Department of Homeland Security
Office of Inspector General

Evaluation of DHS' Information Security Program for Fiscal Year 2010

OIG-11-01

October 2010

Office of Inspector General

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

Homeland Security

OCT 04 2010

Preface

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

This report addresses the strengths and weaknesses of controls over the information security program and practices at DHS. It is based on interviews with selected program officials at the department and components, direct observations, a review of applicable documents, and system testing.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Frank W. Deffer
Assistant Inspector General, IT Audits

Table of Contents/Abbreviations

Appendices

Abbreviations

ATO	Authority to Operate
C&A	Certification and Accreditation
CBP	Customs and Border Protection
CIO	Chief Information Officer
CIS	Citizenship and Immigration Services
CISO	Chief Information Security Officer
CPIC	Capital Planning and Investment Control
DHS	Department of Homeland Security
FDCC	Federal Desktop Core Configuration
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act

Table of Contents/Abbreviations

FLETC	Federal Law Enforcement Training Center
FY	Fiscal Year
HSPD-12	Homeland Security Presidential Directive 12
ICE	Immigration and Customs Enforcement
I&A	Office of Intelligence and Analysis
ISSO	Information Systems Security Officer
ISO	Information Security Office
IT	Information Technology
MGMT	Management Directorate
NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPS	Office of Operations Coordination and Planning
PIA	Privacy Impact Assessment
PIV	Personal Identification Verification
POA&M	Plans of Action and Milestones
PTA	Privacy Threshold Analysis
RAIDS	Radar Air Intrusion Detection System
S&T	Science and Technology
SDLC	System Development Life Cycle
SOC	Security Operations Center
SP	Special Publication
TSA	Transportation Security Administration
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
USSS	United States Secret Service

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

We conducted an independent evaluation of the Department of Homeland Security (DHS) information security program and practices to comply with the requirements of the *Federal Information Security Management Act* (FISMA). In evaluating DHS' progress in implementing its agency-wide information security program, we specifically assessed the department's Plans of Action and Milestones (POA&M), certification and accreditation (C&A) processes, and privacy program. Fieldwork was performed at both the program and component levels.

DHS continues to improve and strengthen its security program. During the past year, DHS developed and implemented the fiscal year (FY) 2010 information security performance plan to focus on areas that the department would like to improve upon throughout the year. Specifically, DHS identified in the performance plan several key elements that are indicative of a strong security program, such as POA&M weakness remediation, quality of C&A, annual testing and validation, and security program oversight. While these efforts have resulted in some improvements, components are still not executing all of the department's policies, procedures, and practices. For example, components have not maintained their information security programs at the department's targeted performance level.

In addition, our review identified the following more significant exceptions to a strong and effective information security program: (1) systems are being accredited though key information is missing or outdated; (2) POA&Ms are not being created for all known information security weaknesses or mitigated in a timely manner; and (3) baseline security configurations are not being implemented for all systems. Additional information security program areas that need improvement include configuration management, incident detection and analysis, specialized training, remote access, account and identity management, continuous monitoring, and contingency planning.

We are making seven recommendations to the Chief Information Security Officer (CISO). The CISO concurred with all of our recommendations and has already begun to take actions to implement them. The department's response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

Due to the increasing threat to information systems and the highly networked nature of the federal computing environment, the Congress, in conjunction with the Office of Management and Budget (OMB), requires an annual review and reporting of agencies' compliance with FISMA requirements. FISMA focuses on the program management, implementation, and evaluation of the security of unclassified and national security systems.

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, entitled FISMA, provides a comprehensive framework to ensure the effectiveness of security controls over information resources that support federal operations and assets.

FISMA requires each federal agency to develop, document, and implement an agency-wide security program. The agency's 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 charged with conducting an annual evaluation of information programs and systems under their purview, as well as an assessment of related security policies and procedures. Offices of Inspector General (OIG) must independently evaluate the effectiveness of an agency's information security program and practices on an annual basis.

OMB issued memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, on April 21, 2010. The memorandum provides updated instructions for agency and OIG reporting under FISMA. In

accordance with OMB's reporting instructions, this annual evaluation summarizes the results of our review of DHS' information security program and practices.

The CISO leads the Information Security Office (ISO) and is responsible for managing DHS' information security program. To aid in managing its security program, DHS developed a process for reporting and capturing known security weaknesses in its POA&Ms. DHS uses an enterprise management tool to collect and track data related to all POA&M activities, including weaknesses identified during self-assessments and the C&A process. DHS' enterprise management tool also collects data on other FISMA metrics, such as the number of systems that have implemented DHS' security baseline configurations and the number of employees who have received information technology (IT) security training.

In addition, DHS uses an enterprise-wide C&A tool to automate and standardize portions of the C&A process. The tool allows DHS components to quickly and efficiently develop their security accreditation packages.

Results of Independent Evaluation

Based on the requirements outlined in FISMA and OMB's annual reporting instructions, our independent evaluation focused on 11 key areas of DHS' information security program (i.e., system inventory; C&A process; POA&M; configuration management; incident response and reporting; security training; remote access; account and identity management; continuous monitoring; contingency planning; and privacy) across 14 components.[1]

This report includes the results of a limited number of systems evaluated during the year and our on-going financial statement review. In addition, it includes the results of our Active Directory, United States Computer Emergency Readiness Team (US-CERT), Cybersecurity,

[1] Customs and Border Protection (CBP), Citizenship and Immigration Services (CIS), Federal Emergency Management Agency (FEMA), Federal Law Enforcement Training Center (FLETC), Immigration and Customs Enforcement (ICE), Office of Intelligence and Analysis (I&A), National Protection and Programs Directorate (NPPD), Management Directorate (MGMT), OIG, Office of Operations Coordination and Planning (OPS), Science and Technology (S&T), Transportation Security Administration (TSA), United States Coast Guard (USCG), and United States Secret Service (USSS).

Homeland Security Presidential Directive 12 (HSPD-12), and Personnel Systems Security audits.[2]

We separated the results of our evaluation into 11 key areas. For each area, we identified the progress that DHS has made since our FY 2009 evaluation and the issues that need to be addressed to be more successful in the respective information security program area.

OVERALL PROGRESS

- The CISO developed the *"Fiscal Year 2010 DHS Information Security Performance Plan"* to enhance DHS' information security program and continue to make additional improvements on existing processes, such as continuous monitoring, POA&M, and C&A.

- The CISO has developed additional metrics [i.e., interconnection security agreements, Federal Information Processing Standards (FIPS) 199, E-Authentication, and Privacy Threshold Analysis (PTA)] for the FISMA scorecard to better evaluate the overall status of the department's information security program.

- The CISO revised the department's baseline IT security policies and procedures in *DHS Sensitive Systems Policy Directive 4300A* and its companion, *DHS 4300A Sensitive Systems Handbook* to reflect the changes made in DHS security policies and various National Institute of Standards and Technology (NIST) guidance.

- As of October 2009, the CISO has implemented an automated process to track and manage the security weaknesses that were identified in DHS' national security systems.

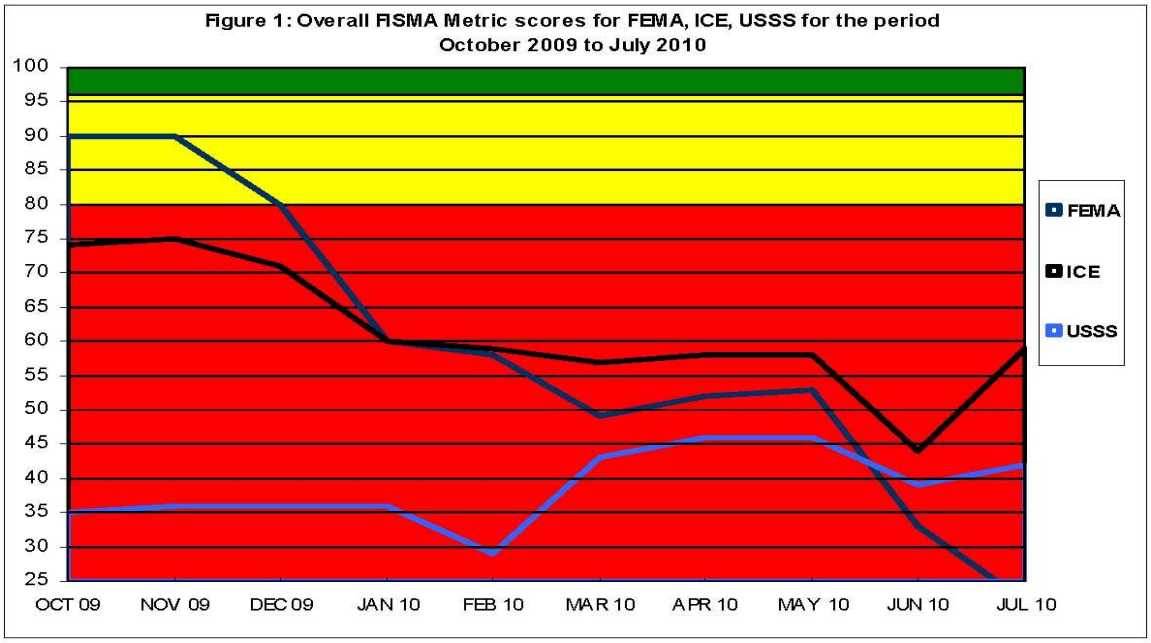
OVERALL ISSUES TO BE ADDRESSED

Despite the actions taken by the CISO to improve the department's overall information security program, components are still not executing all of the department's policies, procedures, and practices. For example, our review of FY 2010 DHS FISMA scorecards revealed that components do not sustain their information security programs on a

[2] *Stronger Security Controls Needed on Active Directory Systems* (OIG-10-86, May 2010), *U.S. Computer Emergency Readiness Team Makes Progress in Securing Cyberspace, but Challenges Remain* (OIG-10-94, June 2010), *DHS Needs to Improve the Security Posture of Its Cybersecurity Program Systems* (OIG-10-111, August 2010), *Resource and Security Issues Hinder DHS' Implementation of Homeland Security Presidential Directive 12* (OIG-10-40, January 2010), and *Management Oversight and Component Participation Are Necessary to Complete DHS' Human Resource Systems Consolidation Effort* (OIG-10-99, July 2010).

year-round basis or perform continuous monitoring to maintain system accreditations and POA&Ms.[3] We identified similar problems in our FY 2009 FISMA report.

