# Department of Homeland Security
Office of Inspector General

# Evaluation of DHS' Information Security Program for Fiscal Year 2009

## (Redacted)

OIG-09-109

September 2009

*Office of Inspector General*

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

Homeland Security

September 23, 2009

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. It is our hope that 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.

Richard L. Skinner

Richard L. Skinner
Inspector General

# Table of Contents/Abbreviations

## Appendices

## Abbreviations

| | |
|---|---|
| ATO | Authority to Operate |
| C&A | Certification and Accreditation |
| CBP | United States Customs and Border Protection |
| CIO | Chief Information Officer |
| CIS | Citizenship and Immigration Services |
| CISO | Chief Information Security Officer |
| DHS | Department of Homeland Security |
| FDCC | Federal Desktop Core Configuration |

# Table of Contents/Abbreviations

| | |
|---|---|
| FEMA | Federal Emergency Management Agency |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Management Act |
| FLETC | Federal Law Enforcement Training Center |
| FY | Fiscal Year |
| ICE | United States Immigration and Customs Enforcement |
| ISO | Information Security Office |
| ISSO | Information Systems Security Officer |
| IT | Information Technology |
| Management | Management Directorate |
| NFRs | Notice of Findings and Recommendations |
| NIST | National Institute of Standards and Technology |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| POA&M | Plan of Action and Milestones |
| PTA | Privacy Threshold Analysis |
| S&T | Science and Technology |
| SOC | Security Operations Center |
| SP | Special Publication |
| Training Office | Information Security Training, Education, and Awareness Office |
| TSA | Transportation Security Administration |
| USCG | United States Coast Guard |
| USSS | United States Secret Service |

# OIG

***Department of Homeland Security***
***Office of Inspector General***

## Executive Summary

We reviewed the Department of Homeland Security (DHS') information security program and practices to comply with the requirements of the *Federal Information Security Management Act of 2002* (*Public Law* 107-347, Sections 301-305). In evaluating DHS' progress in implementing its agency-wide information security program, we reviewed the department's Plan of Action and Milestones (POA&M), as well as its certification and accreditation (C&A) processes. We also performed an evaluation of the department's privacy program. Fieldwork was performed at both the program and component levels.

The department continues to improve and strengthen its security program. During the past year, DHS developed and implemented the fiscal year (FY) 2009 information security performance plan to enhance its security program, focusing 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, our review of DHS scorecards for a two year period revealed that 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:

- Systems are being accredited though key information is missing.
- POA&Ms are not being created for all known information security weaknesses.
- POA&M weaknesses are not being mitigated in a timely manner.
- Baseline security configurations are not being implemented for all systems.

Components' execution of DHS' policies, procedures, and practices must be improved in order for the department to ensure that all information security weaknesses are tracked and remediated, and to

enhance the quality of system C&A. Additional information security program areas that need improvement include configuration management, incident detection and analysis, specialized training, and privacy.

We are making eight recommendations to the Chief Information Officer and Chief Privacy Officer. The department 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 the *Federal Information Security Management Act* (FISMA). 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.

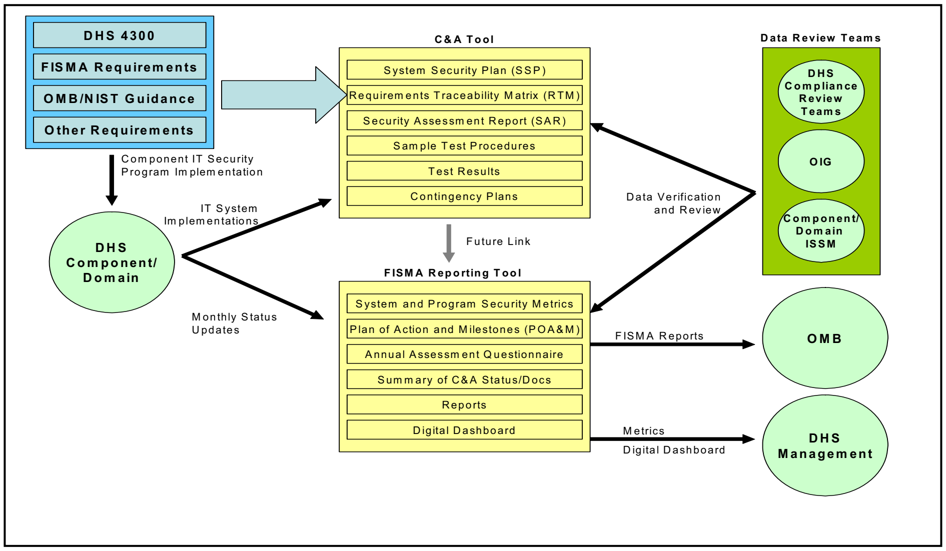
FISMA requires each federal agency to develop, document, and implement an agency-wide security program. The agency's security program should protect the information and the information systems that support the operations and assets of the agency, including those provided or managed by another agency, 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-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, on August 20, 2009. 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 Chief Information Security Officer (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-assessment 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 to assist DHS components in quickly and efficiently developing their security accreditation packages. Below is an illustration on how the enterprise management and C&A tools are used within the department to collect, manage, and report information security metrics.

