level for the People domain.	**Defined (Level 2)**
2.	Please provide the Department/Agency ISCM maturity level for the Processes domain.	**Defined (Level 2)**
3.	Please provide the Department/Agency ISCM maturity level for the Technology domain	**Defined (Level 2)**
4.	Please provide the Department/Agency ISCM maturity level for the ISCM Program Overall.	**Defined (Level 2)**
Comments:	• DHS increased the number of systems participating in the OA program. As of July 2016, 96 systems from 7 Components (CBP, Headquarters, ICE, FLETC, OIG, TSA, and USCIS) were enrolled in the OA program, as compared with 82 systems in FY 2015. • DHS had not implemented an ISCM program for the Department's "Top Secret" systems. Additionally, as of August 2016, DHS was not collecting ISCM metric information for its stand-alone "Secret" systems. • We identified the following deficiencies, which may restrict Components from protecting their systems or preventing unauthorized software/hardware from being installed on their IT assets: ➢ Four Components did not perform network penetration testing. ➢ Five Components did not have technical capabilities to block unauthorized network devices, hardware, and software from being introduced to the network.	

Appendix K
Status of Contingency Planning Program

Status of Contingency Planning Program		
Has the organization established an enterprise-wide business continuity/disaster recovery program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?		
1.	Develops and facilitates recovery testing, training, and exercise programs. (FCD1, NIST SP 800-34, NIST SP 800-53)	**Yes**
2.	Incorporates the system's Business Impact Analysis and Business Process Analysis into analysis and strategy toward development of the organization's Continuity of Operations Plan, Business Continuity Plan, and Disaster Recovery Plan. (NIST SP 800-34)	**Yes**
3.	Develops and maintains documented recovery strategies, plans, and procedures at the division, component, and IT infrastructure levels. (NIST SP 800-34)	**Yes**
4.	Has Business Continuity Plan and Disaster Recovery Plan in place and ready to be executed if necessary. (FCD1, NIST SP 800-34, 2016 CIO FISMA Metrics 5.3, President's Management Council)	**Yes**
5.	Tests Business Continuity Plan and Disaster Recovery Plan for effectiveness and updates plans, if needed. (2016 CIO FISMA Metrics, 5.4)	**Yes**
6.	Tests system-specific contingency plans, in accordance with organizationally defined timeframes, to determine the effectiveness of the plans as well as readiness to execute the plans if necessary. (NIST SP 800-53: CP-4)	**Yes**
7.	Develops after-action reports that address issues identified during contingency/disaster recovery exercises in order to improve contingency/disaster recovery processes. (FCD1, NIST SP 800-34)	**Yes**
8.	Determines alternate processing and storage sites based upon risk assessments that ensure potential disruption of the organization's ability to initiate and sustain operations is minimized, and the sites are not subject to the same physical and/or cybersecurity risks as the primary sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-6, CP-7)	**Yes**
9.	Conducts backups of information at the user- and system-levels and protects the confidentiality, integrity, and availability of backup information at storage sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-9, NIST CF, PR.IP-4, NARA guidance on information systems security records)	**Yes**

10.	Conducts contingency planning that considers supply chain threats.	**Yes**
11.	Provides any additional information on the effectiveness (positive or negative) of the organization's Contingency Planning Program that was not noted in the questions above. Based on all testing performed, is the Contingency Planning Program effective?	**Yes**

Comments:	• Within the past 12 months, DHS and its Components had not tested contingency plans for 41 operational systems with an overall FIPS 199 security categorization of moderate or high.
	• Our review of 10 SA packages disclosed the following deficiencies related to system contingency planning documentation:
	  ➢ Contingency plans for two systems were not tested at the level required by DHS guidance.
	  ➢ Procedures were not in place for four systems to restore operations for handling sensitive information at alternate sites.	

Appendix L
Status of Agency Program to Oversee Contractor Systems

Status of Agency Program to Oversee Contractor Systems		
Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		
1.	Establishes and implements a process to ensure that contracts/statements of work/solicitations for systems and services, include appropriate information security and privacy requirements and material disclosures, Federal Acquisition Regulation clauses, and clauses on protection, detection, and reporting of information. (FAR Case 2007-004, Common Security Configurations, FAR Sections 24.104, 39.101, 39.105, 39.106, 52.239-1; President's Management Council, 2016 CIO Metrics 1.8, NIST 800-53, SA-4 FedRAMP standard contract clauses; Cloud Computing Contract Best Practices)	**Yes**
2.	Specifies within appropriate agreements how information security performance is measured, reported, and monitored on contractor- or other entity-operated systems. (CIO and CAO Council Best Practices Guide for Acquiring IT as a Service, NIST SP 800-35)	**Yes**
3.	Obtains sufficient assurance that security controls for systems operated on the organization's behalf by contractors or other entities and services provided on the organization's behalf meet FISMA requirements, OMB policy, and applicable NIST guidelines. (NIST SP 800-53: CA-2, SA-9)	**Yes**
4.	Provides any additional information on the effectiveness (positive or negative) of the organization's Contractor Systems Program that was not noted in the questions above. Based on all testing performed, is the Contractor Systems Program effective?	**Yes**
Comments:	None.	

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix M
Major Office of Information Technology Audit Contributors to This Report

Chiu-Tong Tsang, Director
Michael Kim, IT Audit Manager
Aaron Zappone, Supervisory Program Analyst
Thomas Rohrback, Supervisory IT Specialist
Jasmine Raeford, IT Specialist
Mahfuza Khanam, IT Auditor
Tunisia Phifer, IT Auditor
Beverly Burke, Referencer

Appendix N
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

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