- Three components (FEMA, ICE, and USSS) have maintained overall FISMA metric scores well below DHS' minimum performance target (80%) between January and July 2010. As a result, it is evident that components have not maintained a robust and effective continuous monitoring program to ensure that the components' C&A packages and POA&Ms are updated as appropriate and contain the necessary information for authorizing officials to make credible risk-based decisions. See Figure 1 below. We identified a similar problem in our FY 2009 report.



[3] In accordance with NIST Special Publication (SP) 800-37, continuous monitoring is the last phase of the risk management framework. OMB noted in its FY10 FISMA reporting instructions that continuous monitoring of security controls is required as part of the security authorization process to ensure controls remain effective over time (e.g., after the initial security authorization or reauthorization of an information system) in the face of changing threats, missions, environments of operation, and technologies. A robust and effective continuous monitoring program will ensure important procedures included in an agency's security authorization package (e.g., as described in system security plans, security assessment reports, and POA&Ms) are updated as appropriate and contain the necessary information for authorizing officials to make credible risk-based decisions regarding the security state of the information system on an ongoing basis.

In addition, we identified the following deficiencies:

- Artifacts supporting the component systems C&A were missing key information restricting the ability of accrediting officials to make a credible risk-based decision.

- Components have not incorporated all known information security weaknesses into their POA&Ms.

- Components have not implemented all of the required DHS baseline configuration and Federal Desktop Core Configuration (FDCC) settings on the information systems selected for review.

- Appropriate training is needed for all individuals with significant security responsibilities.

System Inventory

DHS continues to maintain a process to manage and update its systems inventory on an annual basis, including agency and contractor systems. In addition, DHS conducts site visits as part of the department's annual inventory update process.

PROGRESS

- As of August 31, 2010, DHS has a total of 677 systems, which includes a mix of major applications, general support systems, and systems owned and operated by contractor support.

- During the FY 2010 annual refresh process, DHS conducted more than 180 component site visits.

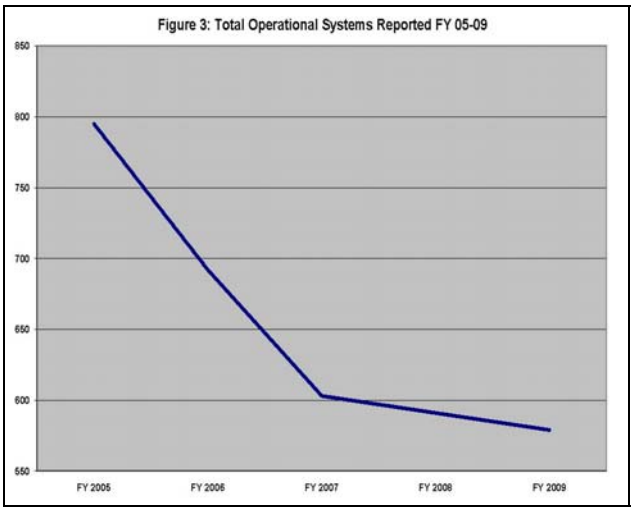
ISSUES TO BE ADDRESSED

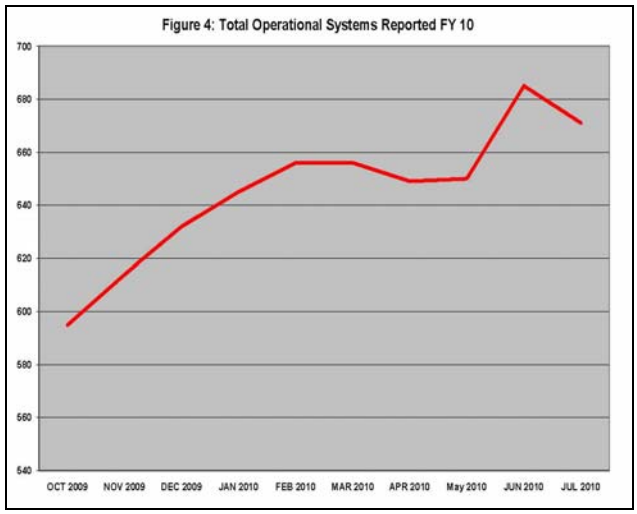
- As of August 31, 2010, DHS had identified 101 new systems across 10 components. Figure 2 identifies the new systems by component, including an overview of the system development life cycle (SDLC) status.

Figure 2: FY 2010 New Systems

	SDLC Status				
Component	Initiation	Development	Implementation	Operational	Total
CBP	0	6	0	5	11
CIS	1	7	1	8	17
FEMA	1	9	0	8	18
FLETC	0	1	0	0	1
ICE	1	5	0	10	16
MGMT	2	10	0	1	13
NPPD	1	1	0	0	2
S&T	0	7	0	4	11
TSA	0	5	0	2	7
USCG	0	4	0	1	5
Total	**6**	**55**	**1**	**39**	**101**

- Of the 101 new systems identified by the DHS Inventory Team, we noted that 39% of these new systems are reported to be in operational status. This could be an indicator that DHS' prior systems inventory methodology was not effective in capturing components' new systems into the DHS system inventory or that components were circumventing DHS' Capital Planning and Investment Control (CPIC) process in procuring new systems. Specifically, DHS' system inventory had been decreasing gradually between FY 2005 and FY 2009. However, DHS' system inventory increased by 14% or from 595 to 677 systems between October 2009 and August 2010. OMB requires agencies to (1) integrate information security into each system and fund it over the lifecycle as it is developed, and (2) meet security requirements for the operations of legacy systems before spending funds on new systems. In addition, DHS requires that business cases and investment portfolios be developed for all capital assets, such as a new information system. DHS' Investment Review Board, which includes the DHS Chief Information Officer (CIO) as a member, will review the business cases and investment portfolios for compliance with applicable criteria and ensure that the cost for security controls is integrated into the new system. Components circumventing DHS' CPIC process to procure new systems may pose a security risk to the department if security controls are inadequate. Further, DHS cannot effectively manage its information security program without an accurate and complete system inventory. See Figures 3 and 4 for system inventory changes.





- USSS had not submitted the required change request to reflect that a system, Radar Air Intrusion Detection System (RAIDS), had been decommissioned since 2005. Subsequently, USSS unintentionally uploaded the accreditation package of the replacement system, e-RAIDS, into DHS' enterprise management tool and reported that RAIDS was accredited for three years. As a result, DHS' system inventory did not reflect the actual operating status for two systems and USSS accrediting officials were not provided with the most updated information to make credible risk-based decisions regarding their systems.

- DHS has not established a real-time capability to keep track of the hardware devices and software installed on its systems.

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

Certification and Accreditation Program

DHS follows the C&A process outlined in NIST SP 800-37 and *DHS Sensitive Systems Policy Directive 4300A* to certify and accredit its systems. Components are required to use an enterprise-wide tool that incorporates NIST recommended security controls required for system C&A. The DHS C&A process requires documentation, such as system security plans, POA&Ms, risk assessments, system test and evaluation plans, security assessment reports, contingency plans, contingency plan test results, and NIST 800-53 self-assessments.

For some of the systems that have been accredited by the components, the artifacts that are required to certify and accredit a system were either missing or incomplete. In addition, some of the self-assessments were not being properly completed by the components.

PROGRESS

- DHS requires components to upload C&A artifacts into its enterprise management tool to monitor the progress in accrediting systems. The artifacts include: Authority to Operate (ATO) letter, system security plan, security assessment report, security test and evaluation, contingency plan, contingency plan test results, FIPS 199 determination, E-authentication determination, PTA/privacy impact assessment (PIA), and NIST SP 800-53 self-assessment.

- The overall quality of C&A documentation has improved in FY 2010, compared to FY 2009. For example, more system C&A packages contain the required artifacts, and there were fewer instances where security documentation was out of date.

