

OFFICE OF INSPECTOR GENERAL

Evaluation of DHS' Information Security Program for Fiscal Year 2014



Homeland
Security

December 12, 2014
OIG-15-16



HIGHLIGHTS

Evaluation of DHS' Information Security Program for Fiscal Year 2014

December 12, 2014

Why We Did This

We reviewed Department of Homeland Security's (DHS) information security program in accordance with the *Federal Information Security Management Act of 2002* (FISMA). Our objective was to determine whether DHS' information security program is adequate, effective, and in compliance with FISMA requirements.

What We Recommend

We recommended that DHS further strengthen its information security program in the areas of continuous monitoring, security authorization, configuration management, and information technology (IT) security weakness remediation.

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 steps to improve its information security program. For example, DHS expanded the ongoing authorization program to improve the security of its information systems through a revised risk management approach. Additionally, DHS developed and implemented the *Fiscal Year 2014 Information Security Performance Plan*, which defines the performance requirements, priorities, and overall goals for the Department. DHS has also taken actions to address the President's cybersecurity priorities, which include the implementation of trusted internet connections, continuous monitoring of the Department's information systems, and strong authentication.

While these efforts have resulted in some improvements, Components are not consistently following DHS' policies and procedures to update the system inventory and plan of action and milestones in the Department's enterprise management systems. Further, Components continue to operate systems without the proper authority. We also identified a significant deficiency in the Department's information security program as the United States Secret Service (USSS) did not provide the Chief Information Security Officer (CISO) with the continuous monitoring data required by the Office of Management and Budget (OMB) during Fiscal Year (FY) 2014. Without this information, CISO was significantly restricted from performing continuous monitoring on the Department's information systems, managing DHS' information security program, or ensuring compliance with the President's cybersecurity priorities. Subsequent to the completion of our fieldwork, USSS established an agreement with the DHS Chief Information Officer (CIO) to provide the required data beginning in FY 2015.

DHS CISO Response

We are making six recommendations to the CISO. The Department concurred with all recommendations.



Table of Contents

Results of Evaluation	4
Background	5
Details	6
Recommendations.....	26
Management Comments and OIG Analysis	27

Appendixes

Appendix A: Transmittal to Action Official.....	31
Appendix B: Scope and Methodology.....	32
Appendix C: Management Comments to the Draft Report.....	34
Appendix D: System Inventory	39
Appendix E: Status of Risk Management Program.....	42
Appendix F: Status of Configuration Management Program.....	44
Appendix G: Status of Incident Response and Reporting Program	45
Appendix H: Status of Security Training Program	46
Appendix I: Status of Plan of Action and Milestones Program	47
Appendix J: Status of Remote Access Program.....	49
Appendix K: Status of Account and Identity Management Program	50
Appendix L: Status of Continuous Monitoring Program	51
Appendix M: Status of Contingency Planning Program	52
Appendix N: Status of Agency Program to Oversee Contractor Systems.....	53
Appendix O: Status of Security Capital Planning Program.....	54
Appendix P: FY 2014 Information Security Scorecard Metric Descriptions	55
Appendix Q: Inspector General Memorandum Regarding USSS' Refusal to Provide Continuous Monitoring Data Feeds	56
Appendix R: USSS Acting Director's Response to Inspector General's Memorandum.....	58
Appendix S: Major Contributors to This Report	59
Appendix T: Report Distribution	60



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Abbreviations

ATO	authority to operate
CBP	Customs and Border Protection
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPIC	Capital Planning and Investment Control
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002, as amended
FLETC	Federal Law Enforcement Training Center
FY	fiscal year
HQ	Headquarters
ICE	Immigration and Customs Enforcement
ISCM	Information System Continuous Monitoring
IT	information technology
NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
S&T	Science and Technology Directorate
SBU	sensitive but unclassified
TIC	Trusted Internet Connections
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



Results of Evaluation

We conducted an independent evaluation of the DHS information security program and practices to comply with the requirements of FISMA. In evaluating DHS' progress in implementing its agency-wide information security program, we specifically assessed the Department's plan of action and milestones (POA&M), security authorization processes, and continuous monitoring programs.

DHS has taken steps to improve its information security program. For example, during the past year, DHS expanded its ongoing authorization program to improve the security of its 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 can provide authorization officials access to security-related information on demand to make risk-based decisions. Additionally, DHS developed and implemented the *Fiscal Year 2014 Information Security Performance Plan*, which defines the performance requirements, priorities, and overall goals for the Department throughout the year. Finally, DHS has taken actions to address the President's cybersecurity priorities which include the implementation of trusted internet connections (TIC), continuous monitoring of the Department's information systems, and multi-factor authentication to gain access to information systems.

While these efforts have resulted in some improvements, Components are not consistently following DHS' policies and procedures to update its system inventories and POA&M in DHS' enterprise management systems. We also determined that Components continue to operate systems without proper authority. For example, the Federal Emergency Management Agency (FEMA) has five "Top Secret" systems that have been operating without the proper authority; some have been expired since August 2013. We also identified a significant deficiency in the Department's information security program as USSS refused to provide CISO with the continuous monitoring data feeds required by OMB. Without this information, CISO is significantly restricted from performing continuous monitoring on the Department's information systems, managing DHS' information security program, or ensuring compliance with the President's cyber priorities. Additional program areas that need improvement include configuration management, incident response and reporting, specialized training, account and identity management, POA&M, and contingency planning.

We are making six recommendations to the Chief Information Security Officer. The Department concurred with all recommendations and has begun to take actions to implement them. The Department's responses are summarized and evaluated in the body of this report and included, in their entirety, as appendix C.



Background

Recognizing the importance of information security to the economic and national security interests of the United States, the Congress enacted Title III of the *E-Government Act of 2002* (Public Law 107-347, Sections 301-305) to improve security within the Federal Government. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Title III of the *E-Government Act*, as amended, entitled *Federal Information Security Management Act of 2002*, 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 Federal 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. As specified in FISMA, agency heads are responsible for conducting an annual evaluation of information programs and systems under their purview, as well as an assessment of related security policies and procedures. FISMA also requires agencies to report any significant deficiency in the adequacy and effectiveness of information security programs as a material weakness. The Office of Inspector General (OIG), or an independent, external auditor determined by the OIG, must independently evaluate annually the effectiveness of an agency's information security program and practices.

OMB issues updated instructions annually for agency and OIG reporting under FISMA. Our annual FISMA evaluation summarizes the results of our review of DHS' information security program and practices based on the reporting metrics, dated December 2, 2013.

In 2012, the Cybersecurity Coordinator and Special Assistant to the President identified three Administration priorities and recommended that Federal agencies focus their resources on the most effective controls to improve cybersecurity and the security of Federal information systems. The priority areas include:

- Continuous Monitoring of Federal Information Systems - transforms the otherwise static security control assessment and authorization process into a dynamic risk mitigation program that provides essential, near real-time security status and remediation, increasing visibility into system operations and helping security personnel make risk-management decisions based on increased situational awareness.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

- Strong Authentication - passwords alone provide little security. Federal smartcard credentials, such as personal identity verification (PIV) and common access cards provide multi-factor authentication and digital signature and encryption capabilities, authorizing users to access Federal information systems with a higher level of assurance.
- TIC - consolidate external internet traffic and ensure a set of common security capabilities for situational awareness and enhanced monitoring.

The CISO, who leads the Information Security Office, is responsible for managing DHS' information security program and helps the Department achieve the Administration's cybersecurity priorities. To aid in managing the program, CISO developed the *Fiscal Year 2014 DHS Information Security Performance Plan* to enhance existing processes, such as risk management and continuous monitoring, aimed at addressing the Administration's cybersecurity priorities. In addition, CISO continues to improve the Department's ongoing authorization methodology to transform the security authorization process from a static paperwork driven effort to a dynamic event-triggered framework.¹

DHS relies on enterprise management systems to create and maintain security authorization documentation and to monitor POA&M activities for its unclassified systems, and those classified as "Secret." During FY 2014, DHS adopted a new enterprise-wide management system for its sensitive but unclassified (SBU) systems, aimed at improving the risk management process by creating a task-based workflow that better aligns with NIST's risk management framework.

Details

Based on the requirements outlined in FISMA and the annual reporting instructions, our independent evaluation focused on 11 key areas of DHS' information security program. Specifically, we reviewed the Department's:

- system inventory,
- risk management,
- POA&M,
- configuration management,

¹ 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.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

- incident response and reporting,
- security training,
- remote access,
- account and identity management,
- continuous monitoring,
- contingency planning, and
- security capital planning.

We separated the results of our evaluation into these key areas, and identified any significant progress made since our FY 2013 evaluation and issues that DHS needs to address.

Overall Progress

DHS has taken steps to improve its information security program during FY 2014. For example, CISO:

- incorporated 61 systems, from 5 Components, into the ongoing authorization program. This program allows the Department to migrate from a static, paperwork-driven, security authorization process (i.e., security controls are tested and documentation are updated at fixed intervals) to a dynamic framework. This framework can provide authorization officials access to security-related information on demand (e.g., frequent updates to system security plans, security assessment reports, and hardware and software inventories) to make risk-based authorization decisions.
- updated the information security scorecard to include additional or revised metrics aimed at better evaluating security processes and continuous monitoring capabilities. For example, the DHS Information Security Office has added “scan coverage” and “ongoing authorization” metrics to the FY 2014 information security scorecard.²
- conducted three site visits to perform quality reviews of selected security authorization packages on FEMA’s “Top Secret” systems.
- updated the DHS Sensitive Systems Policy Directive 4300A to reflect the changes made in various DHS security policies and applicable NIST guidance.
- updated the DHS Information Security Continuous Monitoring (ISCM) Strategy, which describes the Department’s enterprise strategy for

² Scan coverage defines the percentage of unclassified systems and assets scanned and reported to DHS CISO each month. See appendix P for the FY 2014 Information Security Scorecard Metrics Descriptions.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

achieving key continuous monitoring goals and objectives to improve the Department's IT security.³

Overall Issues To Be Addressed

In September 2013, National Security Council, OMB, and DHS Headquarters (HQ) personnel conducted a CyberStat review with FEMA.⁴ The results of the CyberStat review highlighted significant deficiencies at FEMA that may cause harm to the Department's security program if the deficiencies are not corrected timely. For example, FEMA was required to:

- identify authorizing officials and system owners for all FEMA systems;
- update National Security Council on its cybersecurity governance and budget;
- update performance plans to require authorizing officials to achieve a minimum score for cybersecurity; and
- review status regarding TIC waivers.

