OFFICE OF INSPECTOR GENERAL

Evaluation of DHS' Information Security Program for Fiscal Year 2015

Homeland
Security

January 5, 2016
OIG-16-08 (Revised)

DHS OIG HIGHLIGHTS

Evaluation of DHS' Information Security Program for Fiscal Year 2015

January 5, 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, plans 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, DHS developed and implemented the *Fiscal Year 2015 Information Security Performance Plan* to define the performance requirements, priorities, and overall goals of the Department. DHS has also taken steps to address the President's cybersecurity priorities, such as Information Security Continuous Monitoring; Identity, Credential, and Access Management; and anti-phishing and malware defense.

Nonetheless, the Department must ensure compliance with information security requirements in other areas. For example, DHS did not include classified systems information in its monthly information security scorecard or its *Federal Information Security Modernization Act of 2014* reporting submission to the Office of Management and Budget. Contrary to the Under Secretary's guidance, the United States Coast Guard (USCG) did not report its personal identity verification card implementation data to the Department. We also identified inaccurate or incomplete data in DHS' enterprise management systems.

Further, Components did not maintain their information security programs on a year-round, continuous basis or perform weakness remediation reviews as required. Components operated 220 "sensitive but unclassified," "Secret," and "Top Secret" systems with expired authorities to operate. We also identified deficiencies related to plans of action and milestones, configuration management, and continuous monitoring. Without addressing these deficiencies, the Department cannot ensure that its systems are properly secured to protect sensitive information stored and processed in them.

DHS Response

We made six recommendations to the Chief Information Security Officer. The Department concurred with five recommendations.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

January 5, 2016

MEMORANDUM FOR: Jeffrey Eisensmith
Chief Information Security Officer

Sondra F. McCauley

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

SUBJECT: *Evaluation of DHS' Information Security Program for Fiscal Year 2015 (OIG-16-08)*

Attached for your information is our revised final report, *Evaluation of DHS' Information Security Program for Fiscal Year 2015*. We reissued the report with a correction to the number of systems without authority to operate and current contingency plan tests. These revisions do not change the overall findings or recommendations in the report. Please see the attached errata sheet for details.

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

Attachment

Errata page for OIG-16-08

Evaluation of DHS' Information Security Program for Fiscal Year 2015

Change made to the DHS OIG Highlights section, 3rd paragraph (see below):

Changed from:
Components operated 136 "sensitive but unclassified," "Secret," and "Top Secret" systems with expired authorities to operate.

Changed to:
Components operated 220 "sensitive but unclassified," "Secret," and "Top Secret" systems with expired authorities to operate.

Change made to the Overall Issues To Be Addressed section, page 9, 2nd bullet (see below):

Changed from:
Components continued to operate information systems without ATO. For example, the Department had 119 systems sensitive but unclassified (SBU) systems, as well as 17 systems classified as "Secret" and "Top Secret" operating with an expired ATO.

Changed to:
Components continued to operate information systems without ATO. For example, the Department had 203 sensitive but unclassified (SBU) systems, as well as 17 systems classified as "Secret" and "Top Secret" operating with an expired ATO.

Change made to the Risk Management - Issues To Be Addressed section, page 14, 1st bullet (see below):

Changed from:
As of June 2015, DHS had 119 systems classified as "SBU" operating without ATO.

Changed to:
As of June 2015, DHS had 203 systems classified as "SBU" operating without ATO.

Change made to the Risk Management - Issues To Be Addressed section, page 14, Figure 4 (see below):

Changed from:

Figure 4: Number of Component Systems Operating without Valid ATOs

Component	Number of Operational Systems Without ATO
CBP	14
DHS HQ	11
FEMA	25
FLETC	4
ICE	7
NPPD	10
S&T	7
TSA	10
USCG	26
USCIS	3
USSS	2

Changed to:

Figure 4: Number of Component Systems Operating without Valid ATOs

Component	Number of Operational Systems Without ATO
CBP	8
DHS HQ	1
FEMA	111
FLETC	2
ICE	3
NPPD	15
S&T	12
TSA	0
USCG	35
USCIS	0
USSS	16

Change made to the Contingency Planning - Issues To Be Addressed section, page 28, 1st bullet (see below):

Changed from:

For the previous 12 months, DHS and its Components had not tested contingency plans for 203 operational systems with an overall FIPS security category of moderate or high.

Changed to:

For the previous 12 months, DHS and its Components had not tested contingency plans for 106 operational systems with an overall FIPS security category of moderate or high.

Change made to the OIG Analysis section, page 32, 2nd paragraph (see below):

Changed from:
As of June 2015, DHS had 119 SBU and 17 classified systems ("Secret" or "Top Secret") operating without ATOs.

Changed to:
As of June 2015, DHS had 203 SBU and 17 classified systems ("Secret" or "Top Secret") operating without ATOs.

Change made to the Appendix D, page 46, 2nd bullet (see below):

Changed from:
DHS had 119 systems classified as "SBU" and 17 systems classified as "Secret" or "Top Secret" operating without ATO

Changed to:
DHS had 203 systems classified as "SBU" and 17 systems classified as "Secret" or "Top Secret" operating without ATO

Change made to the Appendix L, page 57, 1st bullet (see below)

Changed from:
For the previous 12 months, DHS and its Components had not tested contingency plans for 203 operational systems with an overall FIPS security category of moderate or high.

Changed to:
For the previous 12 months, DHS and its Components had not tested contingency plans for 106 operational systems with an overall FIPS security category of moderate or high.

Table of Contents

Appendixes

Abbreviations

ATO	authority to operate
CBP	Customs and Border Protection
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
HQ	Headquarters
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
OCIO	Office of Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	personal identity verification
POA&M	plans of action and milestones
S&T	Science and Technology
SA	security authorization
SBU	sensitive but unclassified
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 the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other 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 agency Chief Information Officers, in coordination with other senior agency officials, to report annually to the agency head on the effectiveness of the information security program, including progress of remedial actions. The Office of Inspector General (OIG), or an independent external auditor determined by the OIG, must independently evaluate the effectiveness of an agency's information security program and practices each year.

The Office of Management and Budget (OMB) annually issues updated instructions for agency and OIG reporting under FISMA. Our report this year summarizes the results of our evaluation of the Department's information security program based on the FISMA reporting metrics issued in June 2015.[1]

As outlined in the Administration's cybersecurity Cross-Agency Priority Goals, agencies are required to improve their Information Security Continuous Monitoring (ISCM) programs. In addition, agencies must take steps to ensure only authorized users have access to resources and information and implement technologies and processes to reduce the risk of malware. To achieve the Administration's goals, Federal agencies must strengthen their information security operations by implementing the following capabilities:

[1] *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*, Version 1.2, June 19, 2015.

- ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity;
- a set of authentication capabilities for users to access information technology (IT) resources and restrict users' access to only those resources they need to perform their job functions; and
- technologies, processes, and training that reduce the risk of malware being introduced through email and malicious or compromised websites.

As part of OMB's Cybersecurity Sprint Initiative in June 2015, DHS was required to:

- deploy indicators regarding priority threat-actor techniques, tactics, and procedures to scan systems and checklogs;
- apply security patches to mitigate critical vulnerabilities without delay;
- strengthen policies and practices for privileged users; and
- accelerate the implementation of multi-factor authentication, especially for privileged users.

On July 22, 2015, in response to recent cyber attacks on the Federal Government, the Under Secretary for Management issued a memorandum requiring DHS and its Components to strengthen their cyber defenses.[2] DHS Components were to implement cybersecurity infrastructure measures, including the following, within 30 days:

- consolidate all of DHS' internet traffic behind the Department's trusted internet connections;
- implement strong authentication with the use of personal identity verification (PIV) cards for all privileged and unprivileged access accounts;
- achieve 100 percent compliance for security authorization (SA) of 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 and 2003).

According to the Under Secretary for Management's memorandum, Component Heads were required to submit letters of risk acceptance if the Component could not comply with the required cybersecurity infrastructure measures. The

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

letters were to contain detailed plans, including actions and milestones for achieving the measures that were not in compliance. As of September 29, 2015, the Department had received letters of risk acceptance from Customs and Border Protection (CBP), DHS Headquarters (HQ), Federal Emergency Management Agency (FEMA), Federal Law Enforcement Training Center (FLETC), Immigration and Customs Enforcement (ICE), OIG, National Protection and Programs Directorate (NPPD), Science and Technology (S&T), Transportation Security Administration (TSA), and United States Secret Service (USSS).

The Chief Information Security Officer (CISO), who heads the Information Security Office (ISO), manages DHS' information security program for the Department's unclassified systems, as well as the systems classified as "Secret" and "Top Secret." To aid in managing the program, the CISO developed the *Fiscal Year 2015 DHS Information Security Performance Plan.* The CISO also updated the *Ongoing Authorization (OA) Methodology* to enhance existing processes, such as risk management and continuous monitoring, and align DHS with the Administration's cybersecurity priorities. DHS relies on two enterprise management systems to create and maintain SA documentation and monitor plans of action and milestones (POA&M) activities for its unclassified systems, as well as those classified as "Secret."[3]

In December 2014, we recommended the Department declare and report a material weakness, in accordance with *the Federal Information Security Management Act of 2002* requirements, on Components' information security programs that were consistently lagging behind in key performance metrics (e.g., system inventory, SA, continuous monitoring, and weakness remediation) on the information scorecard, or when Components failed to provide the required continuous monitoring data feeds.[4]

In March 2015, we disagreed with the Department's delay in making the decision on whether or not to declare and report a material weakness. As of August 2015, the CISO would not make a decision until the Department could evaluate the Components' progress at the end of September 2015. However, we believe the decision on declaring a material weakness should be based on the

[3] The National Institute of Standards and Technology (NIST) defines "security authorization" as the official management decision given 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 the implementation of an agreed-upon set of security controls.

[4] *Evaluation of DHS' Information Security Program for Fiscal Year 2014*, (OIG-15-16, December 12, 2014).

performance of Components' information security programs during fiscal year (FY) 2014 and not on whether Components have made progress in FY 2015.

Results of Evaluation

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

In FY 2015, DHS has taken steps to strengthen its information security program. For example, the DHS ISO developed and implemented the *Fiscal Year 2015 Information Security Performance Plan* to define the performance requirements, priorities, and overall goals for the Department throughout the year. In addition, DHS has taken actions to address the President's cybersecurity priorities to ensure secure access to information systems.

While improvements have been made, the Department must ensure compliance with information security requirements in other areas. For example, DHS does not include its classified system information as part of its monthly information security scorecard or its FISMA submission to OMB. In addition, USCG is not reporting its PIV data to the Department, which is a contradiction to the Under Secretary for Management's guidance that requires Components to submit this information to the Department.[5] In addition, we identified deficiencies with DHS' enterprise management systems, including inaccurate or incomplete data.

Further, DHS Components are not maintaining their information security programs on a year-round, continuous basis. In addition, Components are continuing to operate information systems without an authority 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 sensitive information stored and processed in them.

[5] Under Secretary for Management Memorandum, *Immediate Implementation and Reporting of Privileged Users Authentication*, June 25, 2015.

Details

Based on the requirements outlined in FISMA and OMB's annual reporting instructions, we focused on 10 key areas of DHS' information security program. Specifically, we reviewed the Department's:

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

We identified any significant progress made in these key areas since our FY 2014 evaluation, along with issues DHS still needs to address.

Overall Progress

DHS took steps to improve its information security program during FY 2015. For example, ISO updated the monthly information security scorecard to include additional or revised metrics aimed at better evaluating security processes and continuous monitoring capabilities. Specifically, ISO added anti-phishing and malware metrics while expanding the configuration management metric to cover Linux, Macintosh, and Unix operating systems.