ISSUES TO BE ADDRESSED

- We selected 25 systems from 9 components and offices to evaluate the quality of DHS' C&A process. Our review revealed that the component CISOs have not performed adequate reviews to ensure that the artifacts contain the required information to meet all applicable DHS, OMB, and NIST guidelines. For some of the systems that have been accredited by the components, the artifacts that are required to certify and accredit a system were either missing, incomplete or outdated. Without this information, agency officials cannot make credible, risk-based decisions on whether to authorize the system to operate. Specifically:

    - We identified four instances where the FIPS 199 determination was outdated or not completed properly. The FIPS 199 determination, when applied properly during the risk assessment process, helps agency officials to select applicable controls for the information systems.
    - Twenty-two instances were identified where system security plans were missing sections that included management plans, security controls, emergency changes, and incident

handling procedures. We also identified three instances where system security plans were out of date. The system security plan should be current, provide an overview of the information system, and describe the security controls implemented or planned to protect the system.
  - We identified 14 instances where contingency plans and testing results were missing certain elements, including the identification of alternate processing facilities, restoration procedures, data sensitivity handling procedures at the alternate site or off-site storage.
  - For systems that require a PIA, we determined that two systems did not have a PIA or supporting PIA documentation. In addition, we identified four instances where systems did not have completed and approved PTAs or were not filled out properly.

- As part of the C&A review, we also evaluated the quality of completed NIST SP 800-53 self-assessments. For example, we determined whether applicable controls were tested and whether components provided supporting documentation for all controls that were reported as "tested." In addition, we evaluated whether POA&Ms were created for any required control that was not tested.

  - In 14 systems, some required security controls from the NIST SP 800-53 that were not tested and were not included in POA&Ms.
  - For 11 systems, there were very few of the DHS CIO recommended supporting artifacts provided in support of the testing conducted.

See Appendix D for our assessment of DHS' Certification and Accreditation Program.

Plans of Action and Milestones Program

DHS requires components to create and maintain POA&Ms for all known IT security weaknesses. In addition, DHS performs automated reviews on POA&Ms for accuracy and completeness and the results are provided to components on a daily basis. In general, the quality of POA&Ms has improved from FY 2009 to FY 2010. Despite these improvements, components are not entering and tracking all IT security weaknesses in DHS' enterprise management tool, nor are all of the data entered by the components accurate and updated in a timely manner.

We identified a similar issue in our FY 2007, FY 2008, and FY 2009 FISMA reports.[4]

PROGRESS

- As of October 1, 2009, DHS has implemented an automated process to track IT security weaknesses identified from its national security systems.
- Components have created POA&Ms for all 158 (100%) notice of findings and recommendations for the weaknesses identified during the FY 2009 financial statement audit.[5]

ISSUES TO BE ADDRESSED

- Components are not correcting all deficiencies identified during DHS' POA&M quality reviews. Our review of DHS' quality reports identified repeated deficiencies, such as inaccurate milestones, lack of resources to mitigate the weaknesses, and delays in resolving the POA&Ms that are not corrected by the components. We identified similar problems in our FY 2008 and FY 2009 FISMA reports.

- Components are not monitoring the status of their high-priority POA&Ms or reviewing them for consistency and completeness. DHS requires component CISOs to monitor the progress of the POA&M implementation and remediation efforts. Specifically, component CISOs are required to review and approve all priority 4 and priority 5 POA&Ms to ensure that the weaknesses are properly prioritized, and that appropriate resources have been identified for remediation. Priority 4 weaknesses are assigned to initial audit findings and priority 5 weaknesses for repeat audit findings. As of June 30, 2010, only 282 out of 388 (73%) priority 4 and 5 POA&Ms have been reviewed and approved by a component CISO.

- DHS components have not created POA&Ms for all known information security weaknesses. Component CISOs are responsible for ensuring that POA&M information is entered accurately and that weaknesses are mitigated timely. For example,

[4] *Evaluation of DHS' Information Security Program for Fiscal Year 2007* (OIG-07-77, September 2007), *Evaluation of DHS' Information Security Program for Fiscal Year 2008* (OIG-08-94, September 2008) and *Evaluation of DHS' Information Security Program for Fiscal Year 2009* (OIG-09-109, September 2009).
[5] *Information Technology Management Letter for the FY 2009 DHS Integrated Audit* (OIG-10-110, May 2010).

MGMT did not create POA&Ms for findings identified in OIG audit reports issued during FY 2010.[6]

- Based on our analysis of data from DHS' enterprise management tool, as of June 30, 2010, component CISOs and information system security officers (ISSO) are not maintaining current information as to the progress of security weakness remediation and all POA&Ms are not being resolved in a timely manner.

  - Component CISOs are not updating information concerning all weaknesses where the estimated completion date has been delayed. Of the 4,122 open POA&Ms with estimated completion dates, 163 (4%) were delayed by at least 3 months (prior to April 1, 2010). Furthermore, 67 POA&Ms had an estimated completion date over 1 year old, dating as far back as March 30, 2008.
  - Resources required for the remediation of 94 (2%) of the 4,122 open POA&Ms were either not identified or listed the cost of remediation as less than $50. DHS requires a reasonable resources estimate of at least $50 be provided to mitigate the weakness identified.
  - 273 (7%) of 4,122 open POA&Ms are scheduled to take more than 2 years to mitigate the weaknesses.
  - Twelve open weaknesses are defined as significant deficiencies. Four of these 12 significant deficiencies were created more than 12 months ago.

See Appendix H for the evaluation of DHS' POA&M Program.

[6] *Resource and Security Issues Hinder DHS' Implementation of Homeland Security Presidential Directive 12* (OIG-10-40, January 2010), and *Stronger Security Controls Needed on Active Directory Systems* (OIG-10-86, May 2010).

Configuration Management

We selected 47 systems and performed manual reviews of selected servers, routers, and databases to evaluate the compliance with DHS baseline configuration requirements. Additionally, we evaluated compliance with FDCC requirements at MGMT, OIG, OPS, and TSA.[7] Results from both sets of testing revealed that the components have not implemented all of the required DHS baseline configuration and FDCC settings. We reported a similar issue in our FY 2009 report.

In addition, we performed in-depth testing on four gateway routers providing access to DHS' wide-area network, OneNet. Testing included using automated tools and manual processes to determine whether security vulnerabilities and divergence from DHS baseline configuration requirements could be exploited to gain unauthorized access to DHS' network.

ISSUES TO BE ADDRESSED

- While MGMT, OIG, OPS, and TSA reported that FDCC settings have been fully implemented, our testing revealed that not all FDCC required settings have been implemented.

- Vulnerability assessments performed at components during our Active Directory, US-CERT, and Cybersecurity review audits identified security concerns with access control, identification and authentication, and configuration management.[8] In these instances, components had not configured their systems based on DHS' configuration guidelines.

- Results from our C&A and configuration reviews indicated that components had not configured their systems based on DHS' configuration guidelines. Components included CBP, CIS, FEMA, ICE, Management, NPPD, S&T, TSA, USCG, and USSS. Deficiencies identified included:

    - Insecure Windows authentication protocols are in use.

[7] A network-based vulnerability testing tool, Nessus, was used with an FDCC Windows XP Desktop audit policy to automatically scan desktop workstations and report any misconfigurations.

[8] *Stronger Security Controls Needed on Active Directory Systems* (OIG-10-86, May 2010), *U.S. Computer Emergency Readiness Team Makes Progress in Securing Cyberspace, but Challenges Remain* (OIG-10-94, June 2010), *DHS Needs to Improve the Security Posture of Its Cybersecurity Program Systems* (OIG-10-111, August 2010).

- Windows and Solaris default accounts and the Oracle public profile are in use and are often given excess access and permissions.
- The logging capability for Cisco routers and Linux servers is not configured to capture a sufficient level of detail.
- Secure Shell, a powerful administrative tool, is insecurely configured on Linux and Solaris systems.
- Simple Network Management Protocol, a network management tool, is in use despite being expressly prohibited by DHS.

- Gateway routers for OneNet were not configured according to DHS policy. The following deficiencies were identified:

  - The logging capability is not enabled on routers to capture and send log data to a centralized server. Further, the denied access attempts are not being captured. Without the logging capability enabled, it may not be possible to reconstruct a security incident and hold individuals accountable for suspicious activities.
  - Network Time Protocol is not used by two routers to synchronize router clocks.[9] Network Time Protocol helps ensure accurate date and time stamps within log records.
  - Telnet, an insecure administration tool, is running on one router. Since information is sent in clear text using telnet, login credentials and system data may be easily compromised and exploited.
  - Outbound and inbound Internet Control Message Protocol messages are not restricted based on message types.[10] Internet Control Message Protocol messages should be blocked as specified by DHS to protect against Internet Control Message Protocol-based network attacks.
  - Multiple unused router interfaces have not been disabled as required by DHS to limit access to the router and network.

See Appendix E for information regarding DHS' Configuration Management.

[9] Network Time Protocol is used for synchronizing the clocks of computer systems and network devices.
[10] Internet Control Message Protocol is used by networked computers to send informational messages for diagnostic and routing purposes.

Incident Response and Reporting Program

DHS has established adequate incident detection, handling, and analysis procedures. However, DHS has not fully implemented its department-wide vulnerability assessment program to evaluate the security posture at all components.