During the CyberStat review, reviewers expressed great concerns related to “an adversary's ability to disrupt FEMA's communications, networks, data and other critical systems during a time of need.” In the Component's response to the National Security Council, FEMA outlined the corrective action to address identified deficiencies and improve its security posture by conducting a comprehensive IT resiliency review. During this review period, the Information Security Office provided FEMA with a temporary exception for completing the required security authorization tasks within the Department's enterprise management system.

In addition, we identified a number of issues that DHS needs to address to strengthen its security program. For example, we determined that Components were not consistently following DHS' policies and procedures to update the system inventory and POA&M in the Department's enterprise management systems. We also determined that Components continued to operate systems without the proper authority and were not complying with OMB and DHS requirements for continuous monitoring. Specifically, we identified the following:

- USSS did not provide the Information Security Office with the required ISCM data feeds during FY 2014. OMB requires agencies to provide ISCM data on a monthly basis, including information related to hardware asset

³ *DHS Information Security Continuous Monitoring Strategy - An Enterprise View*, version 3.0, dated May 14, 2014.

⁴ CyberStat reviews are face-to-face, evidence-based meetings to evaluate agencies' cybersecurity performance and identify mechanisms to ensure that agencies are on track to achieve the President's cybersecurity performance goals.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

management, software asset management, configuration setting management, and common vulnerability management. To comply with this requirement, DHS and its Components must provide automated vulnerability scans for networks and systems, data from endpoint management software, and data from other security tools, which are implemented at the component or system levels.⁵ Throughout FY 2014, USSS refused to provide the CISO with the continuous monitoring data feeds. USSS' refusal to provide the required data created a significant deficiency in the Department's information security program as the CISO was severely restricted from performing continuous monitoring on the Department's information systems, managing DHS' information security program, or ensuring compliance with the President's cyber priorities. Subsequent to the issuance of the draft report, the Inspector General sent a memorandum to the Acting Director of the USSS outlining his concerns at the Component's refusal to provide the required ISCM data to the Department. Shortly after the issuance of this memorandum, USSS established an agreement with the DHS CIO on November 7, 2014, which prescribes the process that will enable the Component to provide the Department with the required ISCM data, as required by OMB. See appendixes Q and R for correspondences between the Inspector General and USSS regarding the ISCM data feeds.

- DHS and its Components are continuing to operate information systems, including systems classified as "Secret" and "Top Secret," without the proper authority to operate (ATO). When operating the systems without a valid ATO, DHS and its Components cannot ensure that they have implemented effective controls to protect the sensitive information stored and processed by these systems. In addition, OMB requires agencies not to spend funds on the development of new systems if agencies' existing operational systems do not have the proper ATO or do not meet applicable NIST and OMB security requirements (e.g., contingency plan testing).⁶
- Components are not consistently updating system inventory information in DHS' enterprise management systems. Without an accurate system inventory, DHS cannot effectively manage the Department's information system program.
- Components have not incorporated or updated all known information security weaknesses (e.g., operating systems without ATOs, prior OIG

⁵ *DHS Information Security Continuous Monitoring Strategy - An Enterprise View*, version 3.0, dated May 14, 2014.

⁶ OMB Memorandum M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, November 18, 2013.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

report recommendations) into POA&M for the Department's operational systems. When Components have not incorporated known security weaknesses into POA&M or updated these weaknesses timely, authorizing officials do not have the most accurate information to make credible risk-based decisions regarding the security posture of DHS systems. We reported a similar issue in FY 2013.⁷

- Components have not implemented all required United States Government Configuration Baseline (USGCB) and DHS baseline configuration settings on the information systems selected for review.
- FEMA and United States Citizenship and Immigration Service (USCIS) are still using the Microsoft Windows XP operating system, which may be vulnerable to potential exploits as Microsoft stopped providing software updates to mitigate security vulnerabilities in April 2014.
- USCIS was not mitigating high-risk vulnerabilities timely. For example, the DHS Security Operations Center issued an alert on June 27, 2014, requiring Components to mitigate "Heartbleed" vulnerability by July 7, 2014.⁸ However, the results from our vulnerability assessments performed on July 23, 2014, revealed that two USCIS workstations had software that was vulnerable to Heartbleed. While USCIS notified us that it had removed the vulnerable software subsequent to our testing, the delay in mitigating the high-risk vulnerability may have exposed sensitive DHS data to potential exploits.

System Inventory

DHS continues to maintain and update its FISMA systems inventory, including agency and contractor systems, on an annual basis. In addition, DHS conducts site visits as part of its annual inventory refresh process to engage directly with Component personnel, identify missing systems, and resolve any other inventory issues.

Progress

As of July 2014, DHS inventory included a total of 652 information systems that were reported as "operational," which include major applications and general support systems that were classified as "SBU,"

⁷ *Evaluation of DHS' Information Security Program for Fiscal Year 2013*, (OIG-14-09, November 2013).

⁸ The Heartbleed vulnerability undermines the encryption process on secure websites, email, instant messaging, and a wide variety of other programs and applications. In addition, if a user's password is intercepted, then a malicious actor could use that password to access the user's account.



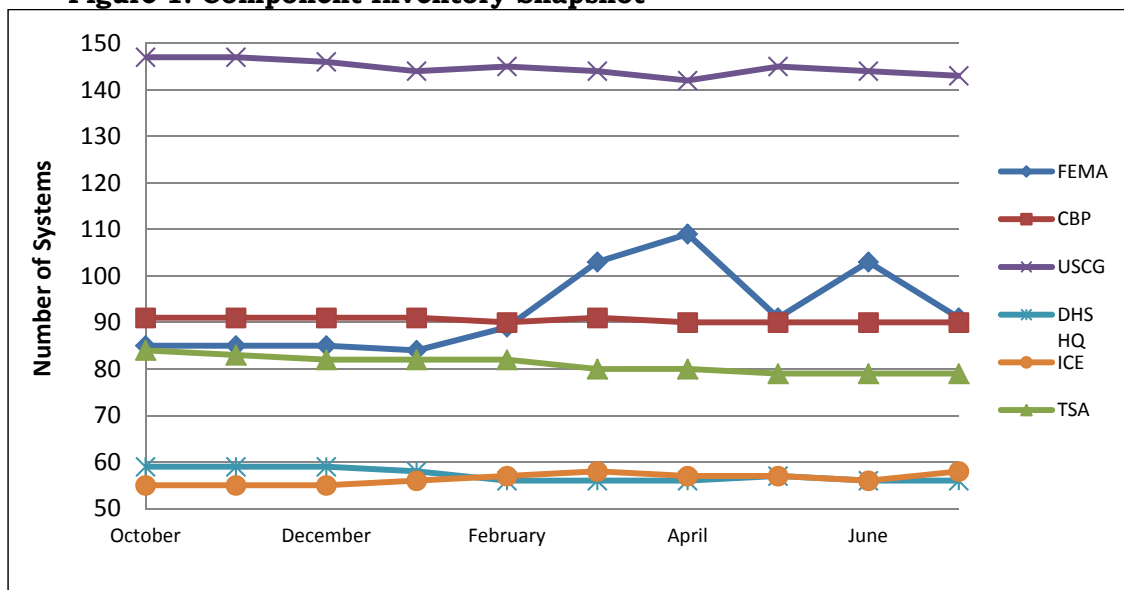
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

“Secret,” and “Top Secret.”⁹ In addition, DHS identified 145 mission essential systems.

Issues To Be Addressed

- FEMA’s system inventory fluctuated significantly between October 2013 and July 2014. Specifically, FEMA reported 85 operational systems in October 2013. The number of systems dropped to 84 in January 2014, increased to 109 in April 2014, and then decreased to 91 systems in July 2014. Due to the lag time required to develop or procure a new system, system inventory levels should not fluctuate significantly from one month to the next. These abnormal fluctuations may indicate that either the Department’s inventory methodology is not accurately capturing the number of systems that Components maintain or Components are circumventing the Department’s capital planning investment process to procure or develop new systems. Figure 1 depicts the fluctuations in system inventory at DHS HQ, FEMA, Transportation Security Administration (TSA), United States Coast Guard (USCG), United States Customs and Border Protection (CBP), and United States Immigration and Customs Enforcement (ICE) between October 2013 and July 2014.

Figure 1: Component Inventory Snapshot



Source: OIG compiled based on data from DHS’ information security scorecards.

⁹ For FISMA reporting purposes, DHS “operational” inventory includes systems in the implementation, modification, and operational system engineering life cycles.
www.oig.dhs.gov



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

- FEMA is not updating the Department’s enterprise management tools to maintain an accurate inventory of its information systems. For example, one FEMA “Top Secret” system, which was decommissioned in 2012, was still reported as operational in DHS’ enterprise management tools in August 2014.
- As of June 2014, DHS only conducted 4 of 23 planned site visits to update its system inventory at selected Components, compared to more than 100 site visits conducted in FY 2013.

See appendix D for information on DHS’ System Inventory and appendix N for the Status of DHS’ Agency Program to Oversee Contractor Systems.

Risk Management Program

Security authorization is the official management decision given by a senior organizational official to authorize operation of an information system and to 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.¹⁰ In addition, the security authorization 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-wide systems to incorporate NIST security controls when performing security authorization on their systems. The enterprise-wide management systems enable Components to develop and maintain system security documentation as well as centralize the documents supporting the ATO for each system.

Components are required to use the automated systems to apply NIST security controls for all system security authorizations. DHS uses security authorization artifacts created in its enterprise management tools by the Components, to monitor their progress in authorizing systems, which 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; and

¹⁰ DHS *Security Authorization Process Guide*, Version 10, June 6, 2013.
www.oig.dhs.gov



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

- Annual Self-Assessment.

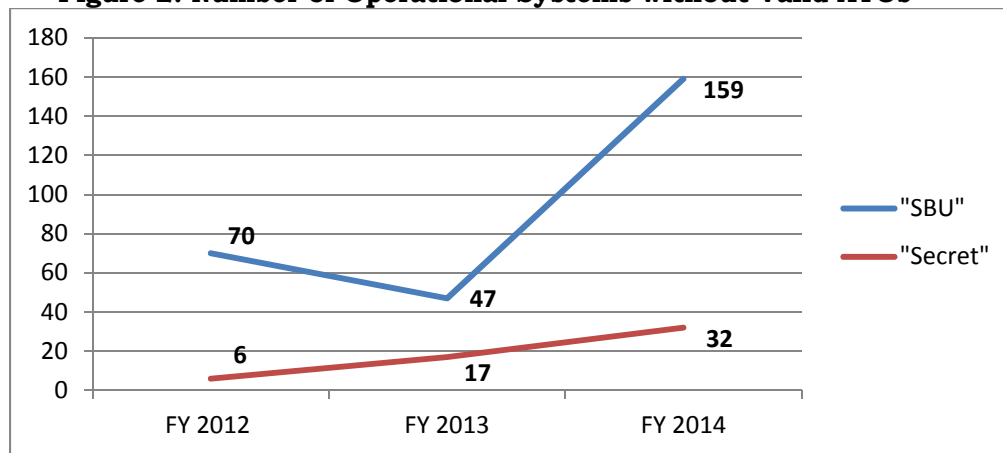
Progress

As of July 2014, OIG, TSA, and USCIS had attained 100 percent compliance for the Department’s security authorization metric.