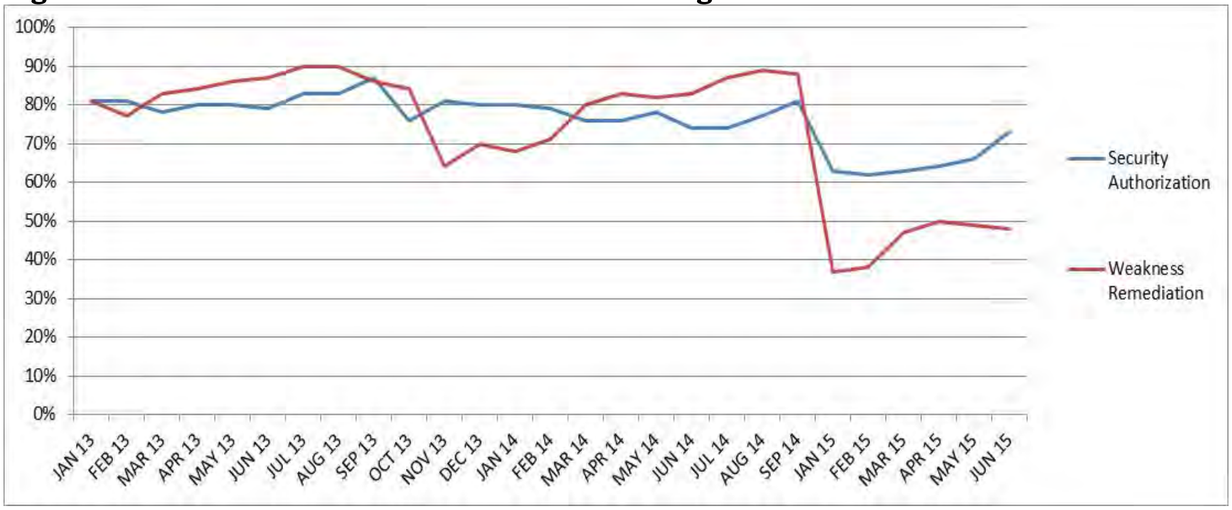
Overall Issues To Be Addressed

Despite the improvements made, the Department must take additional actions to ensure compliance with information security requirements in other areas. For example, DHS did not include classified system information as part of its monthly information security scorecard or its FISMA submission to OMB. USCG reported its PIV implementation to the Defense Information Systems Agency, instead of to DHS as required. In addition, we identified inaccurate or incomplete data in DHS' enterprise management systems.

ISO conducted critical control reviews, outreach and assist visits, and system authorization reviews to strengthen DHS' information security program and ensure Components' compliance with the Department's information security policies and procedures. However, the Components did not consistently follow DHS' requirements to update systems' SA and POA&M documentation in the Department's enterprise management systems. In addition, Components continued to operate systems without the proper authority and did not comply with all OMB and DHS continuous monitoring requirements. Specifically, we identified the following:

- Components did not maintain their information security programs on a year-round, continuous basis. For example, we evaluated the SA and POA&M (i.e., weakness remediation) performance metrics from the Department's information security scorecards for January 2013 to June 2015. Figure 1 depicts that the overall scores for both metrics peaked during the months of Components' annual FISMA reporting (around July–August) and dropped in the subsequent months. We identified a similar issue in 2009.[6] This trend is an indication that Components are not complying with requirements to update and maintain systems' SA and POA&M documentation on a continuous basis.

Figure 1: DHS' SA and Weakness Remediation Progress



Source: OIG compiled based on DHS monthly information security scorecard from July 2013 to June 2015.[7]

- According to DHS Chief Information Officer officials, USCG reported to Defense Information Systems Agency on its PIV implementation. Consequently, DHS does not have complete oversight or visibility

[6] *Evaluation of DHS' Information Security Program for Fiscal Year 2009*, (OIG-09-109, September 2009).

[7] DHS did not produce information security scorecards for the periods of October FY 2014 - December FY 2014.

regarding USCG's information security program, including its implementation of PIV. USCG reporting external to DHS is contrary to the Under Secretary for Management's June 2015 memorandum requiring Components to report internally the status of PIV implementation, including the counts of all privileged access accounts and the number of accounts enabled with PIV.[8]

- Some of the information in the Department's enterprise management systems was inaccurate or incomplete. Specifically, DHS' enterprise management systems lacked input validation controls to ensure accurate data were entered into the system. For example, some data fields (e.g., contingency plan test dates, POA&M remediation funding, POA&M creation/completion dates, accreditation date, ATO approval date) lacked input validation controls, allowing Components to enter unrealistic, invalid, or null values. The data inaccuracy restricted the ability of the Department and Authorizing Officials to oversee and make credible, risk-based decisions regarding their information systems. Until input validation is implemented and data verification is complete, DHS cannot fully rely on information reported by the Components in the enterprise management systems, which impacts overall security program management.

- Our review of the Department's monthly information security scorecards identified discrepancies in the areas of PIV implementation and the continued use of unsupported operating systems. These were indicators that DHS' senior officials may not be providing the most accurate data to make risk-based decisions about the Department's information security program. For example:

    - We identified discrepancies between the Department's monthly scorecard and the data maintained by the Identity, Credential and Access Management Office regarding the status of PIV implementation.
    - We identified significant discrepancies between the Component Heads' letters of risk acceptance and the August 2015 information security scorecard regarding DHS' use of unsupported or obsolete operating systems (i.e., Windows XP, Windows Server 2003). Figure 2 shows the difference between the numbers of unsupported operating systems reported.

[8] Under Secretary for Management Memorandum, *Immediate Implementation and Reporting of Privileged Users Authentication*, June 25, 2015.

Figure 2: Discrepancies on the Number of Unsupported Operating Systems Reported

	CBP	DHS HQ	FEMA	FLETC	ICE	NPPD	OIG	S&T	USCG	USCIS	USSS
August 2015 Information Security Scorecard	**15**	**50**	**87**	**41**	**346**	**84**	**0**	**2**	**221**	**711**	**0**
Letters of Acceptance of Risk from Component Heads[9]	**11**	**58**	**243**	**180**	**405**	**86**	**2**	**0**	**N/A**	**N/A**	**N/A**

Source: OIG compiled based on DHS' monthly information security scorecard and letters of acceptance of risk from Component Heads.

- DHS did not include information related to its "Secret" or "Top Secret" systems in its FISMA submissions to OMB or in its monthly information security scorecard. Without this information, DHS' senior officials and OMB cannot make accurate, risk-based decisions about the Department's information security program.

- Components continued to operate information systems without ATO. For example, the Department had 203 sensitive but unclassified (SBU) systems, as well as 17 classified as "Secret" and "Top Secret" operating with an expired ATO. Without a valid ATO, DHS and its Components cannot ensure they have implemented effective controls to protect the sensitive information stored and processed by these systems.

- DHS had not implemented an ISCM program for its classified systems. As of July 2015, the ISO had not completed its National Security System ISCM strategy to outline the implementation requirements, metrics, and reporting that will be used to evaluate progress toward meeting DHS' continuous monitoring goals.[10]

- Components were not consistently updating system SA and POA&M information in DHS' unclassified and classified enterprise management systems despite the ISO's efforts to perform critical control reviews,

[9] According to ISO personnel, as of September 29, 2015, USCG and United States Citizenship and Immigration Services (USCIS) did not submit a letter of risk acceptance to the Department. Additionally, USSS did not identify the number of unsupported operating systems in the component's submission.

[10] *DHS National Security System Information Security Continuous Monitoring Implementation Plan* (Draft), Version 1.0, January 8, 2015.

component outreach and assist visits, and system authorization quality checks. Without complete or accurate information, DHS cannot effectively manage or oversee the Department's information system program or ensure that known information security weaknesses are remediated.

- As of June 2015, DHS reported that it had Windows Server 2003 operating systems installed on 3,044 servers. DHS also reported 787 machines that were running unsupported versions of Windows, including Windows XP. However, Microsoft ended its support for Windows Server 2003 on July 14, 2015, and Windows XP on April 8, 2014, respectively.[11] On July 22, 2015, the Under Secretary for Management required Components to retire all expired operating systems and servers, including Windows XP and Windows Server 2000/2003 operating systems.[12]

- DHS had not completed its information security scorecard to track FISMA and ISCM compliance for national security systems.

- Based on our FISMA testing activities and other audits conducted during FY 2015, Components had not implemented all the required United States Government Configuration Baseline (USGCB) and DHS baseline configuration settings on the information systems selected for review. We reported a similar finding in FY 2014.[13]

System Inventory

DHS maintained and updated its FISMA systems 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 any other inventory issues. DHS' inventory comprised 743 information systems that the Department reported as "operational," including a mix of major applications and general support systems classified as "SBU" (673), "Secret" (62), and "Top Secret" (8). In addition, DHS had determined that 136 of its systems were mission essential systems.

[11] DHS Chief Information Officer 2015 FISMA Quarter 3 Report, submitted June 26, 2015.

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

[13] *Evaluation of DHS' Information Security Program for Fiscal Year 2014*, (OIG-15-16, December 2014)

Progress

- DHS updated its FISMA System Inventory Methodology guidance in May 2015 to reflect the Department's latest guidance regarding systems inventory management.[14]

- Components were required to identify and report their hardware assets to the Department on a monthly basis for DHS to develop and maintain an accurate inventory. As of July 2015, eight Components had met or exceeded the Department's target of 95 percent for hardware asset reporting on DHS' monthly information security scorecard.

- DHS maintained a change control process to ensure that the Department's inventory of systems remained accurate and up-to-date.

Issues To Be Addressed

- DHS required Components to report all software assets within their organizations as part of their ISCM program. However, as of July 2015, CBP, FEMA, FLETC, ICE, USCG, and USSS had not met the Department's target (95 percent) for software asset management, receiving scores of 69, 15, 82, 65, 65, and 72 percent, respectively.

See Appendix C, System Inventory, and Appendix M, Status of Agency Program to Oversee Contractor Systems, for additional information.

Risk Management Program

SA is the formal management decision by a senior organizational 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 the implementation of an agreed-upon set of security controls.[15] The SA process provides an approach for assessing security controls (e.g., operational, technical, and management) to determine their overall effectiveness. DHS requires Components to use enterprise management systems for incorporating NIST security controls when performing SA on their systems. The enterprise-wide management systems enable Components to

[14] *DHS FISMA System Inventory Methodology*, Version 13.5, May 1, 2015.

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

Components used DHS enterprise management tools to create SA artifacts for monitoring and authorizing their systems. These artifacts include:

- Federal Information Processing Standards (FIPS) Publication 199 Categorization;
- privacy threshold analysis and, if required, privacy impact assessment;
- E-Authentication;
- security plan;
- contingency plan;
- security assessment plan;
- contingency plan test results;
- security assessment report;
- authorization decision letter;
- POA&M; and
- annual self-assessment.

In October 2013, DHS began to allow Components to enroll in the OA program. Components are required to have a strong ISCM process, approved common controls, 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 before each system can also be entered into the program:

- Component OA program acceptance letter;
- OA system admission letter;
- OA recommendation letter;
- system ATO expiration greater than 60 days of submission date;
- information system security officer with collateral responsibilities less than 51 percent;
- information system security officer trained on OA processes; and
- an approved control allocation table.

Progress

- As of July 2015, OIG, TSA, and USCIS had met the Department's SA target of 100 percent for high-value assets and

[15] DHS *Security Authorization Process Guide,* Version 11.1, March 16, 2015.

mission-essential systems. In addition, HQ, FLETC, NPPD, OIG, TSA, and USCIS had exceeded the Department's SA target of 95 percent for all other FISMA systems.