PROGRESS

- DHS continues to implement its vulnerability assessment program as the DHS Security Operations Center (SOC) has the ability to perform full credential scanning on workstations and servers at CBP, CIS, FLETC, and TSA.[11]

ISSUES TO BE ADDRESSED

- DHS' vulnerability assessment program has not been deployed department-wide. The program includes a comprehensive vulnerability alert, assessment, remediation, and reporting process to effectively identify computer security vulnerabilities and track mitigation efforts to resolution. The DHS SOC only has limited access at FEMA, ICE, and MGMT, and cannot perform vulnerability assessments on their workstations and servers. Finally, the DHS SOC has no access at OIG, USCG, and USSS.

See Appendix F for information regarding DHS' Incident Response and Reporting Program.

Security Training Program

The CISO has established a process to validate components' employee security training and has an active role in developing the content for DHS training requirements. However, specific training content for employees with significant security responsibilities has not been implemented.

PROGRESS

- DHS is currently developing four specialized training courses for individuals with significant IT security responsibilities, including

[11] Full credential scanning involves unrestricted access to component networks and enables the use of software tools (i.e., Nessus, WebInspect) to perform comprehensive vulnerability scans.

ISSO, system administrators, system owners, and authorizing officials. The courses are expected to be implemented in FY 2011.

ISSUES TO BE ADDRESSED

- DHS has not yet provided appropriate, specialized security training courses to employees and contractors with significant IT security responsibilities. We reported a similar issue in our FY 2007, FY 2008, and FY 2009 FISMA reports.

- DHS does not currently identify and track all employees with or without login privileges who require security awareness training.

See Appendix G for information regarding DHS' Security Training Program.

Remote Access Program

According to DHS policy, components are responsible for managing all remote access and dial-in connections to their systems through the use of two-factor authentication and audit logging capabilities to protect sensitive information throughout transmission. However, ICE does not currently use remote access.

PROGRESS

- Seven components (CBP, CIS, FLETC, MGMT, NPPD, USCG, and USSS) have developed policies to ensure that effective controls have been implemented to protect remote connections (i.e., multi-factor authentication firewalls) from external threats.
- Encrypted virtual private network connections are used to allow users to securely access network resources remotely at CBP, CIS, FLETC, MGMT, NPPD, USCG, and USSS.

ISSUES TO BE ADDRESSED

- CIS has not enabled a remote access time-out function after 30 minutes of inactivity as required by OMB.

See Appendix I for DHS' Remote Access Program.

Account and Identity Management Program

DHS does not have a centralized capability to identify users and devices connected to its systems. Specifically, components are currently maintaining their respective account and identity management programs. However, the department plans to implement HSPD-12 personal identification verification (PIV) credentials enterprise-wide, which will be used to provide agency-wide system access management by the end of FY 2011.

PROGRESS

- The CIO has created the Identity, Credential and Access Management Program Management Office to coordinate the implementation of a department-wide identity, credentialing, and access management program.

ISSUES TO BE ADDRESSED

- OMB required agencies to issue and use PIV credentials for current employees and contractors by October 27, 2008. DHS was given an extension until December 2010 to issue PIV credentials to its employees and contractors. However, DHS does not plan on completing the issuance of HSPD-12 PIV cards to all DHS employees and contractors until September 30, 2011.[12]

See Appendix J for DHS' Account and Identity Management Program.

Continuous Monitoring Program

DHS has implemented a department-wide continuous monitoring program. Specifically, components are required to perform key control reviews, contingency testing, incident response reporting, and ongoing annual security control testing on its information systems. However, components have not satisfied all of the department's continuous monitoring requirements.

[12] *Resource and Security Issues Hinder DHS' Implementation of Homeland Security Presidential Directive 12* (OIG-10-40, January 2010).

PROGRESS

- DHS has developed policies and procedures to implement its continuous monitoring functions and requirements.

- As of July 2010, CISO has performed 89 critical control reviews on selected information systems to ensure that key controls have been implemented and to help components identify potential weaknesses or vulnerabilities.

ISSUES TO BE ADDRESSED

- DHS has not provided specific strategy documents, plans, or tools that should be followed for all continuous monitoring functions, such as vulnerability scanning, log monitoring, or notification of unauthorized devices.

- As of July 31, 2010, CISO reported that nine components (FEMA, FLETC, I&A, ICE, NPPD, OIG, OPS, USCG, and USSS) have received failing scores on the department's annual assessment requirements to evaluate the effectiveness of the required controls.

- DHS and its components do not have a real-time and automated continuous monitoring capability to keep track of their hardware/network devices, external connections, and software installed on their systems.

- Components have not provided the authorizing officials with up-to-date security status reports and documentation for all system C&A packages. For example, during our review of 25 system security plans, we identified 3 instances where documentation was out of date. Without the current information, authorizing officials cannot make a credible risk-based decision on whether to certify the system.

See Appendix K for DHS' Continuous Monitoring Program.

Contingency Planning Program

DHS has established and is maintaining an entity-wide business continuity and contingency planning program. However, components have not complied with all of DHS' contingency planning requirements.

PROGRESS

- DHS has developed continuity and disaster recovery policies and plans that provide the authority and guidance necessary to reduce the impact of a disruptive event or disaster. For example, DHS has developed the *Department of Homeland Security Headquarters Continuity of Operations Plan*, dated April 22, 2008. The plan is currently undergoing its biennial update and revision.

- DHS has developed training, testing, and exercise approaches for its business continuity and disaster recovery programs. For example, in May 2010 all components participated in the federal government continuity exercise to test activation continuity plans, systems and procedures, and mission-essential functions.

ISSUES TO BE ADDRESSED

- As part of the department's overall contingency planning and disaster recovery efforts, DHS requires all IT systems to complete an IT contingency plan detailing how the system will recover in the event of an emergency or disaster. Based on our review of certification and accreditation packages for 25 systems, we determined that contingency plans and/or testing reports for 14 systems are missing certain elements, including the identification of alternate processing facilities, restoration procedures, data sensitivity handling procedures at the alternate site or off-site storage.

See Appendix L for DHS' Contingency Planning Program.

Privacy

The Privacy Office has updated its PIA guidance and implemented an escalation policy to help improve the PIA review and approval process. In addition, the Privacy Office has made progress on implementing all requirements specified in OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007. Finally, the Privacy Office has defined the consequences for all users, and these consequences will be incorporated into the new Culture of Privacy Training that is scheduled to be released in February 2011.

PROGRESS

- The Privacy Office has established an escalation policy for any PIAs that have been in the review and approval process for an extended period of time.

- The Privacy Office has issued updated PIA guidance since our last review.

- DHS has implemented all of the requirements outlined in OMB M-07-16. Specifically, DHS has defined the consequences for users who do not comply with the policy.

Recommendations

We recommend that the CISO:

Recommendation #1: Revise and strengthen the processes to ensure that components cannot procure a new system without the department's approval and all new systems will be captured in DHS' system inventory.

Recommendation #2: Improve the OIS' review process to ensure that POA&Ms, including those for classified systems, are complete and current.

Recommendation #3: Include all applicable controls in the security documentation when certifying and accrediting systems. Systems accredited with outdated documents or without all applicable controls should not be accepted.

Recommendation #4: Improve the process to implement and maintain DHS baseline configuration requirements on all systems. The process should include testing and the use of automated tools and security templates.

Recommendation #5: Establish appropriate training that is needed for all individuals with significant security responsibilities to perform their security functions.

Recommendation #6: Evaluate and revise the department's current FDCC implementation strategy to ensure the requirements outlined in OMB M-07-11 and M-07-18 are implemented expeditiously.

Recommendation #7: Develop a strategy to implement an automated and real-time continuous monitoring process for tracking the department's inventory, including hardware devices, external connections, and software installed on its systems that complies with applicable OMB and NIST guidance. In addition, the continuous monitoring program should include performing periodic testing to evaluate the security posture at all components.

Management Comments and OIG Analysis

Management Comments to Recommendation #1

DHS concurred with recommendation 1. DHS continues to strengthen and revise processes to ensure that the procurement of new systems is approved by the department and captured into DHS' system inventory.

OIG Analysis

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

Management Comments to Recommendation #2

DHS concurred with recommendation 2. The ISO process has been improved to ensure that all POA&Ms, including those POA&Ms for classified systems, are complete and current. Updates to the *Plan of Action and Milestones (POA&M) Process Guide*, DHS 4300A Sensitive Systems Handbook, for FY 2011, will incorporate process changes based on lessons learned during FY 2010 POA&M monitoring, recently issued NIST 800-37, Revision 1, and the FY 2011 Performance Plan once finalized.

OIG Analysis

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

Management Comments to Recommendation #3

DHS concurred with recommendation 3. The C&A document templates are generated with the applicable controls by the DHS C&A tool at the time the C&A is initiated. Additionally, the required C&A documents are reviewed by the ISO Document Review Team to ensure

that all applicable controls are adequately addressed and documents which are outdated or lack all applicable controls are not accepted.

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

Management Comments to Recommendation #4
DHS concurred with recommendation 4. The CIO has identified continuous monitoring as a High Priority Initiative (HPI) 11-14 in FY 2011. The automated compliance reporting of baseline configuration requirements will be included as part of the continuous monitoring HPI. A department-wide gap analysis is being conducted to evaluate the tools and capabilities currently in place within DHS to address these concerns.