Issues To Be Addressed

- The number of “SBU” and “Secret” systems without valid ATOs has increased significantly over the past 3 years. For example, the number of “Secret” systems without a valid ATO increased from 6 in FY 2012 to 32 in FY 2014. In addition, the number of “SBU” systems increased from 70 in FY 2012 to 159 in FY 2014. Figure 2 illustrates the number of “SBU” and “Secret” systems that have been operating without a valid ATO between FY 2012 and FY 2014.

Figure 2: Number of Operational Systems without Valid ATOs



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

- DHS adopted a new enterprise management system to manage and track the security authorization process for its “SBU” systems. During our evaluation, we identified the following issues associated with the new system:
 - Training data (statistics for specialized and IT security awareness training) are not being tracked or recorded within the system.
 - System contingency planning test dates were inaccurate.
 - POA&M quality check functionalities had not been fully enabled.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

- The Department’s overall security authorization score is 74 percent, well below DHS’ FY 2014 target of 90 percent. We also identified the following deficiencies:
 - FEMA, ICE, USCG, and USSS have not satisfied the Department's requirement for security authorization and received scores of 30, 79, 51, and 76 percent, respectively.
 - 159 systems classified as “SBU” operate without a valid ATO.
 - 32 systems classified as “Secret” operate without a valid ATO.
 - Five “Top Secret” FEMA systems operate without a valid ATO and some have been expired since August 2013.
- FEMA could not provide the annual assessment results for two of its “Top Secret” systems. FISMA and DHS require controls be tested annually. When controls are not tested, FEMA cannot ensure whether implemented controls are operating as designed on its “Top Secret” systems.
- Based on our review of 11 security authorization packages at selected Components, we identified the following deficiencies in the security artifacts:
 - The ATO letters for two systems did not specify the outstanding risks identified during the security authorization process.
 - Components had not completed their required NIST 800-53 annual self-assessment for three systems.
 - The system security plans for seven systems did not contain the required controls, supporting artifacts for testing, and memorandums of understanding/memorandums of agreement.
 - The FIPS 199 artifacts for three systems were either not categorized correctly or there were inconsistencies between the FIPS 199 workbook and other security authorization documentation.

See appendix E for Status on DHS’ Risk Management Program.

Plan of Action and Milestones Program

OMB and DHS require the creation and maintenance of POA&M for all known IT security weaknesses. In addition, DHS performs automated quality reviews on its unclassified and classified POA&M (i.e., “Secret”) for accuracy and completeness and provides the results to Components daily. Despite these efforts, Components are not entering and tracking all IT security weaknesses in DHS’ unclassified and classified enterprise management systems.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Progress

During FY 2014, DHS conducted quality reviews of the POA&M for its “Top Secret” systems.

Issues To Be Addressed

- DHS and its Components have not created POA&M for operational systems that do not have valid ATOs. Without creating POA&M, authorizing officials do not have the most accurate information to make credible risk-based decisions or cannot ensure that all IT security weaknesses have been identified and mitigated in accordance with applicable guidance.
- POA&M were not created for all IT security weakness identified in OIG audit reports. For example, DHS and its Components did not create POA&M for the IT security weaknesses that were identified in the following OIG audit reports:
 - *DHS Needs to Address Portable Device Security* (OIG-12-88, June 2012).
 - *Progress Has Been Made in Securing Laptops and Wireless Networks at FEMA* (OIG-12-93, June 2012).
 - *Evaluation of DHS’ Information Security Program for Fiscal Year 2012* (OIG-13-04, October 2012).
 - *USCG Must Improve the Security and Strengthen the Management of Its Laptops* (OIG-13-93, May 2013).
- FEMA could not provide documentation to support that it maintains POA&M for three of its “Top Secret” systems.
- DHS requires Components to close POA&M within 6 months, including those resulting from previous OIG audit findings. However, DHS has not consistently provided the OIG with timely updates or corrective actions regarding previous audit reports. For example, we have not received any status updates regarding OIG-12-88 since October 26, 2012.¹¹ In addition, we have not received any updates for OIG-13-04 since November 26, 2013.¹²
- Components did not correct all deficiencies identified during DHS’ POA&M quality reviews. Our review of DHS’ quality reports identified repeated deficiencies, such as inaccurate milestones,

¹¹ *DHS Needs to Address Portable Device Security* (OIG-12-88, June 2012).

¹² *Evaluation of DHS’ Information Security Program for Fiscal Year 2012* (OIG-13-04, October 2012).



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

lack of resources to mitigate the weaknesses, and delays in resolving the POA&M. We identified similar problems in our FY 2012 and FY 2013 FISMA reports.

- Components did not maintain current information on the progress of security weakness remediation, and did not resolve all POA&M in a timely manner. We identified the following deficiencies:
 - Components did not update information concerning all weaknesses. DHS requires Components to complete POA&M within 6 months. However, 1,497 (47 percent) of the 3,206 open “SBU” POA&M were delayed. Further, 517 POA&M (16 percent) were past due by 12 months (prior to July 15, 2013). In addition, 199 (6 percent) of open POA&M have been designated as significant deficiencies. We determined that 39 (20 percent) of the 199 significant deficiencies identified were delayed. Further, 230 (7 percent) open POA&M have not been properly assigned a “Severity Level,” as required by DHS guidance.
 - There were 128 POA&M for DHS’ “Secret” systems that were not mitigated. Specifically, 39 (30 percent) of the open POA&M were delayed and 7 (5 percent) of the 128 POA&M were not prioritized, as required by DHS guidance.
- Components only created POA&M for 97 of 103 (94 percent) notices of findings and recommendations for the weaknesses identified during our FY 2013 financial statement audit.¹³
- The results from our quality review of 11 security authorization packages revealed that Components have not created POA&M for the weaknesses identified from contingency plan testing.

See appendix I for Status on DHS’ POA&M Program.

Configuration Management

Issues To Be Addressed

We selected 26 systems from 11 Components [CBP, DHS HQ, FEMA, ICE, National Protection and Programs Directorate (NPPD), OIG, Science and Technology Directorate (S&T), TSA, USCG, USCIS, and USSS] to evaluate the compliance with USGCB and DHS baseline configuration settings. The systems tested include a mix of major applications and general support systems that were categorized as “SBU,” “Secret,” and

¹³ *Information Technology Management Letter for the FY 2012 Department of Homeland Security Financial Statement Audit* (OIG-13-58, April 2013).
www.oig.dhs.gov



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

“Top Secret.” We also performed vulnerability assessments on databases and websites to determine whether Components had implemented effective controls to protect DHS’ sensitive data. Our testing identified the following issues:

USGCB Compliance for Windows 7 and Windows XP Workstations

- Five systems from FEMA, ICE, NPPD, OIG, and USCIS still used Windows XP at the time of testing.¹⁴ Microsoft had stopped providing security updates or offering technical assistance for Windows XP in April 2014, which could lead to unidentified and unpatched vulnerabilities. Based on our review, we also determined the following:
 - USGCB compliance rate was 50 percent or below for Windows XP workstations at ICE and FEMA. Subsequent to the completion of our testing, ICE indicated that the system was decommissioned.
 - USCIS had 3,365 Windows XP workstations in production. USCIS expects to migrate its workstations from Windows XP to Windows 7 operating system by December 31, 2014.
 - OIG had 42 Windows XP workstations in production at the time of our testing. Subsequently, OIG completed its migration to Windows 7 in September 2014 and no longer operates any workstations with Windows XP installed.
- Some Components have not implemented all required USGCB settings or submitted the required waivers to acknowledge and accept the risks of noncompliance. For example, we identified deficiencies associated with both Windows 7 and Windows XP workstations tested. Figure 3 summarizes our USGCB testing results:

¹⁴ We determined that DHS HQ and TSA do not use Windows XP on the systems selected for review. In addition, NPPD had two Windows XP workstations for special use. NPPD submitted a waiver for these workstations, which was pending review.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Figure 3. USGCB Compliance for Windows 7 and Windows XP Operating Systems

Component	Windows 7	Windows XP	
	USGCB	Windows XP Workstations	USGCB Implementation
DHS HQ	94%	Not found	Not applicable
FEMA	95%	Yes	50%
FEMA	96%	Not found	Not applicable
ICE	Not tested	Yes	41%
NPPD	96%	Yes	Not tested
OIG	97%	Yes	Not tested
TSA	90%	Not found	Not applicable
USCIS	98%	Yes	Not tested

Source: OIG compiled based on data from testing results. During our review, we performed testing on two separate local area networks at FEMA.

DHS Baseline Configuration Compliance on Servers

- We evaluated approximately 200 configuration settings on 6 Windows servers. The results from our testing revealed that Components only implemented 76 percent of DHS baseline configuration settings on the six Windows servers.
- We evaluated approximately 85 configuration settings on 4 Redhat LINUX servers. The results from our testing revealed that Components only implemented 67 percent of the DHS baseline configurations settings on the Redhat LINUX servers. On two of the servers, only 57 and 53 percent of the DHS baseline configuration settings were configured, respectively.

Vulnerability Assessments

- Windows 7 workstations had missing security patches for Internet browsers (Internet Explorer, Firefox), media players (Flashplayer, Shockwave, QuickTime), and Microsoft Office products. Some of the missing critical patches dated back to October 2011. Further, a majority of vulnerabilities identified were from Adobe Acrobat and Reader, and Oracle Java. If exploited, these vulnerabilities may allow unauthorized access to DHS data.
- Windows XP workstations had missing security patches for Internet browsers (e.g., Internet Explorer, Firefox), Microsoft Office products, and services used by an operating system (print spooler, networking components). Some of the missing patches identified were for Adobe Acrobat and Oracle Java. Some of the missing critical patches identified dated back to November 2009.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

- The results from our database testing revealed that Components implemented weak passwords, did not apply security patches timely, and assigned excessive permissions, which attackers can exploit to gain unauthorized access to DHS data. DHS requires Components to install security patches timely and to restrict access based on the least privilege principle.¹⁵
- Our security assessment results revealed that one external website was configured to accept weak encryption, which could lead to brute-force or man-in-the-middle attacks.¹⁶ In addition, some of the websites were susceptible to cross-site and cross-frame vulnerabilities, which may allow attackers to impersonate a legitimate user or execute clickjacking attacks.¹⁷
- Our audits conducted throughout the year revealed that Components had not fully implemented all of the required USGCB settings. For example:
 - In March 2014, we reported that NPPD did not implement all USGCB settings on one of its systems.¹⁸
 - In September 2014, we reported that CBP had not implemented all the required DHS baseline configuration settings on selected Windows and Oracle-Linux servers.¹⁹

See appendix F for the Status of DHS' Configuration Management Program.