Issues To Be Addressed

- DHS adopted enterprise management systems to manage and track the SA process for its "SBU" and "Secret" systems. During our evaluation, we identified the following inaccuracies associated with the enterprise management systems and a lack of input validation controls on some data fields:

  - Our analysis of data from the Department's SBU enterprise management system revealed that Component personnel had not entered appropriate data. For example, in key data fields, they input null values or invalid information, such as accreditation date, contingency plan tests, POA&M creation/completion dates, accreditation dates, etc. Without accurate POA&M information, authorizing officials lack the most up-to-date information about their systems and whether sufficient resources are provided to mitigate known security weaknesses.
  - Data from the Department's classified enterprise system were missing key information. For example, Component personnel provided inaccurate or null information for the SA and POA&M data fields for many of the systems identified in the enterprise management system. As a result, ISO must perform manual reviews to carry out its oversight and validation responsibilities for the Department's "Secret" systems.
  - As of July 2015, FEMA, S&T, USCG, and USSS were failing the Department's SA metrics. The Under Secretary for Management requires Components to achieve 100 percent compliance for authorizing systems that Components identify as high-value assets and 95 percent compliance for the remaining systems. Figure 3 identifies the SA compliance for these Components, along with DHS' targets.

Figure 3: SA Status for FEMA, S&T, USCG, and USSS as of July 2015

	FEMA	S&T	USCG	USSS	DHS Target
High Value Assets and Mission Essential Systems	70%	33%	56%	75%	**100%**
All Other FISMA Systems	26%	45%	67%	58%	**95%**

Source: OIG compiled based on DHS' monthly information security scorecard.

- As of June 2015, DHS had 203 systems classified as "SBU" operating without ATO. Figure 4 illustrates the number of operational "SBU" systems, by Component, operating without ATO.

Figure 4: Number of Component Systems Operating without Valid ATOs

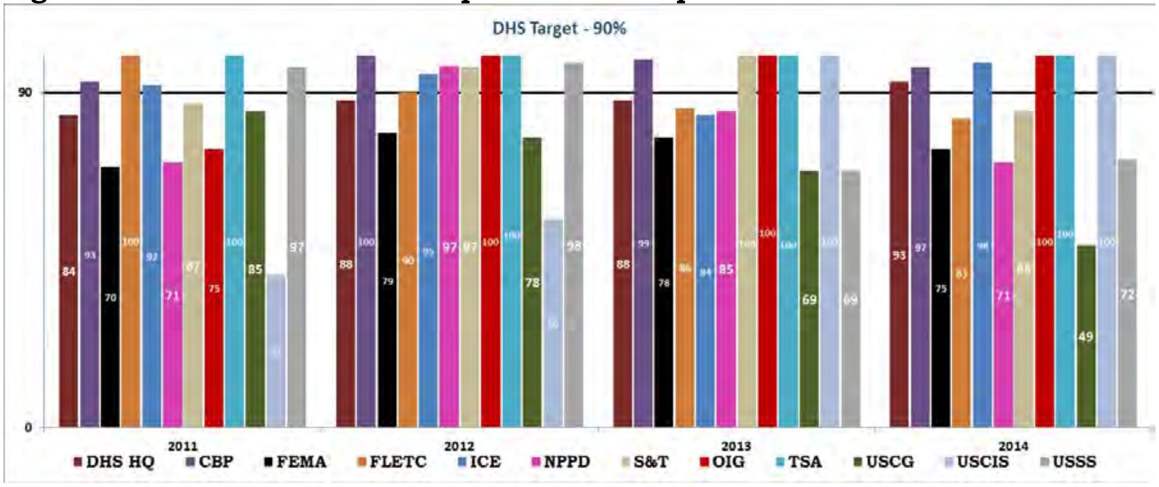
Component	Number of Operational Systems Without ATO
CBP	8
DHS HQ	1
FEMA	111
FLETC	2
ICE	3
NPPD	15
S&T	12
TSA	0
USCG	35
USCIS	0
USSS	16

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

- As of June 2015, DHS had 17 systems classified as "Secret" or "Top Secret" operating without ATOs. Without ATOs, DHS cannot ensure that its systems are properly secured to protect sensitive information stored and processed in them.

- We analyzed the Department's September FY 2011 to FY 2014 information security scorecards to determine whether it was meeting its goal for SA. Based on our analysis, only CBP and TSA met or exceeded the target at any time during the entire period. The other Components either missed or did not sustain the Department's overall 90 percent SA target. In addition, FEMA and USCG did not meet the SA target for any of the years selected for review. Figure 5 compares Component SA scores to the target for the last four fiscal years.

Figure 5: End of Fiscal Year Component SA Comparison



Source: OIG compiled based on our analysis of DHS' information security scorecards for September FY 2011 to FY 2014.

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

  - Three systems had not completed their NIST 800-53 annual self-assessments.
  - The system security plan for one "Secret" system was out of date.
  - The system security plans for six systems did not contain the required security controls.
  - The system security plan for three systems did not contain incident handling procedures, and two systems did not describe the configuration management process.
  - The FIPS 199 artifacts for two systems were either improperly categorized or had missing information.
  - The security assessment plans for two systems did not include specific procedures for testing the required security controls.
  - POA&Ms were not developed for weaknesses identified in the security assessment reports for four systems.

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

Plan of Action and Milestones Program

DHS requires the creation and maintenance of a POA&M for all known information security weaknesses. In April 2015, the DHS ISO conducted a comprehensive POA&M review and developed a weakness analysis report on the Department's SBU and classified POA&Ms.[16] ISO used the review to identify systemic deficiencies in the POA&M management process, issues that prohibited Components from resolving information security weaknesses, areas where additional training was required, and enterprise management system deficiencies. ISO also used the review to formulate recommendations for improving the POA&M process. Despite these efforts, Components did not enter and track all information security weaknesses in DHS' unclassified and classified enterprise management systems as required.

Progress

- Based on our selected sample, Components had created a POA&M for the notices of findings and recommendations for the weaknesses identified during our FY 2014 financial statement audit.[17]

Issues To Be Addressed

- Some of the key deficiencies identified by the ISO's comprehensive POA&M review included:

  - Component personnel (i.e., CISO, information system security managers) did not perform adequate POA&M reviews on systems, as basic quality issues were not identified prior to POA&M creation. DHS requires continuous monitoring of POA&M data and proper identification and prioritization of all weaknesses.[18]
  - POA&Ms were not updated on a monthly basis. DHS requires that Component CISOs or information system security managers review milestone status monthly to determine whether plans of action to remediate security weaknesses are on schedule.
  - Enterprise management systems lacked input validation measures to prevent Component personnel from creating POA&Ms until all DHS and OMB data elements were entered.

[16] *DHS Information Security Office Weakness Analysis Report,* Version 1.0, April 5, 2015.
[17] *Information Technology Management Letter for the FY 2014 Department of Homeland Security Financial Statement Audit,* (OIG-15-93, May 2015).
[18] *DHS 4300A Sensitive Systems Handbook, Attachment H, Process Guide for Plan of Action and Milestones (POA&M)*, Version 11.0, December 3, 2014.

- Compliance reporting was inaccurate and could not accurately track the number of classified POA&Ms within DHS, as Components had been reporting weaknesses using uploaded documents instead of populating automated fields/features within the enterprise management system.
- Classified POA&Ms did not contain sufficient information regarding weakness remediation. DHS requires that Components upload corrective action plans into the Department's classified enterprise management system.
- Security personnel needed better guidance to estimate resources (i.e., funding) required for weakness remediation.

- Components had not created POA&Ms for systems that were operating without ATOs. For example, FEMA had not created any POA&Ms for 11 systems classified as "Secret" or "Top Secret" that were operating without ATOs. Without creating POA&Ms, authorizing officials lacked the most accurate information to make credible risk-based decisions. They also could not ensure that all identified information security weaknesses were mitigated timely. When operating systems without ATOs, DHS and its Components cannot ensure they have implemented effective controls to protect the sensitive information stored and processed by these systems. We reported a similar finding in FY 2014.[19]

- As of June 2015, DHS had 22,294 open SBU POA&Ms, as compared to the 3,206 POA&Ms we reported for the previous year. Given FEMA's IT resiliency effort in 2014 and the addition of over 100 new systems, the component was responsible for 18,654 of the total 22,294 (84 percent) open SBU POA&Ms. According to ISO personnel, most of the milestone descriptions were severely inadequate and did not contain the information needed to address identified weaknesses.

- 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. 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 2015, we identified the following deficiencies in the Department's

[19] *Evaluation of DHS' Information Security Program for Fiscal Year 2014*, (OIG-15-16, December 2014)

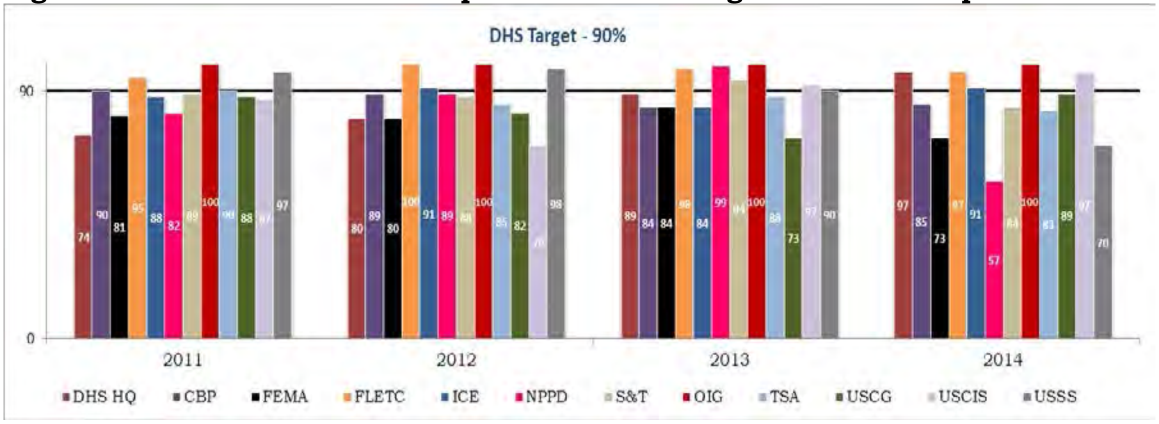
unclassified enterprise management system:

- Of the 22,294 open SBU POA&Ms, 17,663 (79 percent) were overdue. Moreover, 7,665 of the POA&Ms were at least 3 months late while 75 POA&Ms were more than a year past due. DHS requires Components to complete POA&M remediation within 6 months.
- Of the 22,294 open SBU POA&Ms, 20,423 (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.

- The Department had not provided adequate oversight on POA&M remediation for its "Secret" and "Top Secret" systems. For example, Components did not maintain the required POA&M information for its classified systems ("Secret") in the Department's classified enterprise management system. ISO personnel acknowledged they had not provided the oversight or enforcement mechanism needed to ensure Components correctly used the Department's enterprise management system. In FY 2015, DHS migrated to a new enterprise management system for its classified systems. However, many of the essential SA and POA&M data fields were not transferred to the new system, restricting DHS' ability to manage its security program.

- We analyzed the Department's September information security scorecards from FY 2011 to FY 2014 to determine the effectiveness of the Components' POA&M remediation efforts and whether they met DHS' POA&M target (90 percent). Based on our analysis, only OIG and FLETC met or exceeded the target during the entire period. FEMA and USCG were consistently below the target for the entire period. Figure 6 depicts Component POA&M scores for FY 2011 to FY 2014. See appendix H for the status of DHS' POA&M program.

Figure 6: End of Fiscal Year Component POA&M Targeted Score Comparison



Source: OIG compiled based on our analysis of DHS' FISMA September information security scorecards from FY 2011 through FY 2014.