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

Management Comments to Recommendation #5
DHS concurred with recommendation 5. During FY 2011, the ISO will begin providing security training to component ISSOs, System Administrators, System Owners, and Authorizing Officials. Each course will include DHS specific knowledge, policies and procedures for performing significant security responsibilities.

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

Management Comments to Recommendation #6
DHS concurred with recommendation 6. DHS continues to make progress in implementing the FDCC requirements outlined in OMB M-07-11 and M-07-18. The Desktop Working Group tracks and monitors component progress on FDCC implementation. Pilot testing has been completed for all components; FLETC, Headquarters, and OIG have reported full deployment; CBP, CIS, FEMA, ICE, USCG,

and USSS are on track to complete full deployment by the end of FY 2011.

OIG Analysis

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

Management Comments to Recommendation #7

DHS concurred with recommendation 7. The CIO has identified continuous monitoring as a HPI 11-14 in FY 2011. A department-wide gap analysis is being conducted to evaluate the tools and capabilities currently in place within the Department to address these concerns. HPI 11-14 is reviewing FY 2010 OMB guidance issues and NIST continuous monitoring efforts to better define the department's implementation of continuous monitoring.

OIG Analysis

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

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, the requirements outlined in FISMA and using OMB's reporting instructions for FY 2010.[13] We conducted our work at the departmental level and at DHS' organizational components CBP, CIS, FEMA, FLETC, ICE, I&A, MGMT, NPPD, OIG, OPS, S&T, TSA, USCG, and USSS.

In addition to our independent evaluation, we conducted reviews of DHS' information systems and security program-related areas throughout FY 2010. This report includes the results of a limited number of systems evaluated during the year and our on-going financial statement review, including the Active Directory, US-CERT, Cybersecurity, HSPD-12, and Personnel Systems Security audits

As part of our evaluation of DHS' compliance with FISMA, we assessed DHS and its components with 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 C&A, contingency planning, continuous monitoring, incident response, identity management, inventory, privacy, remote access, security training, system reviews, and remote access; and, (5) developed our independent evaluation of DHS' information security program.

We reviewed the quality of C&A packages for a sample of 25 systems at nine components and offices: CIS, FEMA, ICE, MGMT, NPPD, S&T, TSA, USCG, and USSS, to ensure that all of the required documents were completed prior to system accreditation. In addition, we evaluated the implementation of DHS' baseline configurations and compliance with selected NIST SP 800-53 controls for 47 systems at CBP, CIS, FEMA, ICE,

[13] OMB Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, issued on April 21, 2010.

I&A, MGMT, NPPD, OPS, TSA, USCG, and USSS. We reviewed the FDCC settings at four components, including MGMT, OIG, OPS, and TSA.

We conducted our evaluation between April and August 2010 under the authority of the *Inspector General Act of 1978*, as amended, and according to the *Quality Standards for Inspections* issued by the President's Council on Integrity and Efficiency. Major OIG contributors to the evaluation are identified in Appendix N.

The principal OIG point of contact for the evaluation is Frank Deffer, Assistant Inspector General, IT Audits at (202) 254-4100.

Appendix B
Management Response to Draft Report

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

Homeland Security

SEP 20 2010

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General, IT Audits

FROM: Robert West
Chief Information Security Officer

SUBJECT: Response to draft Fiscal Year 2010 FISMA Report

This memorandum responds to the Office of Inspector General draft report titled, *Evaluation of DHS' Information Security Program for Fiscal Year 2010*, dated September 2010.

The Office of Chief Information Security Officer concurs with all seven recommendations within the report. The following actions are already underway to address these recommendations.

Recommendation #1: Revise and strengthen the department's processes to ensure that components cannot procure a new system without the department's approval and all new systems will be captured in DHS' system inventory.

DHS CISO concurs: DHS continues to strengthen and revise processes to ensure procurement of new systems are approved by the Department and captured within DHS' system inventory.

Recommendation #2: Improve the ISO' review process to ensure that POA&Ms, including those for classified systems, are complete and current.

DHS CISO concurs: The Information Security Office (ISO) process has been improved to ensure that all POA&Ms, including those POA&Ms for classified systems, are complete and current. Updates to the *Plan of Action and Milestones (POA&M) Process Guide*, DHS 4300A Sensitive Systems Handbook, for FY 2011 to incorporate process changes based on lessons learned during FY 2010 POA&M monitoring, recently issued NIST 800-37, Revision 1, and the FY 2011 Performance Plan once finalized.

Appendix B
Management Response to Draft Report

Recommendation #3: Ensure that all applicable controls are included in the security documentation when certifying and accrediting systems. Systems accredited with outdated documents or without all applicable controls should not be accepted.

DHS CISO concurs: The Certification and Accreditation (C&A) document templates are generated with the applicable controls by the DHS C&A Tool at the time the C&A is initiated. Additionally, the required C&A documents are reviewed by the ISO Document Review team to ensure that all applicable controls are adequately addressed and documents which are outdated or lack all applicable controls are not accepted.

Recommendation #4: Improve the process to ensure that DHS baseline configuration requirements are implemented and maintained on all systems. The process should include testing and the use of automated tools and security templates.

DHS CISO concurs: The DHS CIO has identified continuous monitoring as a High Priority Initiative (HPI) 11-14 in fiscal year (FY) 2011. The automated compliance reporting of baseline configuration requirements will be included as part of the continuous monitoring HPI. A department-wide gap analysis is being conducted to evaluate the tools and capabilities currently in place within DHS to address these concerns..

Recommendation #5: Establish appropriate training that is needed for all individuals with significant security responsibilities to perform their security functions.

DHS CISO concurs: During FY11, the DHS Information Security Office will begin provide security training to Component Information System Security Officers (ISSO), System Administrators (SA), System Owners (SO), and Authorizing Officials (AO). Each course will include DHS specific knowledge, policies and procedures for performing significant security responsibilities.

Recommendation #6: Evaluate and revise the department's current FDCC implementation strategy to ensure the requirements outlined in OMB M-07-11 and M-07-18 are implemented expeditiously.

DHS CISO concurs: DHS continues to make progress in implementing the FDCC requirements outlined in OMB M-07-11 and M-07-18. The Desktop Working Group (DWG) tracks and monitors Components progress on FDCC implementation. Pilot testing has been completed for all components; FLETC, HQ and OIG have reported full deployment; CBP, FEMA, ICE, USCIS, USCG, and USSS are on track to complete full deployment by the end of FY11.

Recommendation #7: Develop a strategy to implement an automated and real-time continuous monitoring process for tracking the department's inventory, including hardware devices, external connections, and software installed on its systems that complies with applicable OMB and NIST guidance. In addition, the continuous

monitoring program should include performing periodic testing to evaluate the security posture at all components.

DHS CISO concurs: The DHS CIO has identified continuous monitoring as a High Priority Initiative (HPI) 11-14 in FY2011. A department-wide gap analysis is being conducted to evaluate the tools and capabilities currently in place within the Department to address these concerns. HPI 11-14 is reviewing FY2010 OMB guidance issues and NIST continuous monitoring efforts to better define the Department's implementation of continuous monitoring.

Should you have any questions, please call me at (202) 357-6110, or your staff may contact Emery Csulak, Director of Compliance and Technology at (202) 357-6113.

cc: Chief Information Officer
Component CIOs
Component CISOs

Question 1: System Inventory													
1. Identify the number of agency and contractors systems by component and FIPS 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 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 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	21	5	1	0	22	5	5	100%	5	100%	5	100%
	Moderate	42	2	1	0	43	2	2	100%	1	50%	2	100%
	Low	1	0	2	0	3	0	0	0%	0	0%	0	0%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	**64**	**7**	**4**	**0**	**68**	**7**	**7**	**100%**	**6**	**86%**	**7**	**100%**
CIS	High	1	0	3	0	4	0	0	0%	0	0%	0	0%
	Moderate	63	4	28	3	91	7	6	86%	6	86%	7	100%
	Low	1	0	3	1	4	1	0	0%	0	0%	0	0%
	Not Categorized	3	0	2	0	5	0	0	0%	0	0%	0	0%
	Sub-total	**68**	**4**	**36**	**4**	**104**	**8**	**6**	**75%**	**6**	**75%**	**7**	**88%**

DNDO	High	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Moderate	1	0	0	0	1	0	0	0%	0	0%	0	0%
	Low	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-Total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0%**	**0**	**0%**	**0**	**0%**
FEMA	High	14	4	4	1	18	5	5	100%	3	60%	3	60%
	Moderate	23	3	13	2	36	5	5	100%	5	100%	3	60%
	Low	4	0	1	0	5	0	0	0%	0	0%	0	0%
	Not Categorized	31	1	0	0	31	1	0	0%	0	0%	0	0%
	Sub-total	**72**	**8**	**18**	**3**	**90**	**11**	**10**	**91%**	**8**	**73%**	**6**	**55%**
FLETC	High	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Moderate	11	2	1	0	12	2	2	100%	2	100%	2	100%
	Low	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	**11**	**2**	**1**	**0**	**12**	**2**	**2**	**100%**	**2**	**100%**	**2**	**100%**
I&A	High	1	1	1	0	2	1	1	100%	1	100%	0	0%
	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%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	**1**	**1**	**1**	**0**	**2**	**1**	**1**	**100%**	**1**	**100%**	**0**	**0%**
ICE	High	11	2	9	2	20	4	4	100%	2	50%	3	75%
	Moderate	33	1	29	2	62	3	3	100%	3	100%	3	100%
	Low	4	0	3	0	7	0	0	0%	0	0%	0	0%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	**48**	**3**	**41**	**4**	**89**	**7**	**7**	**100%**	**5**	**71%**	**6**	**86%**
ISO	High	2	0	1	0	3	0	0	0%	0	0%	0	0%
	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%