Incident Response and Reporting Program

During FY 2014, the Department transitioned the OneNet Stewardship responsibilities from CBP to DHS Office of the CIO to centralize administration of its incident response and reporting program. For example, DHS Office of the

¹⁵ The principle of least privilege requires that a user (or process) be given no more privileges than necessary to perform a job.

¹⁶ A brute-force attack is a method to gain access by systematically trying every possible password combination until the attacker discovers the correct password to log into a system or website. Man-in-the-middle is an attack in which the attacker positions himself between the information sender and receiver so that the attacker can intercept and alter data transmitting between the sender and receiver.

¹⁷ Cross-site and cross-frame scripting are vulnerabilities that allow attackers to inject malicious code into an otherwise benign website. A clickjacking attack deceives the victim into interacting with user interface elements on the target website without user knowledge, executing privileged functionality on the victim's behalf.

¹⁸ *Implementation Status of EINSTEIN 3 Accelerated* (OIG-14-52, March 2014).

¹⁹ *Enhancements in Technical Controls and Training Can Improve the Security of CBP's Trusted Traveler Programs* (OIG-14-139, September 2014).



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

CIO's Information Technology Services Office assumed program management and engineering functions for the OneNet Network Operations Center. In addition, the Information Security Office accepted all functions and responsibilities of the DHS Security Operations Center.

Progress

According to the July 2014 information security scorecard, the Department received an overall score of 94 percent for the Event Management metric, which tracks Components' response to "moderate" and "critical" security event notifications.

Issues To Be Addressed

DHS did not provide documentation to support that Components were submitting weekly incident reports to the DHS Security Operations Center, as required.

See appendix G for Status on DHS' Incident Response and Reporting Program.

Security Training Program

DHS continues to monitor Component-level security training programs through monthly training status updates and annual site visits. Specifically, the Information Security Office verifies that all DHS employees, contractors, and privileged users identified by Components receive the required annual IT security awareness and specialized security training accordingly.

Progress

During FY 2014, the Information Security Office has accomplished the following:

- Developed a SharePoint training site, which includes a privileged user training module. The SharePoint site allows Components to access and share training courses across the Department. The office also defined "privileged users" in the DHS Information Security Performance Plan.²⁰
- Updated its training policies and procedures to emphasize privacy and incident response training.

²⁰ Privileged users are personnel who have the roles of network/system administrator, database administrator, or account manager.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Issues To Be Addressed

- Components are not consistently reporting the numbers of employees who have received IT security awareness and specialized training on a monthly basis. As a result, the Information Security Office cannot determine if DHS' employees and contractors have received the required trainings.
- The Information Security Office had only conducted one on-site review to capture training data statistics at NPPD, including the number of general and privileged users, training courses, costs, and challenges in FY 2014.
- In June 2014, we reported that some USCIS users had not completed mandatory annual privacy awareness training.²¹ We also reported in September 2014 that some CBP administrators had not received the required specialized training.²²

See appendix H for Status on DHS' Security Training Program.

Remote Access Program

DHS established policies and procedures to mitigate the risks associated with remote access and dial-in capabilities. Specifically, Components are responsible for managing all remote access and dial-in connections to their systems by using two-factor authentication, enabling audit capabilities, and protecting sensitive information throughout transmission. Overall, Components using remote access developed policies outlining controls needed to protect remote connections and implemented mitigating security controls (i.e., multi-factor authentication, firewalls, virtual private network concentrators, etc.) to protect against external threats.

Issues To Be Addressed

Components have not consolidated their external network connections to a DHS TIC. As of March 2014, DHS identified 31 external connections that carry network traffic outside of a DHS TIC at CBP, FEMA, Federal Law Enforcement Training Center (FLETC), NPPD, TSA, USCG, and USCIS. However, we determined that DHS did not have the most accurate inventory of its external connections, as only 21 of the 31 external connections identified were operational as of May 2014.

²¹ *Radio Frequency Identification Security at USCIS Is Managed Effectively, But Can Be Strengthened* (OIG-14-99, June 2014).

²² *Enhancements in Technical Controls and Training Can Improve the Security of CBP's Trusted Traveler Programs* (OIG-14-139, September 2014).



OFFICE OF INSPECTOR GENERAL Department of Homeland Security

See appendix J for Status on DHS' Remote Access Program.

Account and Identity Management Program

DHS' account and identity management program is decentralized as Components are responsible for issuing PIV cards to their employees and contractors. Specifically, each Component uses account management software (e.g., Active Directory) to enforce access policies consistent with DHS procedures and guidance. To strengthen security, DHS continues its effort to implement PIV cards for logical access enterprise-wide that comply with *Homeland Security Presidential Directive*.²³

Progress

- Six Components (DHS HQ, FEMA, FLETC, NPPD, S&T, and USCG) exceeded the 75 percent compliance goal for mandatory PIV use on DHS' monthly information security scorecard.
- The Department has issued 1,024 (17 percent) two-factor authentication tokens on its classified Homeland Secure Data Network to reduce anonymity and improve security. DHS expects to complete this effort by June 2016.

Issues To Be Addressed

- OIG and USSS have not begun the implementation of using PIV cards for logical access.
- According to the July 2014 information scorecard, CBP, ICE, TSA, and USCIS remain below the Department's 75 percent compliance goal of PIV card usage. The Department's overall percentage was 66 percent.

See appendix K for Status on DHS' Account and Identity Management Program.

Continuous Monitoring Program

DHS has taken steps to strengthen its continuous monitoring program. For example, during FY 2014, the Information Security Office conducted oversight activities on its classified systems and increased the number of systems

²³ 'Mandatory PIV logical access' disallows the use of the traditional user name and password as opposed to 'optional PIV logical access,' which provides the user the choice of using either method.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

participating in the Ongoing Authorization program. Additionally, the Information Security Office updated and developed additional ISCM metrics for better evaluation of Component compliance with DHS and OMB continuous monitoring requirements.

Progress

- DHS conducted site visits to perform quality reviews of selected security authorization packages on FEMA’s “Top Secret” systems.
- DHS increased the number of systems that are participating in the Ongoing Authorization program. As of August 2014, 61 systems from 5 Components were enrolled in the Ongoing Authorization program.
- DHS revised its information security scorecard to evaluate Components’ alignment with OMB and DHS goals, which strengthen the Department’s enterprise-wide continuous monitoring program. In addition, the Information Security Office developed a new scan coverage metric to track the percentage of unclassified systems and assets that Components scanned and reported each month.

Issues To Be Addressed

- Our review of DHS’ July 2014 information security scorecard identified the following deficiencies:
 - FEMA and USSS have overall ISCM scores of 67 percent or below, well below the Department’s target of 85 percent.
 - CBP, FEMA, NPPD, and USSS have scores of 78 percent or below for the anti-virus metric. FEMA and USSS have scores of 10 percent or below.
- DHS does not perform continuous monitoring on the Department’s classified systems. Specifically, DHS only collects continuous monitoring data for the Department’s “SBU” systems.
- During FY 2014, the Information Security Office did not perform any critical control reviews and only visited S&T and USCG to evaluate Component technical capabilities, data collection and reporting procedures, scorecard performance, and organizational challenges.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

- Our review of 11 security authorization packages revealed the following deficiencies:
 - Components had not performed penetration testing on seven systems evaluated.
 - Three systems did not have the technical capability to block unauthorized hardware (e.g., USB drives) from connecting to the network.
 - Four Components did not perform continuous monitoring using a real-time data feed of all software installed on devices connected to its network.

See appendix L for Status on DHS' Continuous Monitoring Program.

Contingency Planning Program

DHS continues to maintain an entity-wide business continuity and contingency planning program. However, DHS can take additional steps to strengthen the Department's business continuity and disaster recovery programs.

Progress

DHS developed testing and exercise approaches for its business continuity and disaster recovery programs. Between April and June 2014, DHS also participated in Eagle Horizon, a national-level exercise to execute its continuity and reconstitution plans to test the Department's ability to restore mission essential functions.

Issues To Be Addressed

- The DHS Office of Operations Coordination and Planning finalized its *DHS Continuity Plan* in October 2012. However, as of July 2014, only 5 of 15 planned annexes have been completed and 3 annexes are still being drafted. Completing the annexes will allow DHS to define Component responsibilities on how to execute continuity during various threats or hazardous events.
- The Department has not finalized the *DHS Directive Number 008-03, Continuity Programs* to establish and further clarify its continuity programs policy, responsibilities, and requirements. DHS expects the Directive will be finalized once the Secretary's unity-of-effort efficiency review is complete.
- DHS has not conducted a business impact analysis since 2009. DHS is currently conducting a business process analysis of its



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

essential functions and expects to complete this analysis by the first quarter of 2015. Subsequent to the completion of the business process analysis, DHS plans to conduct a business impact analysis of its essential functions by the first quarter of 2016.

- Our review of 11 security authorization packages identified deficiencies related to system contingency planning documentation. Specifically, we determined the following:
 - One system contingency plan did not include vendor lists or personnel contacts. In addition, some Components had not updated the contingency plan templates to include system specific information.
 - Two contingency plans did not include procedures for restoring system operations regarding the handling of sensitive information at the alternate recovery site.

See appendix M for Status on DHS' Contingency Planning Program.

Security Capital Planning Program

DHS' Capital Planning and Investment Control (CPIC) process is based on OMB's Circular A-11, Part II, Section 55 – *Information Technology Investments*, which provides Federal agencies with guidance regarding the management and reporting requirements of information technology investment portfolios.²⁴ DHS' CPIC guidance provides Components with policies and procedures for planning, budgeting, managing, and maintaining the Department's investment portfolios, including IT, as critical assets for achieving agency strategic goals and missions.²⁵

Progress

DHS uses the Federal IT Dashboard to manage and update DHS' budget information, including for its IT portfolio.