*DHS' Enterprise Security Management Tools Usage*


DHS 4300
FISMA Requirements
OMB/NIST Guidance
Other Requirements
Component IT Security Program Implementation
DHS Component/ Domain
IT System Implementations
Monthly Status Updates
C&A Tool
System Security Plan (SSP)
Requirements Traceability Matrix (RTM)
Security Assessment Report (SAR)
Sample Test Procedures
Test Results
Contingency Plans
Future Link
FISMA Reporting Tool
System and Program Security Metrics
Plan of Action and Milestones (POA&M)
Annual Assessment Questionnaire
Summary of C&A Status/Docs
Reports
Digital Dashboard
Data Verification and Review
Data Review Teams
DHS Compliance Review Teams
OIG
Component/ Domain ISSM
FISMA Reports
OMB
Metrics
Digital Dashboard
DHS Management

Source: *DHS 4300A Sensitive Systems Handbook, Attachment E – FISMA Reporting*

# Results of Independent Evaluation

Based on the requirements outlined in FISMA and OMB's annual reporting instructions, our independent evaluation focused on seven key areas of DHS' information security program, (i.e., system inventory; certification and accreditation process; plan of action and milestones process; configuration management; incident detection, handling, and analysis procedures; security training; and privacy). In addition to our independent evaluation, we conducted reviews of DHS' information systems and security program-related areas throughout FY 2009. This report includes the results of a limited number of systems evaluated during the year and our on-going financial statement review, including the LAN-A, OneNet, Los Angeles International Airport, and web server audits.[1]

We separated the results of our evaluation into seven FISMA areas. For each area, we identified the progress that DHS has made since our FY 2008 evaluation and those 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 2009 DHS Information Security Performance Plan "Maintaining Excellence"* to enhance its information security program, and to make continuous improvements on all existing processes. In addition, the CISO refined its FISMA scorecard metrics to better evaluate components' compliance with the performance plan. See Appendix C and D for examples of the FISMA scorecard.
- 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, such as assessing the effectiveness of controls implemented on information systems, and incorporating security into system life cycles.

[1] *Technical Security Evaluation of DHS Activities at Los Angeles International Airport* (OIG-09-01, October 2008), *Better Monitoring and Enhanced Technical Controls Are Needed to Effectively Manage LAN-A* (OIG-09-55, April 2009)*, Improved Management and Stronger Leadership Are Essential to Complete the OneNet Implementation* (OIG-09-98, September 2009), and *Vulnerabilities Highlight the Need for More Effective Web Security Management* (OIG-09-101, September 2009).

- DHS continues to maintain an effective process in updating and managing an inventory of its agency and contractor systems on an annual basis. In addition, DHS updated its *FISMA System Inventory* methodology to identify the Chief Financial Officer designated systems.
- The CISO implemented more stringent criteria when reviewing the artifacts contained in accreditation packages. Once all the artifacts are approved by the component CISO, DHS reviews the entire accreditation package for consistency and completeness.
- DHS improved on its Vulnerability Assessment Program as the DHS Security Operations Center (SOC) now has full visibility at Customs and Border Protection (CBP), Citizenship and Immigration Services (CIS), Federal Law Enforcement Training Center (FLETC), Management Directorate (Management), National Protection and Programs Directorate (NPPD), Science and Technology (S&T), and Transportation Security Administration (TSA).
- The CISO has taken actions to evaluate classified POA&Ms maintained at the Federal Emergency Management Agency (FEMA), Transportation Security Administration (TSA), and United States Coast Guard (USCG).
- DHS documented the deviations from the Federal Desktop Core Configuration (FDCC) settings and components have taken steps to implement the settings on Windows XP and Vista desktops and laptops. Our testing results confirmed that FLETC had implemented FDCC settings on its Windows XP workstations.