- CBP did not incorporate all known information security weaknesses in a POA&M process for its Analytical Framework for Intelligence system, as required by applicable DHS, OMB, and NIST guidance. Specifically, CBP management officials did not create POA&M to address contingency planning deficiencies identified after its April 2014 testing exercise.[20]

- USSS did not properly maintain POA&M for its Criminal Investigative Division Suite. Specifically, our review of Criminal Investigative Division Suite POA&Ms revealed that key information was missing from their POA&M, such as required resources, status, scheduled completion dates, and milestone information.[21]

Configuration Management

We selected 18 systems from 10 Components (CBP, DHS HQ, FEMA, ICE, NPPD, OIG, TSA, USCG, USCIS, and USSS) to evaluate compliance with USGCB and DHS baseline configuration settings. The systems tested include a mix of major applications and general support systems categorized as "SBU," "Secret," and "Top Secret." We also performed vulnerability assessments on selected databases and websites to determine whether Components had implemented effective controls to protect DHS' sensitive data.

[20] *Enhancements to Technical Controls Can Improve the Security of CBP's Analytical Framework for Intelligence* (OIG-15-137, September 2015).
[21] *DHS Can Strengthen Its Cyber Mission Coordination Efforts* (OIG-15-140, September 2015).

Issues To Be Addressed

Our testing identified the following deficiencies:

<u>USGCB Compliance for Windows 7 and Windows XP Workstations</u>

- Two systems from FEMA and NPPD still used Windows XP at the time of testing. Microsoft had stopped providing security updates or technical support for Windows XP in April 2014, which could lead to unidentified and unpatched vulnerabilities for these older operating systems. We also determined the following:
  - ➢ The Windows XP workstations on one of FEMA's Top Secret systems had a USGCB compliance rate of 38 percent. FEMA had accepted the risk of operating the system with non-compliant settings and an unsupported operating system. However, continued use of the unsupported Windows XP workstations put FEMA's "Top Secret" data at risk.
  - ➢ In May 2015, NPPD officials said they were in the process of replacing 40 Windows XP workstations that were still operational. After we completed our field work, NPPD provided evidence that all of the Windows XP workstations had been removed.[22]

- Components we tested had not implemented all the required USGCB settings. Figure 7 summarizes deficiencies identified on the Components' Windows 7 and Windows XP workstations.

Figure 7: USGCB Compliance for Windows 7 and Windows XP Operating Systems

Component	Windows 7	Windows XP
	USGCB Implementation	USGCB Implementation
FEMA	None	38%
NPPD	73%	76%
TSA	98%	None

Source: OIG compiled based on testing results.

[22] We did not conduct an independent assessment to verify that NPPD had removed all Windows XP workstations.

Server Compliance with DHS Baseline Configuration Settings

- We evaluated approximately 200 configuration settings on four Windows 2008 servers. Overall, 76 percent of the configuration settings that we tested were compliant with the DHS baseline requirements. In addition, only 69 percent of the configuration settings tested on one server was compliant.

- We evaluated 91 configuration settings on a Red Hat Linux server. Our testing revealed that only 71 percent of the configuration settings tested met the DHS baseline requirements. Further, only 60 percent of the baseline configuration settings tested on one SE Linux server was compliant.

- We evaluated 130 configuration settings on three Windows 2003 servers. Our testing revealed that only 31, 47, and 60 percent of the baseline configuration settings tested on these servers met DHS requirements. In addition, only 71 percent of 120 configuration settings tested on one Windows XP system were compliant.

Vulnerability Assessments of Selected Systems

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

- Windows 8.1 workstations were missing security patches for the Firefox Internet browser, Adobe software (e.g., AIR, Flash Player, Reader), and Microsoft Office products and services. Some of the missing patches were high-risk, dating back to February 2015.

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

- Workstations were missing security patches for the Windows XP operating system and the Microsoft Office suite. We also identified missing patches on software such as Adobe (e.g., Acrobat, Flash Player, Reader, and Shockwave) and Oracle Java. Some of the missing high-risk patches dated back to December 2011.

- Components had implemented weak passwords and had not applied security patches on databases timely, which could allow attackers to exploit the vulnerabilities to gain unauthorized access to DHS data. DHS requires Components to apply security patches timely.

- Two of the three internal websites tested were susceptible to cross-site and/or cross-frame vulnerabilities, which could allow attackers to impersonate legitimate users or execute clickjacking attacks.[23] Further, these websites were vulnerable to Structured Query Language injection.[24] Exploitation of these weaknesses could give unauthorized users access to sensitive government data.

- Prior OIG audits in FY 2015 revealed that Components had not fully implemented all of the required configuration settings on selected systems. For example, we reported these deficiencies:

  - Configuration vulnerabilities existed on CBP's Analytical Framework for Intelligence system.[25]
  - ICE had not implemented selected DHS baseline configuration settings on its Cyber Crimes Center workstations and servers as required, which could allow sensitive data to be compromised.[26]

See Appendix E, Status of Configuration Management Program, for more information in this regard.

[23] Cross-site and cross-frame scripting vulnerabilities allow attackers to inject malicious code into otherwise benign websites. A clickjacking attack deceives a victim into interacting with specific elements of a target website without user knowledge, executing privileged functionality on the victim's behalf.

[24] Successful exploitation of a Structured Query Language injection vulnerability allows an attacker to extract, modify, insert, or delete data from a supporting database. One Component assessed stated that it had resolved all identified website vulnerabilities; however, we did not conduct an independent assessment to verify the claim.

[25] *Enhancements to Technical Controls Can Improve the Security of CBP's Analytical Framework for Intelligence* (OIG-15-137, September 2015).

[26] *DHS Can Strengthen Its Cyber Mission Coordination Efforts* (OIG-15-140, September 2015).

Incident Response and Reporting Program

The Department operates the DHS Security Operations Center (SOC) and the Homeland Secure Data Network SOC to ensure that SBU and Secret IT resources are secure.[27] The SOCs are also responsible for ensuring compliance with security policy and controls throughout the Department. The DHS SOC provides situational awareness, serves as a central data repository, and facilitates reporting and coordination regarding computer security incidents across the Department.

Issues To Be Addressed

- Components are required to submit weekly incident reports to the DHS SOC. However, only USCG and USCIS regularly submitted incident reports to the SOC in FY 2015. SOC personnel said they notify Component leadership when weekly incident reports are not submitted regularly as required.

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

Security Training Program

DHS monitors security training completion through monthly status updates provided by the Components. Based on these updates, the ISO monitors and reports on all DHS employees who receive annual IT security awareness and privileged security training as required.

Progress

- DHS reported that, as of June 2015, CBP, DHS HQ, FEMA, ICE, NPPD, S&T, and USCIS had received 100 percent for the privileged training metric, which tracked the number of privileged users who had completed specialized training during the year.

Issues To Be Addressed

- In June 2015, DHS reported that privileged users in some Components had not received specialized training as required.

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

Specifically, the following Components received privileged training scores of 79 percent or less: OIG (60 percent); TSA (79 percent); USCG (59 percent); and USSS (0 percent). Without the required training, DHS cannot ensure Component personnel with significant IT security responsibilities have the appropriate skills and knowledge to secure systems against potential attacks.

- Some Components did not report monthly the numbers of employees who had received IT security awareness and privileged training as required. As of August 2015, NPPD and USSS had submitted no report on privileged user training completion during the year. As a result, ISO could not effectively monitor and report DHS-wide on whether employees and contractors with significant security responsibilities had completed the required specialized training.

- Based on our analysis, ICE, TSA, and USCIS collectively had nearly 600 privileged users that had not completed specialized training as of August 2015. In another report published in September 2015, we similarly stated that ICE and USSS employees with significant security responsibilities had not received required specialized security training.[28]

See Appendix G, 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. Our field work revealed that 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.

[28] *DHS Can Strengthen Its Cyber Mission Coordination Efforts* (OIG-15-140, September 2015)

Issues To Be Addressed

- As of July 2015, CBP, FEMA, NPPD, and TSA had 40 connections that had yet to be consolidated behind a trusted Internet connection as required. Figure 8 illustrates the number of connections by Component.

Figure 8: Number of Non-Trusted Internet Connections by Component

	CBP	FEMA	NPPD	TSA	Total
Number of Non-Trusted Internet Connections	9	12	11	8	40

Source: DHS' July 2015 information security scorecard.

See Appendix I, 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. Each Component used account management software (e.g., Active Directory) to enforce access policies consistent with DHS procedures and guidance. To strengthen security, DHS has been implementing PIV cards compliant with *Homeland Security Presidential Directive-12* and the Administration's Identity, Credential, and Access Management priorities.

Progress

- As of July 2015, seven Components (DHS HQ, FEMA, FLETC, ICE, NPPD, OIG, and S&T) had met the target of 100 percent for mandatory PIV use for privileged access accounts, which was part of the OMB and DHS Cybersecurity Sprint initiative.

- As of August 2015, the Department had issued 4,565 (69 percent) two-factor authentication tokens for all accounts on its classified Homeland Secure Data Network to reduce user anonymity and improve security. Additionally, the Department had issued two-factor authentication tokens to all of its privileged users on the Homeland Secure Data Network.

Issues To Be Addressed

- According to the Office of Chief Information Officer (OCIO) officials, USCG no longer reported key information security metrics to DHS. Instead, USCG had begun reporting its PIV implementation for unprivileged and privileged access accounts to the Defense Information Systems Agency. This practice prohibited DHS from having complete oversight of USCG's information security program, including its implementation of PIV. This practice also was contrary to the Under Secretary for Management's June 2015 memorandum requiring Components to report the status of PIV implementation, including the number of privileged access accounts and the number of accounts with PIV logical access.

- As of July 2015, NPPD had not implemented PIV for its unprivileged access accounts. Further, USSS had received a score of 9 percent for implementation of PIV logical access for its unprivileged access accounts, versus a target score of 100 percent mandatory PIV use.

See Appendix J, Status of Account and Identity Management Program, for summary information.

Continuous Monitoring Program

DHS had taken steps to strengthen its continuous monitoring program. For example, the ISO updated or developed additional ISCM metrics to better evaluate the Components' compliance with applicable OMB and DHS continuous monitoring requirements for 2015. In addition, the ISO expanded the OA program and took steps to develop an ISCM program for the Department's classified systems.

Progress

- DHS increased the number of systems participating in the OA program. As of August 2015, 82 systems from 7 Components (CBP, DHS HQ, ICE, FLETC, OIG, TSA, and USCIS) were enrolled. In FY 2014, we reported that DHS had 61 systems from 5 Components enrolled in the OA program.

- During FY 2015, DHS revised its information security scorecard to evaluate the Components' alignment with OMB and DHS cyber security goals. For example, the ISO developed an anti-phishing/malware metric to evaluate whether Components had installed anti-virus software updates on their workstations, laptops, notebooks, and servers.

Issues To Be Addressed

- In 2013, DHS instituted rigorous eligibility requirements for Components to enroll in the OA program. For example, Components could only enter the OA program if they maintained a strong ISCM program by sustaining SA metrics above 80 and weakness remediation metrics above 60. However, as of August 2015, only 82 systems were enrolled in the program.

- DHS had not implemented an ISCM program for the Department's classified systems. DHS was in the process of finalizing its *National Security System Information Security Continuous Monitoring Implementation Plan,* which identified the requirements, metrics, and reporting that would be used to implement and evaluate the Department's progress toward continuous monitoring goals for its classified systems.

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

  - Four Components did not perform network penetration testing.
  - Five Component systems did not have the technical capability to block unauthorized software from being introduced to any device on the network.
  - Three Components did not have the technical ability to block unauthorized hardware (e.g., USB drives) from connecting to any devices on the network.

See Appendix K, Status of Continuous Monitoring Program.

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 test and exercise approaches for its business continuity and disaster recovery programs. In FY 2015, DHS participated in Eagle Horizon, a mandatory, national-level exercise to test its continuity and reconstitution plans. The exercise also helped participants to evaluate 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 continuity program policy, responsibilities, and requirements.