Issues To Be Addressed

- DHS has not finalized or approved all of its CPIC guidance to incorporate the latest changes from OMB and the Department. Specifically, as of July 2014, DHS had not finalized the *DHS Instruction Manual 102-02-002-02 (Draft), Operational Analysis*. The instruction provides guidance on conducting operational analysis for steady state programs within DHS. Operational analysis

²⁴ OMB's Circular A-11, Part II, Section 55 – *Information Technology Investments*, July 2014.

²⁵ *OMB/DHS Major IT Business Case Guidance*, Version 9.0, June 2014.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

evaluates the effectiveness of an investment relating to customer results, strategic and business results, and financial performance.

- FEMA is not following OMB and DHS' policies and procedures for CPIC. For example, as part of the CPIC process, OMB requires an agency major investment to have unique investment identifier codes for major applications and general support systems. FEMA reported that it had 91 operational systems in its system inventory in the July 2014 information security scorecard. However, in response to the deficiencies cited in the 2013 CyberStat review, FEMA began an inventory refresh process to identify and catalog its information systems. During its inventory refresh process, FEMA identified 406 active systems that had budget-related unique investment identifiers and approximately 246 additional systems that did not have unique investment identification codes.

See appendix O for Status of DHS' Security Capital Planning Program.

Recommendations

We recommend that the CISO:

Recommendation #1:

Declare and report a material weakness, in accordance with FISMA requirements, on Components' information security programs that are consistently lagging behind in key performance metrics (e.g., system inventory, security authorization, continuous monitoring, and weakness remediation) of the information scorecard or when Components fail to provide the required continuous monitoring data feeds.

Recommendation #2:

Evaluate whether the Department's system inventory methodology is effective to prevent Components from circumventing the existing process to procure or develop new systems.

Recommendation #3:

Strengthen the process to ensure that components create, update, and maintain POA&M for all known IT security weaknesses for the Department's "SBU," "Secret," and "Top Secret" systems in accordance with applicable OMB and DHS policy.

Recommendation #4:

Expand the Department's continuous monitoring strategy to include "Secret" and "Top Secret" systems.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Recommendation #5:

Establish a process to ensure that Components implement the required USGCB and DHS configuration settings or follow applicable DHS policy to submit a waiver to acknowledge and accept the risk of non-compliance.

Recommendation #6:

Strengthen the process to ensure that all DHS systems receive the proper authority to operate in accordance with applicable OMB and NIST security authorization guidance.

Management Comments and OIG Analysis

Management Comments to Recommendation #1

DHS concurred with recommendation 1. The DHS CIO will declare and report a material weakness in a Component's information security programs if, once evaluated, the performance gap meets the criteria of a material weakness. DHS CIO will evaluate by January 9, 2015, the findings in this report, as well as updated information regarding ongoing remediation efforts in order to make that decision.

DHS CISO is pleased to report the following corrective actions taken by Components to address the OIG's findings. These ongoing efforts will strengthen the Components' information security programs and will be considered in the CIO's evaluation.

- **USSS:** The DHS CIO and USSS have negotiated an approach to overcome the previous concerns regarding reporting and data sharing. Prior to reaching this agreement with the DHS CIO, data sharing with the Department was kept to a minimum due to the sensitive nature of the USSS mission and the data that supports that mission. USSS has now incorporated its ISCM data in the DHS scorecard.
- **USCG:** USCG has identified process improvements and dedicated security authorization resources to substantially increase its ability to meet accreditation responsibilities. USCG will authorize 75 percent of its IT systems by June 2015 and 90 percent by the end of September 2015.
- **FEMA:** FEMA recently completed an inventory of its systems in response to an FY 2013 Cyberstat Review. The effort resulted in the addition of an unprecedented number of systems, subsequent ATO decisions, and implementation of appropriate remediation efforts for security gaps identified. The results of these efforts are only now being realized due to the challenge of transitioning field



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

work documentation into the Information Assurance Compliance System tool for completion of the Department's security authorization process. By the end of calendar year 2014, FEMA's inventory will be accurately reflected on the FISMA scorecard and the ATO for each system will be up-to-date.

- Continuous Monitoring for Secret and Top Secret systems: DHS CISO will finalize a plan for ISCM reporting for Secret and Top Secret IT systems within the Department by December 31, 2014. The Department will execute that plan and report out the results of its work in a Department Secret and Top Secret scorecard by the end of September 2015.
- IT Security Weakness Remediation: DHS leadership has committed to ensuring the appropriate resourcing for the Components POA&M remediation efforts. DHS will ensure that Components create, update, and maintain POA&M for all known IT security weaknesses for the Department's SBU, Secret, and Top Secret systems in accordance with applicable OMB and DHS policy.

OIG Analysis

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

Management Comments to Recommendation #2

DHS concurred with recommendation 2. DHS will leverage the Capital Planning and Investment Control process to ensure that new Department IT systems are added to its FISMA inventory. Additionally, the FY 2015 annual FISMA inventory refresh process will be further refined to incorporate additional testing that can be performed on a quarterly basis to discover systems that have not been added to the inventory. Estimated completion date: December 31, 2014.

OIG Analysis

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

Management Comments to Recommendation #3

DHS concurred with recommendation 3. In FY 2015, DHS CISO began business process re-engineering for the existing POA&M process. We are identifying required changes to the automated Information Assurance Compliance System tool, in which POA&M are developed and



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

maintained. The business process-re-engineering work will focus on process, procedures, and reporting to include POA&M associated with the Department's Secret and Top Secret systems. Additional funding is also expected to be available in FY 2016 to remediate known IT security weaknesses.

To further strengthen the POA&M process, DHS CISO plans to document and communicate monthly statuses to Component CIOs and CISOs highlighting non-compliance with applicable OMB and DHS policy and the requirement for more timely resolution. The re-engineered processes will be implemented in the second quarter of FY 2015. Estimated completion date: February 2015.

Also during FY 2015, DHS CISO plans to conduct POA&M refresher training for the DHS Components. Component representatives will be trained on the creation of POA&M documents and mitigation processes. Training will improve the skillsets necessary to create and maintain POA&M that appropriately guide the remediation of IT security weaknesses for FISMA systems. Estimated completion date: September 30, 2015.

OIG Analysis

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

Management Comments to Recommendation #4

DHS concurred with recommendation 4. DHS CISO will create a plan to identify a repeatable and automated mechanism to implement ISCM for Secret and Top Secret systems by December 31, 2014. DHS CISO will work with Components to deliver a Department Secret and Top Secret ISCM scorecard associated to that plan by September 30, 2015.

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. DHS will further increase the rigor of the requirements in its FY 2015 Information Security Performance Plan and FY 2015 Information Security Scorecard. Previous year plans and scorecards focused on the existence of configuration management capability across the Components. The focus for FY 2015



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

will be on assessing the effectiveness of configuration management with additional granularity and ensuring that Components document variances in waivers. These metrics will be published in the FY 2015 Information Security Plan and measured in the FY 2015 scorecard. Estimated completion date: March 31, 2015.

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 #6

DHS concurred with recommendation 6. DHS CISO will continue maturing the Ongoing Authorization methodology referenced previously. DHS CISO will also revise the monthly status reports shared with Department and Component CIOs and CISOs to better focus on the requirement for DHS operational systems to receive and maintain the authority to operate. Estimated completion date: December 31, 2014

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.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix A

Transmittal to Action Official

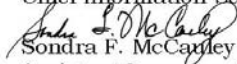


OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, D.C.

December 12, 2014

TO: Jeffrey Eisensmith
Chief Information Security Officer

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

SUBJECT: *Evaluation of DHS' Information Security Program for Fiscal Year 2014*. Report Number OIG-15-16

Attached for your information is our final report, *Evaluation of DHS' Information Security Program for Fiscal Year 2014*. We incorporated the formal comments from the Director, Departmental GAO OIG Liaison Office, in the final report.

The report contains six recommendations aimed at improving the Department's information security program. The Department concurred with all recommendations. Based on information provided in the Department's response to the draft report, we consider recommendations #1 through #6 resolved and will remain open until corrective actions are completed and supporting documentation is provided.

Please provide our office with a written response within 90 days that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Please email a signed pdf copy of responses and closeout requests to OIGITAuditsFollowup@oig.dhs.gov. Refer to the *Department of Homeland Security Directive 077-01, Follow-Up and Resolutions for Office of Inspector General Report Recommendations* for guidance on audit resolution.

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



Appendix B

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 has developed adequate and effective information security policies, procedures, and practices, in compliance with FISMA. 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 in FISMA and the FY 2014 FISMA reporting metrics dated December 2, 2013. We conducted our fieldwork at the Departmental level and at DHS' organizational Components and offices, including CBP, DHS HQ, FEMA, FLETC, ICE, NPPD, OIG, S&T, TSA, USCG, USCIS, and USSS. This report also includes the results from our audits conducted throughout the year and ongoing financial statement reviews.

As part of our evaluation of DHS' compliance with FISMA, we assessed DHS and its Components according to the security requirements mandated by FISMA and other Federal information security policies, procedures, standards, and guidelines. Specifically, we: (1) used last year's FISMA independent evaluation as a baseline for this year's evaluation; (2) reviewed policies, procedures, and practices that DHS has implemented at the program and Component levels; (3) reviewed DHS' POA&M process to ensure that all security weaknesses are identified, tracked, and addressed; (4) reviewed the processes and 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, contingency planning, and security capital planning; and (5) developed our independent evaluation of DHS' information security program.

We performed quality reviews of 11 security authorizations at CBP, DHS HQ, FEMA, FLETC, ICE, NPPD, USCG, USCIS, and USSS for compliance with applicable DHS, OMB, and NIST guidance. In addition, we evaluated the compliance with DHS' baseline configuration settings for 10 systems at CBP, DHS HQ, FEMA, FLETC, ICE, NPPD, USCG, USCIS, and USSS. We also evaluated the compliance with USGCB settings on eight systems at FEMA,



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

DHS HQ, ICE, NPPD, OIG, TSA, and USCIS. Additionally, we evaluated the effectiveness of controls implemented on three databases and five websites. Our evaluation did not include a comprehensive review of the Department's Ongoing Authorization program.

We conducted this review between April and August 2014 under the authority of the *Inspector General Act of 1978*, as amended, and according to the Quality Standards for Inspections issued by the Council of the Inspectors General on Integrity and Efficiency.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix C

Management Comments to the Draft Report


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



**Homeland
Security**

December 4, 2014

MEMORANDUM FOR: Richard Harsche
Acting Assistant Inspector General
Office of Information Technology Audits

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

SUBJECT: OIG Draft Report: "Evaluation of DHS' Information Security
Program for Fiscal Year 2014" (Project No. 14-043-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's) work in planning and conducting its review and issuing this report.