	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	**2**	**0**	**1**	**0**	**3**	**0**	**0**	**0%**	**0**	**0%**	**0**	**0%**
ITSO RMC	High	7	1	6	4	13	5	5	100%	5	100%	5	100%
	Moderate	4	4	5	3	9	7	7	100%	6	86%	5	71%
	Low	0	0	2	1	2	1	1	100%	1	100%	1	100%
	Not Categorized	0	0	4	0	4	0	0	0%	0	0%	0	0%
	Sub-total	**11**	**5**	**17**	**8**	**28**	**13**	**13**	**100%**	**12**	**92%**	**11**	**85%**
NPPD	High	7	2	5	0	12	2	2	100%	2	100%	2	100%
	Moderate	4	0	11	5	15	5	5	100%	4	80%	4	80%
	Low	2	1	2	0	4	1	1	100%	1	100%	1	100%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	**13**	**3**	**18**	**5**	**31**	**8**	**8**	**100%**	**7**	**88%**	**7**	**88%**
OIG	High	3	1	0	0	3	1	1	100%	1	100%	0	0%
	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%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	**3**	**1**	**0**	**0**	**3**	**1**	**1**	**100%**	**1**	**100%**	**0**	**0%**
OPS	High	2	0	0	0	2	0	0	0%	0	0%	0	0%
	Moderate	2	1	0	0	2	1	1	100%	1	100%	1	100%
	Low	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	**4**	**1**	**0**	**0**	**4**	**1**	**1**	**100%**	**1**	**100%**	**1**	**100%**
S&T	High	3	0	0	0	3	0	0	0%	0	0%	0	0%
	Moderate	5	1	14	0	19	1	1	100%	1	100%	1	100%
	Low	1	0	2	0	3	0	0	0%	0	0%	0	0%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	**9**	**1**	**16**	**0**	**25**	**1**	**1**	**100%**	**1**	**100%**	**1**	**100%**

TSA	High	22	2	4	0	26	2	2	100%	2	100%	2	100%
	Moderate	28	4	18	0	46	4	4	100%	3	75%	4	100%
	Low	4	0	2	0	6	0	0	0%	0	0%	0	0%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	**54**	**6**	**24**	**0**	**78**	**6**	**6**	**100%**	**5**	**83%**	**6**	**100%**
USCG	High	37	2	5	2	42	4	4	100%	2	50%	2	50%
	Moderate	53	4	18	3	71	7	5	71%	6	86%	4	57%
	Low	11	1	5	1	16	2	2	100%	1	50%	2	100%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	**101**	**7**	**28**	**6**	**129**	**13**	**11**	**85%**	**9**	**69%**	**8**	**62%**
USSS	High	3	1	0	0	3	1	0	0%	0	0%	1	100%
	Moderate	6	0	0	0	6	0	0	0%	0	0%	0	0%
	Low	1	1	0	0	1	1	1	100%	1	100%	1	100%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	**10**	**2**	**0**	**0**	**10**	**2**	**1**	**50%**	**1**	**50%**	**2**	**100%**
Agency Totals	**High**	**134**	**21**	**39**	**9**	**173**	**30**	**29**	**97%**	**23**	**77%**	**23**	**77%**
	Moderate	**275**	**26**	**138**	**18**	**413**	**44**	**41**	**93%**	**38**	**86%**	**36**	**82%**
	Low	**29**	**3**	**22**	**3**	**51**	**6**	**5**	**83%**	**4**	**67%**	**5**	**83%**
	Not Categorized	**34**	**1**	**6**	**0**	**40**	**1**	**0**	**0%**	**0**	**0%**	**0**	**0%**
	Total	**472**	**51**	**205**	**30**	**677**	**81**	**75**	**93%**	**65**	**80%**	**64**	**79%**

Appendix D
Status of Certification and Accreditation Program

Section 2: Status of Certification and Accreditation Program	
	Response:
1. Choose one: **A. The Agency has established and is maintaining a certification and accreditation program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:** **1. Documented policies and procedures describing the roles and responsibilities of participants in the certification and accreditation process.** **2. Establishment of accreditation boundaries for agency information systems.** **3. Categorizes information systems.** **4. Applies applicable minimum baseline security controls,** **5. Assesses risks and tailors security control baseline for each system.** **6. Assessment of the management, operational, and technical security controls in the information system.** **7. Risks to Agency operations, assets, or individuals analyzed and documented in the system security plan, risk assessment, or an equivalent document.** **8. The accreditation official is provided (i) the security assessment report from the certification agent providing the results of the independent assessment of the security controls and recommendations for corrective actions; (ii) the plan of action and milestones from the information system owner indicating actions taken or planned to correct deficiencies in the controls and to reduce or eliminate vulnerabilities in the information system; and (iii) the updated system security plan with the latest copy of the risk assessment.**	✓
B. The Agency has established and is maintaining a certification and accreditation program. However, the Agency needs to make significant improvements as noted below.	
C. The Agency has not established a certification and accreditation program.	

Appendix D
Status of Certification and Accreditation Program

2. If B. chosen above, indicate areas that need significant improvement: **a. Certification and accreditation policy is not fully developed.** **b. Certification and accreditation procedures are not fully developed or consistently implemented.** **c. Information systems are not properly categorized (FIPS 199/SP 800-60).** **d. Accreditation boundaries for agency information systems are not adequately defined.** **e. Minimum baseline security controls are not adequately applied to information systems (FIPS 200/SP 800-53).** **f. Risk assessments are not adequately conducted (SP 800-30).** **g. Security control baselines are not adequately tailored to individual information systems (SP 800-30).** **h. Security plans do not adequately identify security requirements (SP 800-18).** **i. Inadequate process to assess security control effectiveness (SP800-53A).** **j. Inadequate process to determine risk to agency operations, agency assets, or individuals, or to authorize information systems to operate (SP 800-37).** **k. Inadequate process to continuously track changes to information systems that may necessitate reassessment of control effectiveness (SP 800-37).** **l. Other**	
3. Comments:	• DHS bases its C&A process on NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* and *DHS Sensitive Systems Policy Directive 4300A for its unclassified systems.* Components are required to follow Department of Defense Information Assurance Certification and Accreditation Process when certifying and accrediting its classified systems. • Based on our review of C&A packages for 25 systems, we determined some artifacts required to certify and accredit a system were either missing, incomplete, or outdated. In addition, some of the self-assessments were not being properly completed by the components.

Appendix E
Status of Configuration Management

Section 3: Status of Configuration Management	
	Response:
4. Choose one: **A. The Agency has established and is maintaining a security configuration management program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:** **1. Documented policies and procedures for configuration management.** **2. Standard baseline configurations.** **3. Scanning for compliance and vulnerabilities with baseline configurations.** **4. FDCC baseline settings fully implemented and/or any deviations from FDCC baseline settings fully documented.** **5. Documented proposed or actual changes to the configuration settings.** **6. Process for the timely and secure installation of software patches.**	✓
B. The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below.	
C. The Agency has not established a security configuration management program.	
5. If B. chosen above, indicate areas that need significant improvement: **a. Configuration management policy is not fully developed.** **b. Configuration management procedures are not fully developed or consistently implemented.** **c. Software inventory is not complete (NIST 800-53: CM-8).** **d. Standard baseline configurations are not identified for all software components (NIST 800-53: CM-8).** **e. Hardware inventory is not complete (NIST 800-53: CM-8).** **f. Standard baseline configurations are not identified for all hardware components (NIST 800-53: CM-2).** **g. Standard baseline configurations are not fully implemented (NIST 800-53: CM-** **h. FDCC is not fully implemented (OMB) and/or all deviations are not fully documented.** **i. Software scanning capabilities are not fully implemented (NIST 800-53: RA-5, SI-2).** **j. Configuration related vulnerabilities have not been remediated in a timely manner (NIST 800-53: CM-4, CM-6, RA-5, SI-2).** **k. Patch management process is not fully developed (NIST 800-53: CM-3, SI-2).** **l. Other**	

6. Identify baselines reviewed: **a. Software Name** **b. Software Version**	**- Cisco IOS** **- Oracle** **- Microsoft Structured Query Language Server** **- Security Enhanced Linux /Linux** **- Solaris** **- Windows Server** **- Windows XP**
7. Comments:	• Based on our review of 44 systems at DHS components, we found that components had not fully implemented DHS baseline configuration settings. • While MGMT, OIG, OPS, and TSA reported that FDCC setting had been fully implemented, our testing revealed that not all FDCC required settings had been implemented. • Based on our in-depth system testing, we determined the OneNet access routers are not configured according to DHS policy.