Issues To Be Addressed

- For the previous 12 months, DHS and its Components had not tested contingency plans for 106 operational systems with an overall FIPS security category 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:

  - ➢ One system with an overall security categorization of “high” and another categorized as “moderate” did not contain procedures to restore operations for handling sensitive information at alternate sites.
  - ➢ One system with an overall security categorization of “moderate” did not identify alternate or off-site storage facilities. In addition, the contingency plan did not identify vendor points of contact as required.

  - A contingency plan had not been tested for one system with an overall security categorization of "high."

- CBP did not update the contingency plan for its Analytical Framework for Intelligence system to address deficiencies identified in the last contingency plan test. As a result, CBP may have encountered difficulties restoring its operations in the event of a service disruption.[29]

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

Recommendations

We recommend that the CISO:

Recommendation #1:
Establish a process to inform senior Department officials on planned remedial actions to strengthen Components' information security programs that consistently lagged behind in key performance metrics (e.g., security authorization, weakness remediation) on the FY 2015 information scorecard, or when Components failed to provide information as required, consistent with FISMA and DHS policies.

Recommendation #2:
Strengthen the FISMA reporting process to ensure that DHS' classified system data are included on the Department's monthly information security scorecard and submitted to OMB.

Recommendation #3:
Strengthen the Department's oversight of the Component's information security programs to ensure they comply with requirements throughout the year instead of peaking in compliance during the months leading up to annual FISMA reporting.

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

[29] *Enhancements to Technical Controls Can Improve the Security of CBP's Analytical Framework for Intelligence* (OIG-15-137, September 2015).

Recommendation #5:
Implement input validation controls on DHS' enterprise management systems and perform quality reviews to validate that the information entered is accurate.

Recommendation #6:
Ensure that information reported in the monthly scorecard is accurate, including the number of unsupported operating systems (i.e., Windows XP, Windows Server 2003) and the status of PIV implementation.

Management Comments and OIG Analysis

Management Comments to Recommendation #1

DHS concurred with recommendation 1. The DHS ISO will improve its recently established process of informing senior Department officials on planned remedial actions to strengthen Components' information security programs that 1) consistently lagged behind in key performance metrics (e.g., security authorization, weakness remediation) on the FY 2015 information scorecard, or when Components failed to provide information as required, consistent with FISMA and DHS policies. Estimated completion date: February 29, 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 did not concur with recommendation 2. The FY 2015 CIO Annual FISMA Metrics guidance developed cooperatively by DHS, OMB, the National Security Council, and the DHS NPPD, Office of Cybersecurity and Communications do not require the submission of agency classified system data. Important and relevant criteria for national security systems (i.e., "Secret" and "Top Secret" systems) are different from SBU systems, and a separate monthly scorecard has been created for national security systems and it is distributed to DHS OCIO management and OIG.

In addition, there may be a need in the future to make the national security systems scorecard a classified document, which would necessitate separate reporting from our SBU systems. The separate monthly scorecard is available for the OIG's review from August 2015 to date.

OIG Analysis

Under FISMA 2014, agencies can submit the annual report in unclassified form but may include classified annex. According to OMB Memorandum M-14-04, agencies are required to summarize the performance of their information security program to secure all of their information systems in their annual FISMA report. Agencies are required to perform annual reviews and reporting of all systems, including national security systems. Further, agencies can either provide responses either in aggregate or separate from their non-national security systems. The CIO for the Office of Director of National Intelligence reports on systems processing, storing, or transmitting sensitive compartmentalized information across the Intelligence Community and those other systems for which the Director of National Intelligence is the principal accrediting authority.

As such, we maintain that the Department should include its classified system data (e.g., total number of systems, number of systems with ATOs, open POA&M, closed POA&M, etc.) on the Department's monthly information security scorecard and submitted to OMB. This recommendation is unresolved and will remain open until we obtain clarification from OMB and NPPD's Office of Cybersecurity and Communications on agencies' classified FISMA reporting requirements for "Secret" and "Top Secret" systems.

Management Comments to Recommendation #3

DHS concurred with recommendation 3. Over the last two years, DHS has been implementing its OA methodology to improve Components' compliance with information security program requirements throughout the year instead of peaking in compliance during the months leading up to annual FISMA reporting. OA improves the security of the Department's information systems through a new risk management approach. This revised approach transitions the Department from a static, paperwork driven, security authorization process to a dynamic framework that provides for security related information on demand to make risk-based decisions based on frequent updates to security plans, security assessment reports, and hardware and software inventories. DHS ISO has observed more steady compliance for the Component systems that have transitioned to OA.

To address this recommendation, DHS ISO will focus efforts on working closely with Components, including meeting quarterly, to develop plans to expedite the transition of the remaining Component systems to OA. Estimated completion date: February 29, 2016.

OIG Analysis

According to OMB M-15-01, prior to transitioning a system to ongoing authorization, two conditions must be satisfied: (1) an organizational ISCM program is in place that has the capability to monitor all implemented security controls with the appropriate degree of rigor and at the appropriate frequencies specified by the organization in accordance with their ISCM strategy and NIST guidance; and (2) the information system has been granted an initial ATO and has entered the operations/maintenance phase of the system development life cycle. As part of the July 22, 2015 memorandum, the Under Secretary for Management established a 100 percent SA compliance target for high value assets and 95 percent compliance for the remaining systems.

We do not agree that the Department's proposed corrective actions will improve Components' compliance with DHS' information security program requirements throughout the year, instead of peaking in compliance during the months leading up to annual FISMA reporting. Since establishing the program in 2013, the Department has made limited progress in expanding the OA program. Specifically, as of August 2015, there are only 82 SBU systems across 7 Components that are included in the OA program. Further, the Department has not approved any classified ("Secret" or "Top Secret") systems into the OA program. As of June 2015, DHS had 203 SBU and 17 classified systems ("Secret" or "Top Secret") operating without ATOs. These systems cannot be migrated to the Department's OA program until they are granted with the initial ATO. This recommendation is unresolved and will remain open until DHS provides corrective actions that will strengthen the Department's oversight of the Component's information security programs to ensure they comply with requirements throughout the year.

Management Comments to Recommendation #4

DHS concurred with recommendation 4. The DHS ISO continues to strengthen its oversight of Component developed POA&Ms in the Department's classified and unclassified enterprise information assurance and compliance systems. DHS has launched a formal IT Weakness Remediation project as of February 2015 and has been working with the Components to:
(1) develop effective weakness remediation plans,

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

Additionally, DHS Senior leadership has committed to ensuring the appropriate resourcing for the Components' remediation efforts in FY 2016 and FY 2017 for the IT Weakness Remediation project. ISO will provide a detailed briefing to the OIG of the improvements in its oversight to resolve this recommendation. Estimated completion date: January 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 #5

DHS concurred with recommendation 5. The DHS ISO will obtain and examine examples of the weaknesses identified by the OIG as we are unable to replicate the issues noted in the report. Once we pinpoint the weaknesses, the ISO will work closely with the vendor supporting the enterprise information assurance and compliance systems to address them. Estimated completion date: To be determined.

OIG Analysis

In September 2015, the OIG provided ISO with sample data deficiencies that we identified during our review of the enterprise management systems. In addition, ISO identified a number of issues associated with the enterprise management tool in its *DHS Information Security Office Weakness Analysis Report*, dated April 5, 2015. For example, ISO noted in its report that a number of POA&Ms had a creation date of a month or more into the future. ISO also noted that data validation checks were needed in the enterprise management systems to prevent Components from future dating POA&M creation dates or back dating actual POA&M completion dates.

This recommendation is unresolved and will remain open until DHS provides estimated completion dates and documentation to support that corrective actions have been completed.

Management Comments to Recommendation #6

DHS concurred with recommendation 6. The DHS ISO will examine and improve, as needed, the metrics, techniques, and tools used to generate the monthly scorecard to ensure its accuracy. Estimated completion date: February 29, 2016.

OIG Analysis

The Department did not provide detailed corrective actions on how to ensure that information reported in the monthly scorecard is accurate, including the number of unsupported operating systems (i.e., Windows XP, Windows Server 2003) and PIV implementation. This recommendation is unresolved until the Department provides detailed corrective actions. In addition, the recommendation will remain open until documentation is provided 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 for FY 2015, in compliance with FISMA, as amended. In addition, we evaluated DHS' progress in developing, managing, and implementing its information security program.

Our independent evaluation focused on DHS' information security program based on the requirements outlined FY 2015 reporting metrics. We conducted our field work at DHS Headquarters and at its organizational Components and offices, including CBP, DHS HQ, FEMA, ICE, NPPD, OIG, TSA, USCG, USCIS, and USSS. This report references the results of related audits we conducted throughout the year, as well as our ongoing financial statement reviews.

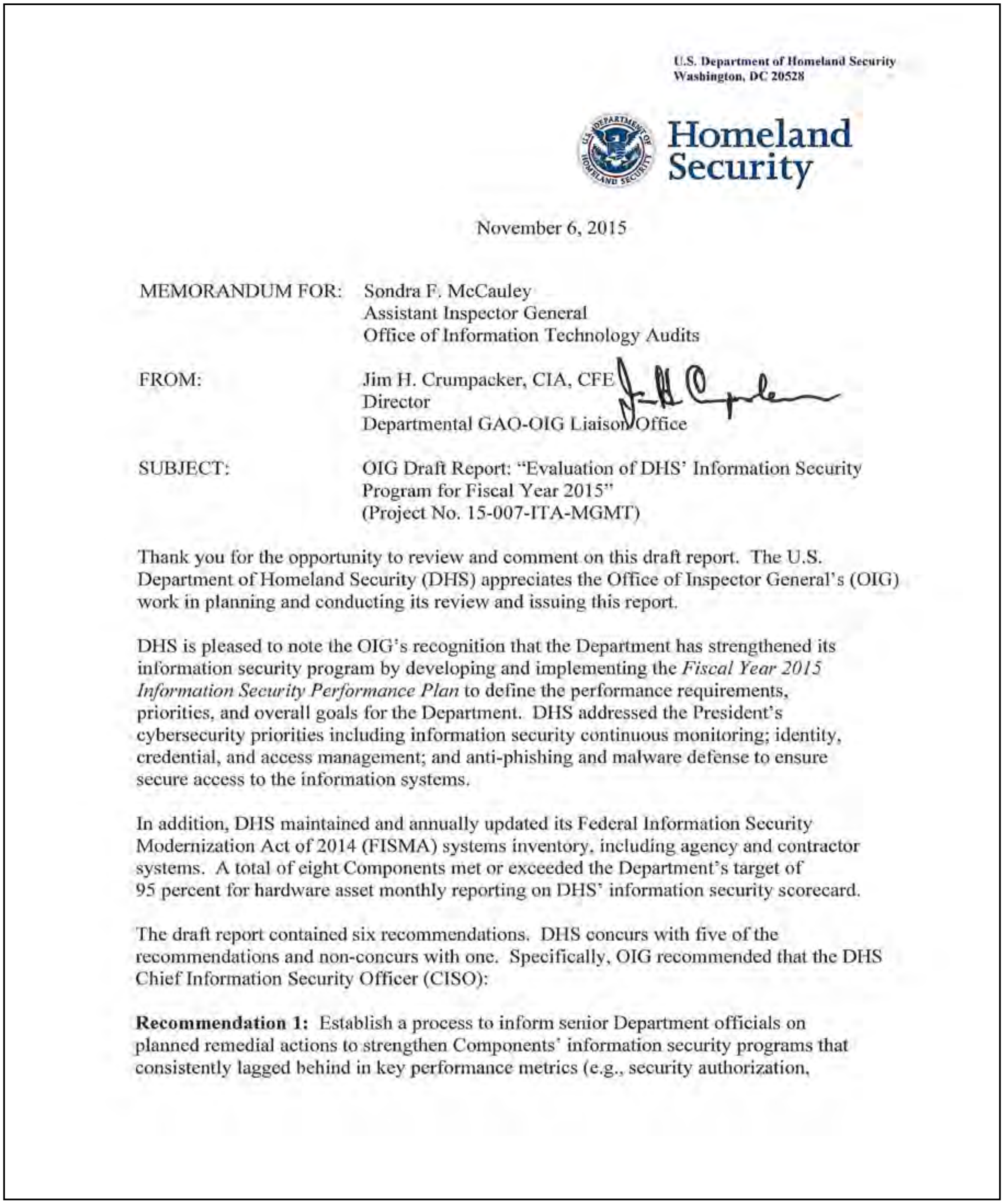
As part of our evaluation, we assessed compliance by DHS and its Components' with mandatory FISMA security requirements and other applicable Federal information security policies, procedures, standards, and guidelines. Specifically, we: (1) used last year's FISMA evaluation as a baseline for this year's 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 DHS' department-wide information security program, 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 evaluation of DHS' information security program.