DIIS is pleased to note the OIG's recognition that the Department has expanded its Ongoing Authorization (OA) program. OA improves the security of information systems by taking advantage of on-demand continuous monitoring data. Authorizing officials are able to receive instantaneous and up-to-date security data for DHS systems. This aids in making risk-based decisions concerning the health of these systems and taking corrective action in a rapid fashion.

In addition, the report acknowledges that DIIS developed and implemented its "Fiscal Year 2014 Information Security Performance Plan," which formalized related performance requirements, priorities, and overall goals for the Department. Also, DHS has taken actions to address the President's cybersecurity priorities such as the implementation of trusted internet connections; and the use of multi-factor authentication to gain access to information systems.

The draft report contained six recommendations with which DHS concurs. Specifically, OIG recommended that the DHS Chief Information Security Officer (CISO):

Recommendation 1: Declare and report a material weakness, in accordance with FISMA [Federal Information Security Management Act] requirements, on components' information security programs that are consistently lagging behind in key performance metrics (e.g.,



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

system inventory, security authorization, continuous monitoring, and weakness remediation) of the information security scorecard or when components fail to provide the required continuous monitoring data feeds.

Response: Concur. The DHS Chief Information Officer (CIO) will declare and report a material weakness in a Component's information security programs if, once evaluated, the performance gap meets the criteria of a material weakness. DHS CIO will evaluate the findings in this report, as well as updated information regarding ongoing remediation efforts in order to make that decision.

It is important to note the following corrective actions already in progress by Components to address OIG's findings. These efforts will strengthen the Components' information security programs and will also be considered in the CIO's evaluation.

- United States Secret Service (USSS): The DHS CIO and USSS have negotiated an approach to overcome the previous concerns regarding reporting and data sharing. Prior to reaching this agreement with the DHS CIO, data sharing with the Department was kept to a minimum due to the sensitive nature of the USSS mission and the data that supports that mission. USSS has now incorporated its Information Security Continuous Monitoring (ISCM) data into the DHS scorecard.
- United States Coast Guard (USCG): USCG has identified process improvements and dedicated security authorization resources to substantially increase its ability to meet accreditation responsibilities. USCG will authorize 75 percent of their Information Technology (IT) systems by June 2015 and 90 percent by the end of September 2015.
- Federal Emergency Management Agency (FEMA): FEMA recently completed an inventory of its systems in response to an FY 2013 Cyberstat Review. The effort resulted in the addition of an unprecedented number of systems, subsequent Authority to Operate decisions, and implementation of appropriate remediation efforts for security gaps identified. The results of these efforts are only now being realized due to the challenge of transitioning field work documentation into the Information Assurance Compliance System (IACS) tool for completion of the Department's security authorization process. By the end of calendar year 2014, FEMA's inventory will be accurately reflected on the FISMA scorecard and the Authority to Operate for each system will be up-to-date.
- Continuous Monitoring for Secret and Top Secret Systems: DHS CISO will finalize a plan for ISCM reporting for Secret and Top Secret General Service (GENSER) IT systems within the Department by December 31, 2014. The Department will execute that plan and report out the results of its work in a



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Department Secret and Top Secret GENSER scorecard by the end of September 2015.

- IT Security Weakness Remediation: DHS leadership has committed to ensuring the appropriate resourcing for the Components' plans of action and milestones (POA&M) remediation efforts. DHS will ensure that components create, update, and maintain POA&Ms for all known IT security weaknesses for the Department's SBU, Secret, and Top Secret systems in accordance with applicable Office of Management and Budget and DHS policy.

Estimated Completion Date (ECD) for DHS CIO decision: January 31, 2015.

Recommendation 2: Evaluate whether the Department's system inventory methodology is effective to prevent components from circumventing the existing process to procure or develop new systems.

Response: Concur. DHS CISO will leverage the Capital Planning and Investment Control process to ensure that new Department IT systems are added to its FISMA inventory. Additionally, the FY 2015 annual FISMA inventory refresh process will be further refined to incorporate additional testing that can be performed on a quarterly basis to discover systems that have not been added to the inventory. ECD: December 31, 2014.

Recommendation 3: Strengthen the process to ensure that components create, update, and maintain POA&Ms for all known IT security weaknesses for the Department's "SBU," "Secret," and "Top Secret" systems in accordance with applicable OMB and DHS policy.

Response: Concur. In FY 2015, DHS CISO began business process re-engineering (BPR) for the existing POA&M process. We are identifying required changes to the automated Information Assurance Compliance System tool, in which POA&Ms are developed and maintained. The BPR work will focus on process, procedures and reporting to include POA&Ms associated with the Department's Secret and Top Secret systems. Additional funding is also expected to be available in FY 2016 to remediate known IT security weaknesses.

To further strengthen the POA&M process, DHS CISO plans to document and communicate monthly statuses to Component CIOs and CISOs highlighting non-compliance with applicable OMB and DHS policy and the requirement for more timely resolution. The re-engineered processes will be implemented during the second quarter of FY 2015.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Also during FY 2015, DHS CISO plans to conduct POA&M refresher training for the DHS Components. Component representatives will be trained on the creation of POA&M documents and mitigation processes. Training will improve the skillsets necessary to create and maintain POA&Ms that appropriately guide the remediation of IT security weaknesses for FISMA systems. ECD: September 30, 2015.

Recommendation 4: Expand the Department's continuous monitoring strategy to include "Secret" and "Top Secret" systems.

Response: Concur. DHS CISO will create a plan to identify a repeatable and automated mechanism to implement ISCM for Secret and Top Secret GENSER systems by December 31, 2014. In addition, DHS CISO will work with Components to deliver a Department Secret and Top Secret GENSER ISCM scorecard associated with the plan. ECD: September 30, 2015.

Recommendation 5: Establish a process to ensure that Components implement the required United States General Configuration Baseline (USGCB) and DHS configuration settings or follow applicable DHS policy to submit a waiver to acknowledge and accept the risk of non-compliance.

Response: Concur. DHS CISO will further increase the rigor of the requirements in its FY 2015 Information Security Performance Plan and FY 2015 Information Security Scorecard. Previous year plans and scorecards focused on the existence of configuration management capability across the Components. The focus for FY 2015 will be on assessing the effectiveness of configuration management with additional granularity and ensuring that Components document variances in waivers. These metrics will be published in the FY 2015 Information Security Plan and measured in the FY 2015 scorecard. ECD: March 31, 2015.

Recommendation 6: Strengthen the process to ensure that all DHS systems receive the proper authority to operate in accordance with applicable OMB and NIST [National Institute of Standards and Technology] security authorization guidance.

Response: Concur. DHS CISO will continue maturing the OA methodology referenced previously. DIIS CISO will also revise the monthly status reports shared with Department and Component CIOs and CISOs to better focus on the requirement for DHS operational systems to receive and maintain the authority to operate. ECD: December 31, 2014.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Again, thank you for the opportunity to review and comment on this draft report. Technical and sensitivity comments have been sent under separate cover. We look forward to working with you in the future.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix D

System Inventory as of September 2014

Question 1: System Inventory													
1. 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.													
Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing													
2. For the Total Number of Systems identified by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.													
		Question 1						Question 2					
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems (Agency and Contractor systems) (Column A + Column B)		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and reviewed in the past year		c. Number of systems for which contingency plans have been tested in accordance with policy	
Bureau Name	FIPS Pub 199 System Impact Level	Number	Number Reviewed	Number	Number Reviewed	Total Number	Total Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
CBP	High	17	4	0	0	17	4	17	100%	17	100%	17	100%
	Moderate	67	2	2	0	69	2	66	96%	68	99%	69	100%



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

	Low	2	0	0	0	2	0	2	100%	2	100%	2	100%
	Undefined	2	0	0	0	2	0	0	0%	0	0%	0	0%
	Sub-total	88	6	2	0	90	6	85	94%	87	97%	88	98%
DHS HQ	High	15	2	3	0	18	2	15	83%	16	89%	17	94%
	Moderate	25	1	8	0	33	1	32	97%	32	97%	33	100%
	Low	0	0	3	0	3	0	3	100%	3	100%	3	100%
	Undefined	3	2	0	0	3	2	0	0%	0	0%	2	67%
	Sub-total	43	5	14	0	57	5	50	88%	51	89%	55	96%
FEMA	High	20	3	2	0	22	3	10	45%	11	50%	20	91%
	Moderate	41	3	11	0	52	3	23	44%	24	46%	45	87%
	Low	6	0	0	0	6	0	1	17%	1	17%	6	100%
	Undefined	60	2	0	0	60	2	0	0%	0	0%	0	0%
	Sub-Total	127	8	13	0	140	8	34	24%	36	26%	71	51%
FLETC	High	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Moderate	9	3	2	0	11	3	8	73%	8	73%	10	91%
	Low	0	0	1	0	1	0	1	100%	1	100%	1	100%
	Undefined	0	0	0	0	0	0	0	0%	0	0%	0	0%
		9	3	3	0	12	3	9	75%	9	75%	11	92%
ICE	High	13	3	0	0	13	3	9	69%	12	92%	10	77%
	Moderate	33	3	8	1	41	4	36	88%	39	95%	41	100%
	Low	1	0	0	0	1	0	1	100%	1	100%	1	100%
	Undefined	1	0	0	0	1	0	1	100%	1	100%	0	0%
		48	6	8	1	56	7	47	84%	53	95%	52	93%
NPPD	High	6	0	5	0	11	0	10	91%	10	91%	11	100%
	Moderate	12	2	7	0	19	2	15	79%	18	95%	19	100%
	Low	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Undefined	2	0	0	0	2	0	0	0%	0	0%	1	50%
	Sub-total	20	2	12	0	32	2	25	78%	28	88%	31	100%
OIG	High	2	1	0	0	2	1	2	100%	2	100%	2	100%
	Moderate	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Low	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Undefined	1	0	0	0	1	0	1	100%	1	100%	0	0%
	Sub-total	3	1	0	0	3	1	3	100%	3	100%	2	67%