Appendix F
Status of Incident Response and Reporting Program

Section 4: Status of Incident Response & Reporting Program	
	Response:
8. Choose one: **A. The Agency has established and is maintaining an incident response and reporting program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:** **1. Documented policies and procedures for responding and reporting to incidents.** **2. Comprehensive analysis, validation and documentation of incidents.** **3. When applicable, reports to US-CERT within established timeframes.** **4. When applicable, reports to law enforcement within established timeframes.** **5. Responds to and resolves incidents in a timely manner to minimize further damage.** **B. The Agency has established and is maintaining an incident response and reporting program. However, the Agency needs to make significant improvements as noted below.** **C. The Agency has not established an incident response and reporting program.**	✓
9. If B. chosen above, indicate areas that need significant improvement: **a. Incident response and reporting policy is not fully developed.** **b. Incident response and reporting procedures are not fully developed, sufficiently detailed, or consistently implemented.** **c. Incidents were not identified in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).** **d. Incidents were not reported to US-CERT as required (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).** **e. Incidents were not reported to law enforcement as required.** **f. Incidents were not resolved in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).** **g. Incidents were not resolved to minimize further damage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).** **h. There is insufficient incident monitoring and detection coverage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).** **i. Other**	
10. Comments:	

Appendix G
Status of Security Training Program

Section 5: Status of Security Training Program	
	Response:
11. Choose one: **A. The Agency has established and is maintaining a security training program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:** **1. Documented policies and procedures for security awareness training.** **2. Documented policies and procedures for specialized training for users with significant information security responsibilities.** **3. Appropriate training content based on the organization and roles.** **4. Identification and tracking of all employees with login privileges that need security awareness training.** **5. Identification and tracking of employees without login privileges that require security awareness training.** **6. Identification and tracking of all employees with significant information security responsibilities that require specialized training.**	
B. The Agency has established and is maintaining a security training program. However, the Agency needs to make significant improvements as noted below.	✓
C. The Agency has not established a security training program.	

Appendix G
Status of Security Training Program

12. If B. chosen above, indicate areas that need significant improvement: **a. Security awareness training policy is not fully developed.** **b. Security awareness training procedures are not fully developed, sufficiently detailed, or consistently implemented.** **c. Specialized security training policy is not fully developed.** **d. Specialized security training procedures are not fully developed or sufficiently detailed (SP 800-50, SP 800-53).** **e. Training material for security awareness training does not contain appropriate content for the Agency (SP 800-50, SP 800-53).** **f. Identification and tracking of employees with login privileges that require security awareness training is not adequate (SP 800-50, SP 800-53).** **g. Identification and tracking of employees without login privileges that require security awareness training is not adequate (SP 800-50, SP 800-53).** **h. Identification and tracking of employees with significant information security responsibilities is not adequate (SP 800-50, SP 800-53).** **i. Training content for individuals with significant information security responsibilities is not adequate (SP 800-53, SP 800-16).** **j. Less than 90% of employees with login privileges attended security awareness training in the past year.** **k. Less than 90% of employees, contractors, and other users with significant security responsibilities attended specialized security awareness training in the past year.** **l. Other**	**f, g, i**
13. Comments:	Although DHS has established and is maintaining a security training program that is generally consistent with NIST's and OMB's FISMA requirements, we identified the following deficiencies: • DHS has not yet implemented specific training content for employees with significant security responsibilities. • DHS does not currently have the capability to identify and track all employees with or without login privileges who require security awareness training.

Appendix H
Status of Plans of Actions and Milestones (POA&M) Program

Section 6: Status of Plans of Actions & Milestones (POA&M) Program	
	Response:
14. Choose one: **A. The Agency has established and is maintaining a POA&M program that is generally consistent with NIST's and OMB's FISMA requirements and tracks and monitors known information security weaknesses. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:** **1. Documented policies and procedures for managing all known IT security weaknesses.** **2. Tracks, prioritizes and remediates weaknesses.** **3. Ensures remediation plans are effective for correcting weaknesses.** **4. Establishes and adheres to reasonable remediation dates.** **5. Ensures adequate resources are provided for correcting weaknesses.** **6. Program officials and contractors report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POAM activities at least quarterly.**	✓
B. The Agency has established and is maintaining a POA&M program that tracks and remediates known information security weaknesses. However, the Agency needs to make significant improvements as noted below.	
C. The Agency has not established a POA&M program.	

Appendix H
Status of Plans of Actions and Milestones (POA&M) Program

15. If B. chosen above, indicated areas that need significant improvement: **a. POA&M Policy is not fully developed.** **b. POA&M procedures are not fully developed, sufficiently detailed, or consistently implemented.** **c. POA&Ms do not include all known security weaknesses (OMB M-04-25).** **d. Remediation actions do not sufficiently address weaknesses (NIST SP 800-53, Rev. 3, Sect. 3.4 Monitoring Security Controls).** **e. Initial date of security weaknesses are not tracked (OMB M-04-25).** **f. Security weaknesses are not appropriately prioritized (OMB M-04-25).** **g. Estimated remediation dates are not reasonable (OMB M-04-25).** **h. Initial target remediation dates are frequently missed (OMB M-04-25).** **i. POA&Ms are not updated in a timely manner (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).** **j. Costs associated with remediating weaknesses are not identified (NIST SP 800-53, Rev. 3, Control PM-3 & OMB M-04-25).** **k. Agency CIO does not track and review POA&Ms (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).** **l. Other**	
16. Comments:	• DHS requires components to create and manage POA&Ms for all known IT security weaknesses. • As of June 30, 2010, DHS has 4,122 open POA&Ms. However, POA&Ms have not been created for all weaknesses identified during the C&A process. Furthermore, components are not consistently maintaining and tracking their classified POA&Ms. • DHS creates quarterly POA&M progress reports, tracking weakness remediation and maintenance.

Appendix I
Status of Remote Access Program

Section 7: Status of Remote Access Program	
	Response:
17. Choose one: **A. The Agency has established and is maintaining a remote access program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:** **1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.** **2. Protects against unauthorized connections or subversion of authorized connections.** **3. Users are uniquely identified and authenticated for all access.** **4. If applicable, multi-factor authentication is required for remote access.** **5. Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.** **6. Requires encrypting sensitive files transmitted across public networks or stored on mobile devices and removable media such as CDs and flash drives.** **7. Remote access sessions are timed-out after a maximum of 30 minutes of inactivity after which re-authentication is required.**	✓
B. The Agency has established and is maintaining a remote access program. However, the Agency needs to make significant improvements as noted below.	
C. The Agency has not established a program for providing secure remote access.	

18. If B. chosen above, indicate areas that need significant improvement: **a. Remote access policy is not fully developed.** **b. Remote access procedures are not fully developed, sufficiently detailed, or consistently implemented.** **c. Telecommuting policy is not fully developed (NIST 800-46, Section 5.1).** **d. Telecommuting procedures are not fully developed or sufficiently detailed (NIST 800-46, Section 5.4).** **e. Agency cannot identify all users who require remote access (NIST 800-46, Section 4.2, Section 5.1).** **f. Multi-factor authentication is not properly deployed (NIST 800-46, Section 2.2, Section 3.3).** **g. Agency has not identified all remote devices (NIST 800-46, Section 2.1).** **h. Agency has not determined all remote devices and/or end user computers have been properly secured (NIST 800-46, Section 3.1 and 4.2).** **i. Agency does not adequately monitor remote devices when connected to the agency's networks remotely (NIST 800-46, Section 3.2).** **j. Lost or stolen devices are not disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines).** **k. Remote access rules of behavior are not adequate (NIST 800-53, PL-4).** **l. Remote access user agreements are not adequate (NIST 800-46, Section 5.1, NIST 800-53, PS-6).** **m. Other**	
19. Comments:	• According to DHS policy, components are responsible for managing all remote access and dial in connections to their systems through the use of two-factor authentication and audit logging capabilities to protect sensitive information throughout transmission. • Seven out of eight components are currently utilizing remote access programs. • One component out of the seven has not implemented a time-out function after a maximum of 30 minutes of inactivity.

Appendix J
Status of Account and Identity Management Program

Section 8: Status of Account and Identity Management Program	
	Response:
20. Choose one: **A. The Agency has established and is maintaining an account and identity management program that is generally consistent with NIST's and OMB's FISMA requirements and identifies users and network devices. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:** **1. Documented policies and procedures for account and identity management.** **2. Identifies all users, including federal employees, contractors, and others who access Agency systems.** **3. Identifies when special access requirements (e.g., multifactor authentication) are necessary.** **4. If multi-factor authentication is in use, it is linked to the Agency's PIV program.** **5. Ensures that the users are granted access based on needs and separation of duties principles.** **6. Identifies devices that are attached to the network and distinguishes these devices from users.** **7. Ensures that accounts are terminated or deactivated once access is no longer required.**	✓
B. The Agency has established and is maintaining an account and identity management program that identifies users and network devices. However, the Agency needs to make significant improvements as noted below.	
C. The Agency has not established an account and identity management program.	