We performed quality reviews of 10 SA packages at DHS HQ, CBP, FEMA, ICE, NPPD, USCG, USCIS, and USSS for compliance with applicable DHS, OMB, and NIST guidance. We evaluated the compliance of 10 systems at CBP, DHS HQ, FEMA, ICE, NPPD, USCG, USCIS, and USSS with DHS' baseline configuration settings. We assessed the compliance of three systems at FEMA, NPPD and TSA with USGCB settings. We also determined the effectiveness of controls implemented on two databases at FEMA and ICE and three websites at CBP, OIG and TSA. Our evaluation did not include a comprehensive review of the Department's Ongoing Authorization program.

We conducted this review between May and August 2015 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.

Appendix B

Management Comments to the Draft Report



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

Homeland Security

November 6, 2015

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: OIG Draft Report: "Evaluation of DHS' Information Security Program for Fiscal Year 2015"
(Project No. 15-007-ITA-MGMT)

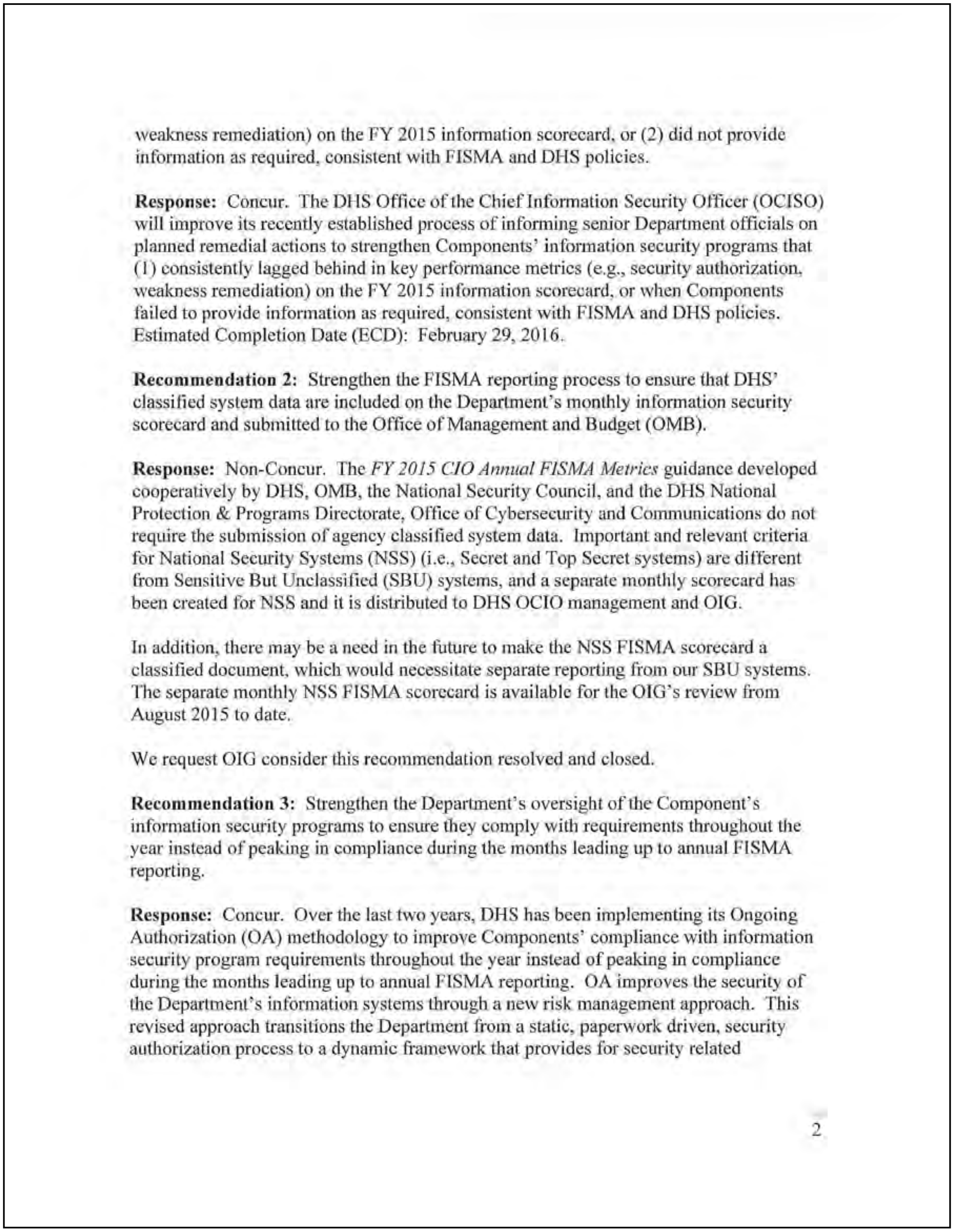
Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the Office of Inspector General's (OIG) work in planning and conducting its review and issuing this report.

DHS is pleased to note the OIG's recognition that the Department has strengthened its information security program by developing and implementing the *Fiscal Year 2015 Information Security Performance Plan* to define the performance requirements, priorities, and overall goals for the Department. DHS addressed the President's cybersecurity priorities including information security continuous monitoring; identity, credential, and access management; and anti-phishing and malware defense to ensure secure access to the information systems.

In addition, DHS maintained and annually updated its Federal Information Security Modernization Act of 2014 (FISMA) systems inventory, including agency and contractor systems. A total of eight Components met or exceeded the Department's target of 95 percent for hardware asset monthly reporting on DHS' information security scorecard.

The draft report contained six recommendations. DHS concurs with five of the recommendations and non-concurs with one. Specifically, OIG recommended that the DHS Chief Information Security Officer (CISO):

Recommendation 1: Establish a process to inform senior Department officials on planned remedial actions to strengthen Components' information security programs that consistently lagged behind in key performance metrics (e.g., security authorization,



weakness remediation) on the FY 2015 information scorecard, or (2) did not provide information as required, consistent with FISMA and DHS policies.

Response: Concur. The DHS Office of the Chief Information Security Officer (OCISO) will improve its recently established process of informing senior Department officials on planned remedial actions to strengthen Components' information security programs that (1) consistently lagged behind in key performance metrics (e.g., security authorization, weakness remediation) on the FY 2015 information scorecard, or when Components failed to provide information as required, consistent with FISMA and DHS policies. Estimated Completion Date (ECD): February 29, 2016.

Recommendation 2: Strengthen the FISMA reporting process to ensure that DHS' classified system data are included on the Department's monthly information security scorecard and submitted to the Office of Management and Budget (OMB).

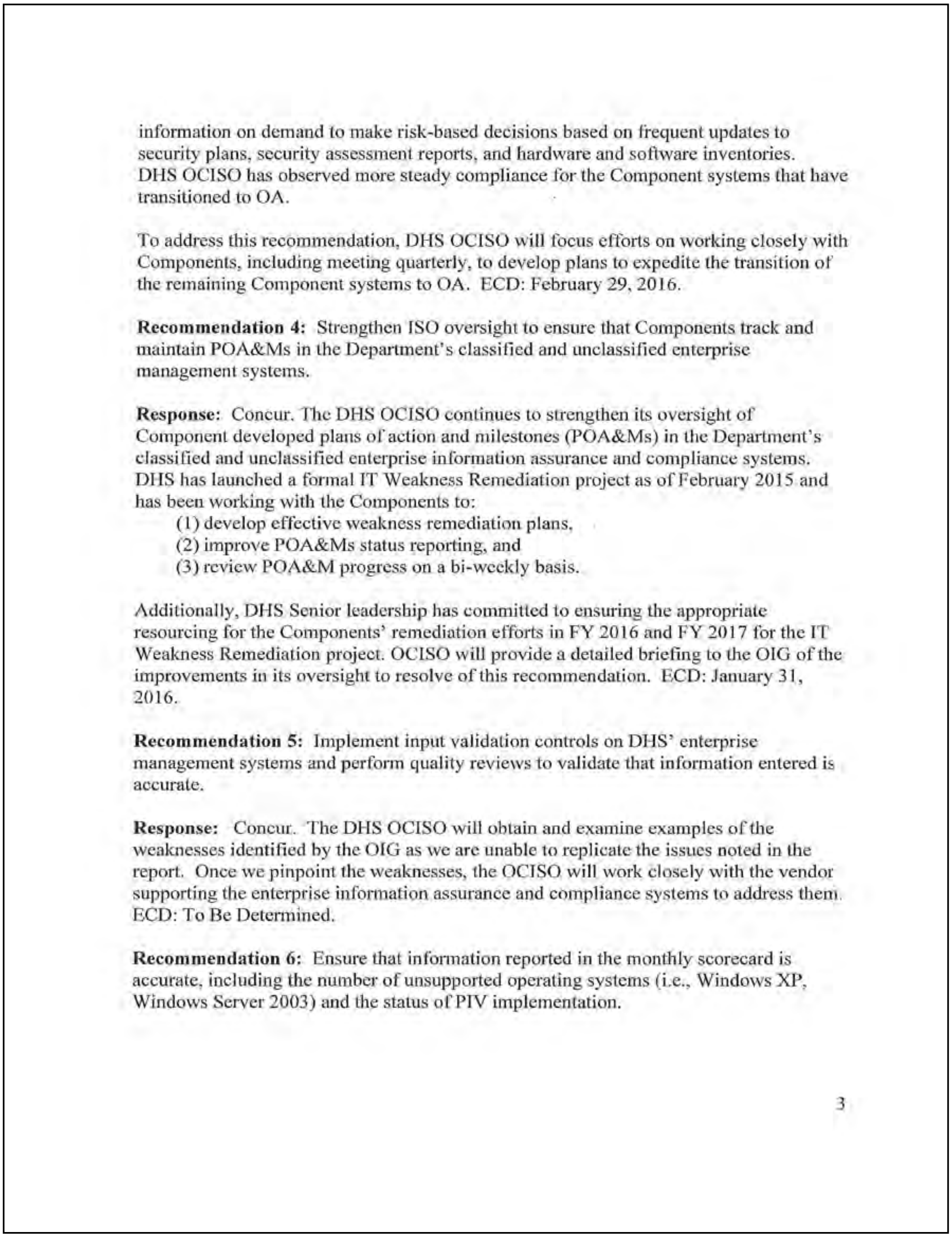
Response: Non-Concur. The *FY 2015 CIO Annual FISMA Metrics* guidance developed cooperatively by DHS, OMB, the National Security Council, and the DHS National Protection & Programs Directorate, Office of Cybersecurity and Communications do not require the submission of agency classified system data. Important and relevant criteria for National Security Systems (NSS) (i.e., Secret and Top Secret systems) are different from Sensitive But Unclassified (SBU) systems, and a separate monthly scorecard has been created for NSS and it is distributed to DHS OCIO management and OIG.