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

S&T	High	1	0	0	0	1	0	1	100%	1	100%	1	100%
	Moderate	12	0	10	1	22	1	18	82%	19	86%	22	100%
	Low	1	0	0	0	1	0	1	100%	1	100%	1	100%
	Undefined	2	0	0	0	2	0	2	100%	2	100%	0	0%
	Sub-total	16	0	10	1	26	1	22	85%	23	88%	24	92%
TSA	High	21	3	0	0	21	3	21	100%	21	100%	21	100%
	Moderate	34	1	11	0	45	1	45	100%	45	100%	45	100%
	Low	6	0	2	0	8	0	8	100%	8	100%	8	100%
	Undefined	5	0	0	0	5	0	5	100%	5	100%	5	100%
	Sub-total	66	4	13	0	79	4	79	100%	79	100%	79	100%
USCG	High	9	0	5	1	14	1	12	86%	12	86%	14	100%
	Moderate	69	2	16	2	85	4	46	54%	47	55%	76	89%
	Low	6	0	0	0	6	0	3	50%	3	50%	5	83%
	Undefined	38	0	1	0	39	0	13	33%	13	33%	4	10%
	Sub-total	122	2	22	3	144	5	74	51%	75	52%	99	69%
USCIS	High	6	1	0	0	6	1	6	100%	6	100%	6	100%
	Moderate	37	4	0	0	37	4	37	100%	37	100%	37	100%
	Low	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Undefined	0	0	1	0	1	0	1	100%	1	100%	1	100%
	Sub-total	43	5	1	0	44	5	44	100%	44	100%	44	100%
USSS	High	6	1	0	0	6	1	3	50%	3	50%	5	83%
	Moderate	11	0	0	0	11	0	10	91%	10	91%	10	91%
	Low	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Undefined	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	17	1	0	0	17	1	13	76%	13	76%	15	88%
Agency	High	116	18	15	1	131	19	106	81%	111	85%	124	95%
	Moderate	350	21	75	4	425	25	336	79%	347	82%	407	96%
	Low	22	0	6	0	28	0	20	71%	20	71%	27	96%
	Undefined	114	4	2	0	116	4	23	20%	23	20%	13	11%
	Total	602	43	98	5	700	48	485	69%	501	72%	571	82%



Appendix E

Status of Risk Management Program

Section 2: Status of Risk Management Program	
	Response:
<p>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?</p> <ol style="list-style-type: none"> 1. Documented policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process. 2. 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. 3. 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. 4. 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. 5. Has an up-to-date system inventory. 6. Categorizes information systems in accordance with government policies. 7. Selects an appropriately tailored set of baseline security controls. 8. Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation. 9. 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. 10. 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. 11. Ensures information security controls are monitored on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials. 12. Information-system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization. 13. Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO). 14. 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 	<p>Yes</p>



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

- the ongoing management of information-system-related security risks.
15. Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies (NIST SP 800-18, 800-37 Rev. 1).
16. Security authorization package contains accreditation boundaries, defined in accordance with government policies, for organization information systems.

Comments:

- As of July 2014, DHS' system inventory included a mix of 652 major applications and general support systems that were reported as "operational" and classified as "SBU," "Secret," and "Top Secret."
- FEMA's system inventory fluctuated significantly between October 2013 and July 2014. Additionally, FEMA did not update the Department's enterprise management tools to maintain an accurate inventory of its classified information systems.
- A total of 196 DHS' "SBU", "Secret", and "Top Secret" systems were operating without valid ATOs.
- Our review of 11 security authorization packages identified deficiencies with the associated security artifacts.



Appendix F

Status of Configuration Management Program

Section 3: Status of Configuration Management Program	
	Response:
<p>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?</p> <ol style="list-style-type: none"> 1. Documented policies and procedures for configuration management. 2. Defined standard baseline configurations. 3. Assessments of compliance with baseline configurations. 4. Process for timely (as specified in organization policy or standards) remediation of scan result deviations. 5. For Windows-based components, USGCB secure configuration settings are fully implemented, and any deviations from USGCB baseline settings are fully documented. 6. Documented proposed or actual changes to hardware and software configurations. 7. Process for timely and secure installation of software patches. 8. Software assessing (scanning) capabilities are fully implemented (NIST SP 800-53: RA-5, SI-2). 9. 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). 10. Patch management process is fully developed, as specified in organization policy or standards (NIST SP 800-53; CM-3, SI-2). 	<p>Yes</p>
<p>Comments:</p>	<ul style="list-style-type: none"> • The results from our testing revealed that some Components had not implemented all of (1) the required USGCB settings or submitted the required waivers to acknowledge and accept the risks of non-compliance, and (2) DHS baseline configuration settings on selected Windows and Redhat LINUX servers tested. • Five systems were still using Windows XP at the time of testing. • During our audits conducted throughout the year, we determined that CBP and NPPD had not implemented all of the required USGCB and DHS baseline configuration settings.



Appendix G

Status of Incident Response and Reporting Program

Section 4: Status of Incident Response & Reporting Program	
	Response:
<p>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?</p> <ol style="list-style-type: none"> 1. Documented policies and procedures for detecting, responding to, and reporting incidents (NIST SP 800-53: IR-1). 2. Comprehensive analysis, validation, and documentation of incidents. 3. When applicable, reports to US-CERT within established timeframes (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19). 4. When applicable, reports to law enforcement within established timeframes (SP 800-61). 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). 6. Is capable of tracking and managing risks in a virtual/cloud environment, if applicable. 7. Is capable of correlating incidents. 8. 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). 	<p>Yes</p>
<p>Comments:</p>	<ul style="list-style-type: none"> • DHS did not provide documentation to support that Components were submitting the required weekly incident reports to the DHS Security Operations Center.



Appendix H

Status of Security Training Program

Section 5: Status of Security Training Program	
	Response:
<p>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?</p> <ol style="list-style-type: none"> 1. Documented policies and procedures for security awareness training (NIST SP 800-53: AT-1). 2. Documented policies and procedures for specialized training for users with significant information security responsibilities. 3. Security training content based on the organization and roles, as specified in organization policy or standards. 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. 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. 6. Training material for security awareness training contains appropriate content for the organization (NIST SP 800-50, 800-53). 	<p>Yes</p>
Comments:	<ul style="list-style-type: none"> • Components are not always reporting monthly the numbers of employees who have received IT security awareness and specialized training. • In June 2014, we reported that some USCIS users had not completed mandatory annual privacy awareness training. We also reported in September 2014 that some CBP administrators had not received the required specialized training.



Appendix I

Status of Plan of Action and Milestones Program

Section 6: Status of Plans of Actions & Milestones Program	
	Response:
<p>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?</p> <ol style="list-style-type: none">1. Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation.2. Tracks, prioritizes, and remediates weaknesses.3. Ensures remediation plans are effective for correcting weaknesses.4. Establishes and adheres to milestone remediation dates.5. Ensures resources and ownership are provided for correcting weaknesses.6. POA&M 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).7. Costs associated with remediating weaknesses are identified (NIST SP 800-53, Control PM-3; OMB M-04-25).8. Program officials report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53, Control CA-5; OMB M-04-25).	<p>Yes</p>



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Comments:	<ul style="list-style-type: none">• DHS and its Components have not created POA&M for operational systems that do not have valid ATOs.• DHS and its Components did not create POA&M for the IT security weaknesses identified in OIG audit reports.• FEMA could not provide documentation to support that it maintains POA&M for three of its “Top Secret” systems.• Components did not maintain current information on the progress of security weakness remediation, and not all POA&M were resolved in a timely manner. For example, while DHS requires Components to complete POA&M within 6 months, we determined that 1,497 of the 3,206 (47 percent) open “SBU” POA&M were delayed. Further, 517 of the 3,206 (16 percent) open POA&M were past due by 12 months (prior to July 15, 2013). In addition, 199 of the 3,206 (6 percent) open POA&M have been designated as significant deficiencies. We also determined that 39 of the 199 (20 percent) significant deficiencies identified were delayed. Finally, 230 of the 3,206 (7 percent) open POA&M have not been properly assigned a “Severity Level,” as required by DHS guidance.• DHS did not consistently provide the OIG with timely updates or corrective actions regarding previous audit reports.
------------------	---



Appendix J

Status of Remote Access Program

Section 7: Status of Remote Access Program	
	Response:
<p>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?</p> <ol style="list-style-type: none"> 1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST SP 800-53: AC-1, AC-17). 2. Protects against unauthorized connections or subversion of authorized connections. 3. Users are uniquely identified and authenticated for all access (NIST SP 800-46, Section 4.2, Section 5.1). 4. Telecommuting policy is fully developed (NIST SP 800-46, Section 5.1). 5. If applicable, multi-factor authentication is required for remote access (NIST SP 800-46, Section 2.2, Section 3.3). 6. Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms. 7. Defines and implements encryption requirements for information transmitted across public networks. 8. Remote access sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required. 9. Lost or stolen devices are disabled and appropriately reported (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines). 10. Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4). 11. Remote-access user agreements are adequate in accordance with government policies (NIST SP 800-46, Section 5.1; NIST SP 800-53, PS-6). 	<p>Yes</p>
<p>Comments:</p>	<ul style="list-style-type: none"> • DHS did not have an accurate inventory of its external connections that carry network traffic outside of a DHS TIC. • Components had not consolidated all their external network connections to a DHS TIC.



Appendix K

Status of Account and Identity Management Program

Section 8: Status of Account and Identity Management Program	
	Response:
<p>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?</p> <ol style="list-style-type: none"> 1. Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1). 2. Identifies all users, including Federal employees, contractors, and others who access organization systems (NIST SP 800-53, AC-2). 3. Identifies when special access requirements (e.g., multi-factor authentication) are necessary. 4. If multi-factor authentication is in use, it is linked to the organization's PIV program where appropriate (NIST SP 800-53, IA-2). 5. 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). 6. 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). 7. Ensures that the users are granted access based on needs and separation-of-duties principles. 8. Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users. (For example: IP phones, faxes, and printers are examples of devices attached to the network that are distinguishable from desktops, laptops, or servers that have user accounts.) 9. Identifies all user and non-user accounts. (Refers to user accounts that are on a system. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes. They are not associated with a single user or a specific group of users.) 10. Ensures that accounts are terminated or deactivated once access is no longer required. 11. Identifies and controls use of shared accounts. 	<p>Yes</p>
<p>Comments:</p>	<ul style="list-style-type: none"> • OIG and USSS had not begun the implementation of using PIV card for logical access. • As of July 2014, CBP, ICE, TSA, and USCIS remained below the Department's 75 percent compliance goal of PIV card usage. The Department's overall compliance rating was 66 percent.