Appendix J
Status of Account and Identity Management Program

21. If B. chosen above, indicated areas that need significant improvement: **a. Account management policy is not fully developed.** **b. Account management procedures are not fully developed, sufficiently detailed, or consistently implemented.** **c. Active Directory is not properly implemented (NIST 800-53, AC-2).** **d. Other Non-Microsoft account management software is not properly implemented (NIST 800-53, AC-2).** **e. Agency cannot identify all User and Non-User Accounts (NIST 800-53, AC-2).** **f. Accounts are not properly issued to new users (NIST 800-53, AC-2).** **g. Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2).** **h. Agency does not use multi-factor authentication where required (NIST 800-53, IA-2).** **i. Agency has not adequately planned for implementation of PIV for logical access (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01).** **j. Privileges granted are excessive or result in capability to perform conflicting functions (NIST 800-53, AC-2, AC-6).** **k. Agency does not use dual accounts for administrators (NIST 800-53, AC-5, AC-6).** **l. Network devices are not properly authenticated (NIST 800-53, IA-3).** **m. Other**	
22. Comments:	• DHS does not utilize multi-factor authentication for access and identity management. However, DHS is in the process of deploying HSPD-12 credentials to the entire department with plans of using the PIV cards for multi-factor authentication.

Appendix K
Status of Continuous Monitoring Program

Section 9: Status of Continuous Monitoring Program	
	Response:
23. Choose one: **A. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:** **1. Documented policies and procedures for continuous monitoring.** **2. Documented strategy and plans for continuous monitoring, such as vulnerability scanning, log monitoring, notification of unauthorized devices, sensitive new accounts, etc.** **3. Ongoing assessments of selected security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.** **4. Provides system authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions.**	
B. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems. However, the Agency needs to make significant improvements as noted below.	✓
C. The Agency has not established a continuous monitoring program.	
24. If B. chosen above, indicate areas that need significant improvement: **a. Continuous monitoring policy is not fully developed.** **b. Continuous monitoring procedures are not fully developed, sufficiently detailed, or consistently implemented.** **c. Strategy or plan has not been fully developed for entity-wide continuous monitoring (NIST 800-37).** **d. Ongoing assessments of selected security controls (system-specific, hybrid, and common) have not been performed (NIST 800-53, NIST 800-53A).** **e. The following were not provided to the system authorizing official or other key system officials: security status reports covering continuous monitoring results, updates to security plans, security assessment reports, and POA&Ms (NIST 800-53, NIST 800-53A).** **f. Other**	**c, d, e**

25. Comments:	DHS has established an entity-wide continuous monitoring program that assesses the security state of information systems that is generally consistent with NIST's and OMB's FISMA requirements. However, we identified the following deficiencies: • DHS has not provided specific strategy documents, plans, or tools that should be followed for all continuous monitoring functions, such as vulnerability scanning, log monitoring, or notification of unauthorized devices. However, components are performing continuous monitoring functions, such as vulnerability scanning and log monitoring. • Based on our review of 25 systems, we determined that 14 did not have all required NIST SP 800-53 controls tested and included in a POA&M. • All DHS components have not provided authorizing officials and other key officials with up-to-date security status reports with updates to security documentation. For example, during our review of 25 system security plans, we identified 3 instances where documentation was out of date.

Appendix L
Status of Contingency Planning Program

Section 10: Status of Contingency Planning Program	
	Response:
26. Choose one: **A. The Agency established and is maintaining an entity-wide business continuity/disaster recovery program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:** **1. Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster.** **2. The agency has performed an overall Business Impact Assessment.** **3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures.** **4. Testing of system specific contingency plans.** **5. The documented business continuity and disaster recovery plans are ready for implementation.** **6. Development of training, testing, and exercises (TT&E) approaches.** **7. Performance of regular ongoing testing or exercising of continuity/disaster recovery plans to determine effectiveness and to maintain current plans.**	✓
B. The Agency has established and is maintaining an entity-wide business continuity/disaster recovery program. However, the Agency needs to make significant improvements as noted below.	
C. The Agency has not established a business continuity/disaster recovery program.	

27. If B. chosen above, indicate areas that need significant improvement: **a. Contingency planning policy is not fully developed.** **b. Contingency planning procedures are not fully developed, sufficiently detailed, or consistently implemented.** **c. An overall business impact assessment has not been performed (NIST SP 800-34).** **d. Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (NIST SP 800-34).** **e. A business continuity/disaster recovery plan has not been developed (FCD1, NIST SP 800-34).** **f. A business continuity/disaster recovery plan has been developed, but not fully implemented (FCD1, NIST SP 800-34).** **System contingency plans missing or incomplete (FCD1, NIST SP 800-34, NIST SP 800-53).** **g. Critical systems contingency plans are not tested (FCD1, NIST SP 800-34, NIST SP 800-53).** **h. Training, testing, and exercises approaches have not been developed (FCD1, NIST SP 800-34, NIST 800-53).** **i. Training, testing, and exercises approaches have been developed, but are not fully implemented (FCD1, NIST SP 800-34, NIST SP 800-53).** **j. Disaster recovery exercises were not successful revealed significant weaknesses in the contingency planning (NIST SP 800-34).** **k. After-action plans did not address issues identified during disaster recovery exercises (FCD1, NIST SP 800-34).** **l. Critical systems do not have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).** **m. Alternate processing sites are subject to same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).** **n. Backups of information are not performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).** **o. Backups are not appropriately tested (FCD1, NIST SP 800-34, NIST SP 800-53).** **p. Backups are not properly secured and protected (FCD1, NIST SP 800-34, NIST SP 800-53).** **q. Other**	
28. Comments:	DHS has established and is maintaining an entity-wide business continuity/disaster recovery program that is generally consistent with NIST's and OMB's FISMA requirements. However, based on our review of 25 system certification and accreditation plans, we identified that contingency plans and/or testing reports for 14 systems are missing certain elements, such as the identification of alternate processing facilities, restoration procedures, data sensitivity handling procedures at the alternate site or off-site storage.

Appendix M
Status of Agency Program to Oversee Contractor Systems

Section 11: Status of Agency Program to Oversee Contractor Systems	
	Response:
29. Choose one: **A. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:** **1. Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors or other entities and that the Agency obtains sufficient assurance that security controls of systems operated by contractors or others on its behalf are effectively implemented and comply with federal and agency guidelines.** **2. A complete inventory of systems operated on the Agency's behalf by contractors or other entities.** **3. The inventory identifies interfaces between these systems and Agency-operated systems.** **4. The agency requires agreements (MOUs, Interconnect Service Agreements, contracts, etc.) for interfaces between these systems and those that is owns and operates.** **5. The inventory, including interfaces, is updated at least annually.** **6. Systems that are owned or operated by contractors or entities are subject to and generally meet NIST and OMB's FISMA requirements.**	✓
B. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. However, the Agency needs to make significant improvements as noted below.	
C. The Agency does not have a program to oversee systems operated on its behalf by contractors or other entities.	

Appendix M
Status of Agency Program to Oversee Contractor Systems

30. If B. chosen above, indicated areas that need significant improvement: **a. Policies to oversee systems operated on the Agency's behalf by contractors or other entities are not fully developed.** **b. Procedures to oversee systems operated on the Agency's behalf by contractors or other entities are not fully developed, sufficiently detailed, or consistently implemented.** **c. The inventory of systems owned or operated by contractors or other entities is not sufficiently complete.** **d. The inventory does not identify interfaces between contractor/entity-operated systems to Agency owned and operated systems.** **e. The inventory of contractor/entity operated systems, including interfaces, is not updated at least annually.** **f. Systems owned or operated by contractors and entities are not subject to NIST and OMB's FISMA requirements (e.g., certification and accreditation requirements).** **g. Systems owned or operated by contractor's and entities do not meet NIST and OMB's FISMA requirements (e.g., certifications and accreditation requirements).** **h. Interface agreements (e.g., MOUs) are not properly documented, authorized, or maintained.** **i. Other**	
31. Comments:	• DHS has established and maintains a program to oversee systems operated on its behalf by contractors or other entities.

Appendix N
Major Contributors to this Report

Information Security Audit Division

Chiu-Tong Tsang, Director
Aaron Zappone, Program Analyst
Amanda Strickler, IT Specialist
Michael Kim, IT Auditor
David Bunning, IT Specialist
Megan Ryno, Program Analyst
Joseph Landas, Management/Program Assistant
Michael Bann, Management/Program Assistant
Joshua Wessling, Management/Program Assistant
Basil Badley, Management/Program Assistant

Advanced Technology Division

John Molesky, IT Specialist

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Assistant Secretary for Legislative and Intergovernmental Affairs
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
Chief Information Officer
Deputy Chief Information Officer
Chief Financial Officer
Chief Privacy Officer
Chief Human Capital Officer
Chief Information Security Officer
Director, GAO/OIG Liaison Office
Director, Compliance and Oversight Program, Office of CIO
Deputy Director, Compliance and Oversight Program, Office of CIO
Director, Privacy Compliance
Chief Information Officer Audit Liaison
Chief Information Security Officer Audit Liaison
Privacy Office Audit Liaison
Component CIOs
Component CISOs

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigations - Hotline,
  245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.