In addition, there may be a need in the future to make the NSS FISMA scorecard a classified document, which would necessitate separate reporting from our SBU systems. The separate monthly NSS FISMA scorecard is available for the OIG's review from August 2015 to date.

We request OIG consider this recommendation resolved and closed.

Recommendation 3: Strengthen the Department's oversight of the Component's information security programs to ensure they comply with requirements throughout the year instead of peaking in compliance during the months leading up to annual FISMA reporting.

Response: Concur. Over the last two years, DHS has been implementing its Ongoing Authorization (OA) methodology to improve Components' compliance with information security program requirements throughout the year instead of peaking in compliance during the months leading up to annual FISMA reporting. OA improves the security of the Department's information systems through a new risk management approach. This revised approach transitions the Department from a static, paperwork driven, security authorization process to a dynamic framework that provides for security related



information on demand to make risk-based decisions based on frequent updates to security plans, security assessment reports, and hardware and software inventories. DHS OCISO has observed more steady compliance for the Component systems that have transitioned to OA.

To address this recommendation, DHS OCISO will focus efforts on working closely with Components, including meeting quarterly, to develop plans to expedite the transition of the remaining Component systems to OA. ECD: February 29, 2016.

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

Response: Concur. The DHS OCISO continues to strengthen its oversight of Component developed plans of action and milestones (POA&Ms) in the Department's classified and unclassified enterprise information assurance and compliance systems. DHS has launched a formal IT Weakness Remediation project as of February 2015 and has been working with the Components to:

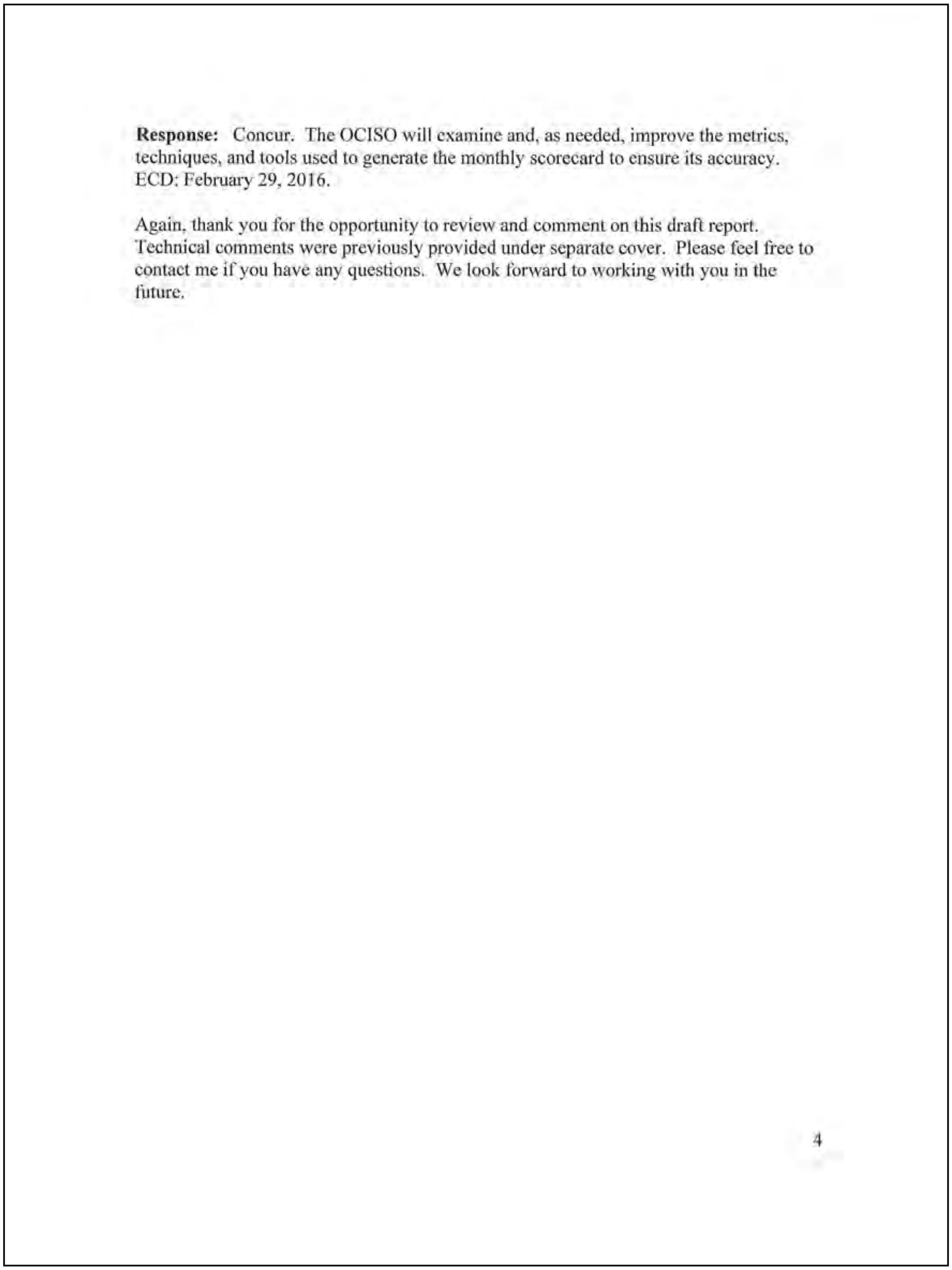
(1) develop effective weakness remediation plans,
(2) improve POA&Ms status reporting, and
(3) review POA&M progress on a bi-weekly basis.

Additionally, DHS Senior leadership has committed to ensuring the appropriate resourcing for the Components' remediation efforts in FY 2016 and FY 2017 for the IT Weakness Remediation project. OCISO will provide a detailed briefing to the OIG of the improvements in its oversight to resolve of this recommendation. ECD: January 31, 2016.

Recommendation 5: Implement input validation controls on DHS' enterprise management systems and perform quality reviews to validate that information entered is accurate.

Response: Concur. The DHS OCISO will obtain and examine examples of the weaknesses identified by the OIG as we are unable to replicate the issues noted in the report. Once we pinpoint the weaknesses, the OCISO will work closely with the vendor supporting the enterprise information assurance and compliance systems to address them. ECD: To Be Determined.

Recommendation 6: Ensure that information reported in the monthly scorecard is accurate, including the number of unsupported operating systems (i.e., Windows XP, Windows Server 2003) and the status of PIV implementation.



Response: Concur. The OCISO will examine and, as needed, improve the metrics, techniques, and tools used to generate the monthly scorecard to ensure its accuracy. ECD: February 29, 2016.

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.

Appendix C

System Inventory

Section 1: System Inventory							
Identify the number of agency and contractors' systems by Component and FIPS Pub 199 impact level (low, moderate, high). Please also identify the number of systems that are used by your agency but owned by another Federal agency (i.e., ePayroll, etc.) by Component and FIPS Pub 199 impact level.							
		A. Agency Systems		**B. Contractor Systems**		**Total Number of Systems (Agency and Contractor systems) (Column A + Column B)**	
Component	**FIPS Pub 199 System Impact Level**	**Number**	**Number Reviewed by OIG**	**Number**	**Number Reviewed by OIG**	**Total Number**	**Total Number Reviewed by OIG**
CBP	High	13	4	0	0	13	4
	Moderate	66	3	2	0	68	3
	Low	0	0	0	0	0	0
	Undefined	2	0	0	0	2	0
	Sub total	**81**	**7**	**2**	**0**	**83**	**7**

DHS HQ	High	17	1	3	0	20	1
	Moderate	24	1	8	0	32	1
	Low	0	0	3	0	3	0
	Undefined	5	0	0	0	5	0
	Sub total	**46**	**2**	**14**	**0**	**60**	**2**
FEMA	High	68	5	2	0	70	5
	Moderate	86	3	9	0	95	3
	Low	11	0	0	0	11	0
	Undefined	37	1	0	0	37	1
	Sub total	**202**	**9**	**11**	**0**	**213**	**9**
FLETC	High	0	0	0	0	0	0
	Moderate	9	0	2	0	11	0
	Low	0	0	1	0	1	0
	Undefined	0	0	0	0	0	0
	Sub total	**9**	**0**	**3**	**0**	**12**	**0**
ICE	High	12	3	0	0	12	3
	Moderate	35	4	5	0	40	4
	Low	1	0	0	0	1	0
	Undefined	1	1	0	0	1	1
	Sub total	**49**	**8**	**5**	**0**	**54**	**8**
NPPD	High	5	0	4	0	9	0
	Moderate	11	2	6	0	17	2
	Low	0	0	0	0	0	0
	Undefined	2	0	0	0	2	0
	Sub total	**18**	**2**	**10**	**0**	**28**	**2**

OIG	High	2	1	0	0	2	1
	Moderate	0	0	0	0	0	0
	Low	0	0	0	0	0	0
	Undefined	0	0	0	0	0	0
	Sub total	**2**	**1**	**0**	**0**	**2**	**1**
S&T	High	1	0	0	0	1	0
	Moderate	11	0	10	0	21	0
	Low	1	0	0	0	1	0
	Undefined	2	0	0	0	2	0
	Sub total	**15**	**0**	**10**	**0**	**25**	**0**
TSA	High	18	2	0	0	18	2
	Moderate	37	5	7	0	44	5
	Low	6	0	2	0	8	0
	Undefined	5	0	0	0	5	0
	Sub total	**66**	**7**	**9**	**0**	**75**	**7**
USCG	High	7	5	5	0	12	5
	Moderate	63	11	15	1	78	12
	Low	3	1	0	0	3	1
	Undefined	36	0	0	0	36	0
	Sub total	**109**	**17**	**20**	**1**	**129**	**18**
USCIS	High	5	0	0	0	5	0
	Moderate	38	2	2	0	40	2
	Low	0	0	0	0	0	0
	Undefined	0	0	1	0	1	0
	Sub total	**43**	**2**	**3**	**0**	**46**	**2**

USSS	High	5	0	0	0	5	0
	Moderate	10	3	0	0	10	3
	Low	0	0	0	0	0	0
	Undefined	1	0	0	0	1	0
	Sub total	**16**	**3**	**0**	**0**	**16**	**3**
Agency	**High**	**153**	**21**	**14**	**0**	**167**	**21**
	Moderate	**390**	**34**	**66**	**1**	**456**	**35**
	Low	**22**	**1**	**6**	**0**	**28**	**1**
	Undefined	**91**	**2**	**1**	**0**	**92**	**2**
	Total	**656**	**58**	**87**	**1**	**743**	**59**

Source: OIG-generated based on data from DHS' Enterprise Management System and CISO personnel.