Appendix L

Status of Continuous Monitoring Program

Section 9: Status of Continuous Monitoring Program	
	Response:
<p>Has the organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems 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?</p> <ol style="list-style-type: none"> 1. Documented policies and procedures for continuous monitoring (NIST SP 800-53: CA-7). 2. Documented strategy for information security continuous monitoring. 3. Implemented ISCM for information technology assets. 4. Conduct and report on ISCM results in accordance with their ISCM strategy. 5. Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST SP 800-53, 800-53A). 6. Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans (NIST SP 800-53, 800-53A). 	<p>Yes</p>
<p>Comments:</p>	<ul style="list-style-type: none"> USSS refused to provide the continuous monitoring data feeds to DHS CISO, which is a significant deficiency to the Department's information security program. As a result of USSS' refusal, the DHS CISO is severely restricted performing continuous monitoring on the Department's information systems, managing DHS' information security program, or ensuring compliance with the President's cyber priorities. FEMA and USSS have overall ISCM scores of 67 percent or below, well below the Department's target of 85 percent. DHS did not perform continuous monitoring on the Department's classified systems. Specifically, DHS only collects continuous monitoring data for the Department's "SBU" systems.



Appendix M

Status of Contingency Planning Program

Section 10: Status of Contingency Planning Program	
	Response:
<p>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?</p> <ol style="list-style-type: none"> 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). 2. The organization has incorporated the results of its system’s Business Impact Analysis (BIA) into the analysis and strategy development efforts for the organization’s Continuity of Operations Plan (COOP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) (NIST SP 800-34). 3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures (NIST SP 800-34). 4. Testing of system-specific contingency plans. 5. The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34). 6. Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53). 7. Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans. 8. After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34). 9. Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53). 10. Alternate processing sites are not subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53). 11. Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53). 12. Contingency planning that considers supply chain threats. 	<p>Yes</p>
<p>Comments:</p>	<ul style="list-style-type: none"> • DHS has not conducted a business impact analysis since 2009. DHS is currently conducting a business process analysis of its essential functions and expects to be completed by the first quarter of 2015. Subsequent to the completion of the business process analysis, DHS plans to conduct a business impact analysis of its essential functions by the first quarter of 2016. • Our review of 11 security authorization packages identified deficiencies related to system contingency planning documentation.



Appendix N

Status of Agency Program to Oversee Contractor Systems

Section 11: Status of Agency Program to Oversee Contractor Systems	
	Response:
<p>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?</p> <ol style="list-style-type: none">1. Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in a public cloud.2. The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and organization guidelines (NIST SP 800-53: CA-2).3. A complete inventory of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in a public cloud.4. The inventory identifies interfaces between these systems and organization-operated systems (NIST SP 800-53: PM-5).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.6. The inventory of contractor systems is updated at least annually.7. Systems that are owned or operated by contractors or entities, including organization systems and services residing in a public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.	<p>Yes</p>



Appendix O

Status of Security Capital Planning Program

Section 12: Status of Security Capital Planning Program	
	Response:
<p>Has the organization established a security capital planning and investment program for information security? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?</p> <ol style="list-style-type: none"> 1. Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process. 2. Includes information security requirements as part of the capital planning and investment process. 3. Establishes a discrete line item for information security in organizational programming and documentation (NIST SP 800-53: SA-2). 4. Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST SP 800-53: PM-3). 5. Ensures that information security resources are available for expenditure as planned. 	<p>Yes</p>
<p>Comments:</p>	<ul style="list-style-type: none"> • DHS has not finalized or approved all of its CPIC guidance to incorporate the latest changes from OMB and the Department. • FEMA did not follow DHS and OMB' policies and procedures for CPIC. Specifically, FEMA began an inventory refresh process to identify and catalog its information systems in response to the deficiencies cited in the 2013 CyberStat review. During its inventory refresh process, FEMA identified approximately 246 systems that did not have a universal investment identification number.



Appendix P

FY 2014 Information Security Scorecard Metric Descriptions

Metric	Description
ISCM Metrics	
In-Scope Assets	# of the organization's hardware assets connected to the organization's unclassified network
Managed Assets	# of the organization's scanned assets providing a non-null hostname and a valid FISMA ID
Hardware Asset Management	% of managed assets that are properly scanned and identified
Scan Coverage (I)	% of unclassified systems and "in-scope" assets that are scanned and reported to DHS CISO each month
Software Asset Management	% of Windows platforms providing application common platform enumeration data via a credentialed scan
Whitelisting (I)	% of Windows platforms providing approved application common platform enumerations
Configuration Management	% of workstations and applicable servers providing one or more common configuration enumerations via a credentialed scan
Vulnerability Management	% of identified assets that meet or exceed the common vulnerabilities and exposures threshold of 100 % of identified assets that have a vulnerability scan
Information Security Vulnerability Management (ISVM)	% of applicable assets that have mitigated all common vulnerabilities and exposures associated with selected ISVMs
Anti-Virus	% of applicable assets that have updated their anti-virus within 30 days of the "scan date" provided in data feeds
Security Process Metrics (SPM)	
FISMA Systems	# of systems deemed operational according to DHS FISMA Inventory Methodology
Mission Essential Systems	# of systems deemed essential during an emergency; must be operational; cannot be an external system or have a low FIPS availability
Authorization	% of systems with a valid Authorization package in the Information Assurance Compliance System or through ongoing authorization
Ongoing Authorization(I)	% of systems currently in ongoing authorization. If 0%, has the CISO approved your Component for ongoing authorization (Y/N)?
Privacy (I)	% of systems with validated privacy documents
Weakness Remediation	% of POA&M passing timeliness, management, and quality checks
Training	% of users compliant with security training requirements
Event Management	Average time it takes (over established thresholds) to close or escalate Critical and Moderate security event notifications
TIC Consolidation	% of all external network traffic that is secured by a TIC access point
Mandatory Access (PIV)	% of unprivileged, privileged, and remote users required to use PIV for network access.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix Q

Inspector General Memorandum Regarding USSS' Refusal to Provide Continuous Monitoring Data Feeds




OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

OCT 29 2014

MEMORANDUM FOR: The Honorable Joseph Clancy
Acting Director
United States Secret Service

FROM: John Roth 
Inspector General

SUBJECT: Secret Service Refusal to Provide Continuous
Monitoring Data Feeds

I am writing you because there is a matter we discovered in the course of one of our audits that requires your personal attention. We have just completed an audit, required by the *Inspector General Act* and the *Federal Information Security Management Act (FISMA)*, in which the Secret Service has been found to be deficient and is refusing to comply with mandated computer security policies.

Since 2011, Federal agencies have been required to submit monthly continuous monitoring data feeds to the Office of Management and Budget (OMB). Consistent with those requirements, the DHS Chief Information Security Officer collects the following continuous monitoring data elements from DHS components on a monthly basis to ensure that DHS information systems are FISMA compliant:

- Hardware management
- Software management
- Vulnerability management
- Configuration management

On September 12, 2014, the Secret Service Chief Information Officer (CIO) informed the Department's CIO that, due to concerns for operational security, it would not provide the required continuous monitoring data feeds of its unclassified systems to the Department. This has resulted in the Secret Service receiving a score of "zero" in the Department's Information Security Scorecard. More importantly, your agency's action puts at risk its own information systems and those of the Department as a whole.

I recognize the vital investigative and protective missions performed by the Secret Service. However, I am deeply concerned that your agency's



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

unwillingness to provide the required continuous monitoring data feeds prevents the Department from overseeing and managing an effective information security program. Moreover, you, as Acting Director of the Secret Service, have no independent assurances that Secret Service information systems are being managed correctly and are compliant with Federal security requirements.

Further, I am not convinced that the Secret Service CIO's objection is well founded. Your CIO has given us no reason to believe that the established procedures for handling the continuous feeds, established by the Department's Chief Information Security Officer, presents a credible security concern. All Department components handle sensitive information, and each of them, except for the Secret Service, complies with this requirement.

For these reasons, I am asking you to review your CIO's refusal to provide the continuous monitoring data feeds to the Department, as required by OMB. I am attaching the Department's September 2014 Information Security Scorecard and our draft FY14 FISMA report for your information.

Our draft FISMA report will be made final in 30 days and transmitted to the Secretary, the relevant House and Senate committees with oversight over the Department, and published on our website. Unless appropriate action is taken, the draft report will reflect the Secret Service's "significant deficiency" with regard to computer security compliance.

I appreciate your attention to this matter. Please feel free to contact me with any questions.

Attachments



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix R

USSS Acting Director's Response to Inspector General's Memorandum



U.S. Department of Homeland Security
UNITED STATES SECRET SERVICE

Washington, D.C. 20223

November 7, 2014

MEMORANDUM FOR: John Roth
Inspector General
U.S. Department of Homeland Security

FROM: Joseph P. Clancy *JPC*
Acting Director
United States Secret Service

SUBJECT: OIG Draft Report: "Evaluation of DHS' Information Security Program for Fiscal Year 2014" (Project No. 14-043-ITA- MGMT)

Thank you for your correspondence dated October 29, 2014, concerning our position regarding Continuous Diagnostics and Mitigation (CDM) and we appreciate being afforded an opportunity to respond. Of significance in this matter, on November 3, 2014, the U.S. Secret Service Chief Information Officer (CIO) and the CIO at DHS agreed in principal that the Secret Service would provide needed CDM data and the methodology for doing so that will satisfy reporting requirements. Since then, Secret Service subject matter experts from our Information Resources Management Resource Division (Security Engineering) and the Chief Information Security Officer's Division have met with counterparts at DHS to determine the specific requirements for reporting, the result of which is a formally signed memorandum of understanding (MOU) between DHS and the Secret Service CIO's, dated November 7, 2014.

I would also like to take this opportunity to add information that I hope will clarify some of the points raised in your letter. The Secret Service, in keeping with security policies and due diligence practices, agrees with and supports continuous monitoring and in fact we currently perform the same functions on behalf of our mission partners. We did however have a concern with DHS's method for providing the results which we believe we have now resolved. We will fulfill the reporting requirements through the manner reached in the above cited MOU and we fully expect that the Federal Information Security Management Act (FISMA) reporting will now reflect the actual practices we have implemented rather than a score indicative of the reporting method used.

In summary, the Secret Service had previously complied with FISMA and CDM reporting requirements through a manual, on-site process that had been in place for some time. However, it is my expectation that with the agreement reached between the DHS and the Secret Service CIO's that we will be able to move forward, briskly, in compliance with the intent and spirit of CDM reporting requirements.



Appendix S

Major Contributors to This Report

Chiu-Tong Tsang, Director
Tarsha Cary, IT Audit Manager
Aaron Zappone, Team Lead
Thomas Rohrback, IT Specialist
Michael Kim, IT Auditor
Josh Wilshere, Referencer



Appendix T

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
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
DHS Component Liaison

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