Appendix D

Status of Risk Management Program

Section 2: Status of Risk Management Program	
Has the organization established a risk management 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. Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1.	**Yes**
2. Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800-37, Rev. 1.	**Yes**
3. Addresses risk from an information system perspective and is guided by the risk decisions from an organizational perspective and the mission and business perspective, as described in NIST SP 800-37, Rev. 1.	**Yes**
4. Has an up-to-date system inventory.	**Yes**
5. Categorizes information systems in accordance with government policies.	**Yes (See Comments)**
6. Selects an appropriately tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.	**Yes**
7. Implements the approved set of tailored baseline security controls.	**Yes**
8. Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	**Yes**
9. Authorizes information system operation 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.	**Yes (See Comments)**
10. Information-system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization.	**Yes**
11. Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO).	**Yes**

12. Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information-system-related security risks.	**Yes**
13. SA package contains system security plan, security assessment report, POA&M, accreditation boundaries in accordance with government policies for organization information systems (NIST SP 800-18, 800-37 Rev. 1).	**Yes (See Comments)**
14. The organization has an accurate and complete inventory of their cloud systems, including identification of Fed RAMP approval status.	**Yes**
15. For cloud systems, the organization can identify the security controls, procedures, policies, contracts, and service level agreements (SLA) in place to track the performance of the Cloud Service Provider (CSP) and manage the risks of Federal program and personal data stored on cloud systems.	**Yes**
Comments:	• DHS' inventory comprised of 743 information systems that were reported as "operational," including a mix of major applications and general support systems that were classified as "SBU" (673), "Secret" (62), and "Top Secret"(8). • DHS had 203 systems classified as "SBU" and 17 systems classified as "Secret" or "Top Secret" operating without ATO. • Based on our quality review of 10 SA packages at selected Components, we identified the following deficiencies: ➢ The system security plans for six systems did not contain the required security controls. ➢ The FIPS 199 artifacts for two systems were either improperly categorized or had missing information. ➢ The security assessment plans for two systems did not include specific procedures for testing the required security controls.

Appendix E

Status of Configuration Management Program

Section 3: Status of Configuration Management Program	
Has the organization established a security configuration management 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 configuration management.	**Yes**
2. Defined standard baseline configurations.	**Yes**
3. Assessments of compliance with baseline configurations.	**Yes**
4. Process for timely (as specified in organization policy or standards) remediation of scan result deviations.	**Yes**
5. For Windows-based Components, USGCB secure configuration settings are fully implemented, and any deviations from USGCB baseline settings are fully documented.	**No (See Comments)**
6. Documented proposed or actual changes to hardware and software configurations.	**Yes**
7. Implemented software assessing (scanning) capabilities (NIST SP 800-53: RA-5, SI-2).	**Yes**
8. Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2).	**No (See Comments)**
9. Patch management process is fully developed, as specified in organization policy or standards, including timely and secure installation of software patches (NIST SP 800-53; CM-3, SI-2).	**Yes**
10. Does the organization have an enterprise deviation handling process and is it integrated with an automated scanning capability?	**Yes**
11. Is there a process for mitigating the risk introduced by those deviations? A deviation is an authorized departure from an approved configuration. As such it is not remediated but may require compensating controls to be implemented.	**Yes**

Comments:	• The Department has published guidelines that enforce USGCB settings, and approved deviations are documented in the guidelines. Further, the Department has established processes for approval of configuration-related weaknesses. However, Components still are not fully implementing required guidelines or seeking approval from DHS Management for non-compliant settings: ➢ FEMA only implemented 38 percent of the USGCB settings for its Windows XP operating system. ➢ NPPD implemented the USGCB settings for its Windows 7 and Windows XP operating systems at 73 percent and 76 percent, respectively. ➢ TSA implemented 98 percent of the USGCB settings for its Windows 7 operating system. • Components have not implemented all of the required DHS baseline configuration guidance settings. • We identified missing security patches on Windows 8.1, Windows 7, and Windows XP workstations selected for review.

Appendix F

Status of Incident Response and Reporting Program

Section 4: Status of Incident Response & Reporting Program	
Has the organization established an incident response and reporting 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 detecting, responding to, and reporting incidents (NIST SP 800-53: IR-1).	**Yes**
2. Comprehensive analysis, validation, and documentation of incidents.	**Yes**
3. When applicable, reports to US-CERT within established timeframes (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).	**Yes**
4. When applicable, reports to law enforcement and the agency Inspector General within established timeframes (SP 800-61).	**Yes**
5. Responds to and resolves incidents in a timely manner, as specified in organization policy or standards, to minimize further damage (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).	**Yes**
6. Is capable of correlating incidents.	**Yes**
7. Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).	**Yes**
Comments:	• Components are required to submit weekly incident reports to the DHS SOC. However, only USCG and USCIS regularly submitted incident reports to the SOC in FY 2015.

Appendix G

Status of Security Training Program

Section 5: Status of Security Training Program	
Has the organization established a security training 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 security awareness training (NIST SP 800-53: AT-1).	**Yes**
2. Documented policies and procedures for specialized training for users with significant information security responsibilities.	**Yes**
3. Security training content based on the organization and roles, as specified in organization policy or standards.	**Yes**
4. Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other organization users) with access privileges that require security awareness training.	**Yes**
5. Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training.	**No (See Comments)**
6. Training material for security awareness training contains appropriate content for the organization (NIST SP 800-50, 800-53).	**Yes**
Comments:	• Some Components did not report monthly the numbers of employees who had received IT security awareness and privileged training as required. • As of August 2015, NPPD and USSS had submitted no report on privileged user training completion during the year. Additionally, ICE, TSA, and USCIS collectively had nearly 600 privileged users that had not completed specialized training.

Appendix H

Status of Plan of Action and Milestones Program

Section 6: 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. Documented 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.	**No (See Comments)**
5. Ensures resources and ownership are provided for correcting weaknesses.	**No (See Comments)**
6. POA&Ms include security weaknesses discovered during assessments of security controls and 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. Costs associated with remediating weaknesses are identified in terms of dollars (NIST SP 800-53, Control PM-3; OMB M-04-25).	**No (See Comments)**
8. Program officials report progress on remediation to Chief Information Officer on a regular basis, at least quarterly, and the Chief Information Officer centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53: CA-5; OMB M-04-25).	**Yes**

Comments:	- Component personnel did not perform adequate POA&M reviews on systems. - FEMA had not created any POA&Ms for 11 systems classified as "Secret" or "Top Secret" that were operating without ATOs. - 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. - As of June 2015, we identified the following deficiencies in the Department's unclassified enterprise management system: ➢ Of the 22,294 open SBU POA&Ms, 17,663 (79 percent) were overdue. Moreover, 7,665 of the POA&Ms were at least 3 months late while 75 POA&Ms were more than 1 year past due. ➢ Of the 22,294 open SBU POA&Ms, 20,423 (92 percent) had weakness remediation estimates less than $50.

Appendix I

Status of Remote Access Program

Section 7: 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. Protects against unauthorized connections or subversion of authorized connections.	**Yes**
3. Users are uniquely identified and authenticated for all access (NIST SP 800-46, Section 4.2, Section 5.1).	**Yes**
4. Telecommuting policy is fully developed (NIST SP 800-46, Section 5.1).	**Yes**
5. Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms.	**Yes**
6. Defines and implements encryption requirements for information transmitted across public networks.	**Yes**
7. Remote access sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required.	**Yes**
8. Lost or stolen devices are disabled and appropriately reported (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines).	**Yes**
9. Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4).	**Yes**
10. Remote-access user agreements are adequate in accordance with government policies (NIST SP 800-46, Section 5.1; NIST SP 800-53, PS-6).	**Yes**
11. Does the organization have a policy to detect and remove unauthorized (rogue) connections?	**Yes**
Comments:	• As of July 2015, CBP, FEMA, NPPD, and TSA had 40 connections that had yet to be consolidated behind a trusted internet connection as required.

Appendix J

Status of Identity and Access Management Program

Section 8: Status of Identity and Access Management Program	
Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines, and which identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes?	
1. Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1).	**Yes**
2. Identifies all users, including Federal employees, contractors, and others who access organization systems (NIST SP 800-53, AC-2).	**Yes**
3. Organization has planned for implementation of PIV for logical 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**
4. Organization has adequately planned for implementation of 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. Ensures that the users are granted access based on needs and separation-of-duties principles.	**Yes**
6. Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, or servers) from those without user accounts (e.g., IP phones, faxes, printers).	**Yes**
7. Ensures that accounts are terminated or deactivated once access is no longer required according to organizational policy.	**Yes**
8. Identifies and controls use of shared accounts.	**Yes**
Comments:	• According to OCIO officials, USCG no longer reported key information security metrics to DHS. Instead, USCG had begun reporting its PIV implementation for unprivileged and privileged access accounts to the Defense Information Systems Agency. • As of July 2015, NPPD had not implemented PIV for its unprivileged access accounts. Further, USSS had received a score of 9 percent for implementation of PIV logical access for its unprivileged access accounts, versus a target score of 100 percent mandatory PIV use.

Appendix K

Status of Continuous Monitoring Program

Section 9: Status of Continuous Monitoring Program	
Utilizing the ISCM maturity model definitions, please assess the maturity of the organization's ISCM program along the domains of people, processes, and technology. Provide a maturity level for each of these domains as well as for the ISCM program overall.	
1. Please provide the D/A ISCM maturity level for the People domain.	**Defined (Level 2)**
2. Please provide the D/A ISCM maturity level for the Processes domain.	**Defined (Level 2)**
3. Please provide the D/A ISCM maturity level for the Technology domain	**Defined (Level 2)**
4. Please provide the D/A ISCM maturity level for the ISCM Program Overall.	**Defined (Level 2)**
Comments:	• As of August 2015, only 82 operational systems were included in the OA program. • DHS had not implemented an ISCM program for the Department's classified systems. • We identified the following deficiencies, which may restrict Components from protecting their systems or preventing unauthorized software/hardware from being installed on their information technology assets: ➢ Four Components did not perform network penetration testing. ➢ Five Component systems did not have the technical capability to block unauthorized software from being introduced to any device on the network. ➢ Three Components did not have the technical ability to block unauthorized hardware (e.g., USB drives) from connecting to any devices on the network.

Appendix L

Status of Contingency Planning Program

Section 10: Status of Contingency Planning Program	
Has the organization established an enterprise wide business continuity/disaster recovery 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 business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST SP 800-53: CP-1).	**Yes**
2. The organization has incorporated the results of its system's Business Impact Analysis (BIA) into the appropriate analysis and strategy development efforts for the organization's Continuity of Operations Plan, Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) (NIST SP 800-34).	**Yes**
3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures (NIST SP 800-34).	**Yes**
4. Testing of system-specific contingency plans.	**Yes**
5. The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34).	**Yes**
6. Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53).	**Yes**
7. Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans.	**Yes**
8. After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34).	**Yes**
9. Alternate processing sites are not subject to the same risks as primary sites. Organization contingency planning program identifies alternate processing sites for systems that require them (FCD1, NIST SP 800-34, NIST SP 800-53).	**Yes**
10. Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).	**Yes**
11. Contingency planning that considers supply chain threats.	**Yes**

Comments:	• For the previous 12 months, DHS and its Components had not tested contingency plans for 106 operational systems with an overall FIPS security category of moderate or high. • Our review of 10 SA packages identified deficiencies related to system contingency planning documentation. • CBP did not update the contingency plan for its Analytical Framework for Intelligence system to address deficiencies identified in the last contingency plan test. As a result, CBP may have encountered difficulties restoring its operations in the event of a service disruption.

Appendix M

Status of Agency Program to Oversee Contractor Systems

Section 11: 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. Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities (including other government agencies), including organization systems and services residing in a public, hybrid, or private cloud.	**Yes**
2. The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and compliant with FISMA requirements, OMB policy, and applicable NIST guidelines (NIST SP 800-53: CA-2).	**Yes**
3. A complete inventory of systems operated on the organization's behalf by contractors or other entities (including other government agencies), including organization systems and services residing in a public, hybrid, or private cloud.	**Yes**
4. The inventory identifies interfaces between these systems and organization-operated systems (NIST SP 800-53: PM-5).	**Yes**
5. The organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.	**Yes**
6. The inventory of contractor systems is updated at least annually.	**Yes**
Comments:	

Appendix N

Major Office of Information Technology Audit Contributors to This Report

Chiu-Tong Tsang, Director
Tarsha Cary, IT Audit Manager
Aaron Zappone, Supervisory Program Analyst
Thomas Rohrback, IT Specialist
Tonya McKinnon, IT Auditor
Anthony Nicholson, Referencer

Appendix O

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