## **OVERALL ISSUES TO BE ADDRESSED**

Despite the progress made to the department's overall information security program, components are still not executing fully the department's policies, procedures, and practices. For example, our review of DHS FISMA scorecards for the period June 2007 through July 2009 revealed that components do not sustain their information security programs on a year round basis or do not perform continuous monitoring to maintain system accreditations and POA&Ms. For example:

- Components' overall scores drop considerably following July (FISMA reporting cut-off) and do not show any significant progress until the months leading up to the subsequent annual FISMA reporting. Furthermore, scores remain below the minimum performance target (80%) for the majority of the year. Components are reaching outstanding performance levels (green) only at the time of FISMA reporting. See Figure 1.[2]

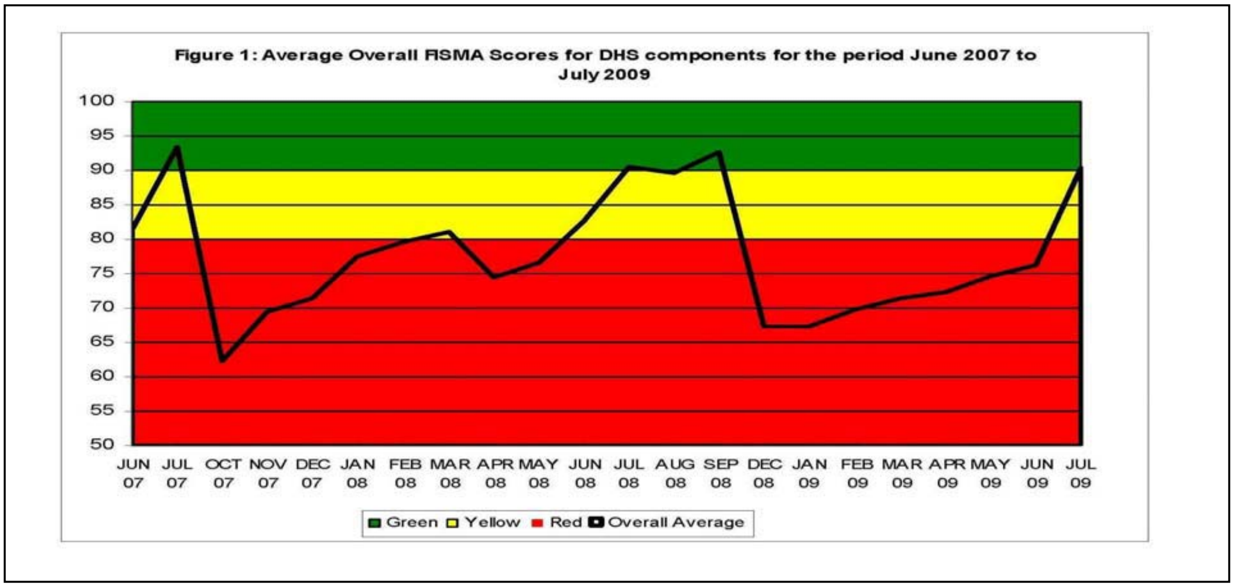


Figure 1: Average Overall FISMA Scores for DHS components for the period June 2007 to July 2009

- To evaluate the effectiveness of components' continuous monitoring program, we selected two significant metrics from DHS scorecards: C&A and POA&Ms quality. As depicted in Figure 2, the scores for both metrics peak in the months of annual FISMA reporting (around July) and quickly drop in subsequent months.[3] As such, systems' C&A packages and POA&Ms are not being updated as required by the components.[4] See Appendix C for June and July 2009 DHS scorecards and Appendix D for June and July 2008.

[2] DHS could not provide the scorecards for the months of August 2007, September 2007, October 2008, and November 2008.

[3] DHS could not provide the scorecards for the months of October and November 2008.

[4] In accordance with NIST 800-37, "continuous monitoring" is the fourth phase of the C&A process (i.e., after the information system has been certified and accredited). OMB noted in its FY09 FISMA reporting instructions that "Continuous monitoring of security controls is a cost-effective and important part of managing enterprise risk and maintaining an accurate understanding of the security risks confronting agency's information systems. Continuous monitoring of security controls is required as part of the security C&A process to ensure controls remain effective over time (e.g., after the initial authorization or reauthorization of an information system). A robust and effective continuous monitoring program will ensure important procedures included in an agency's accreditation package (e.g., as described in system security plans, security assessment reports, and POAMs) 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.

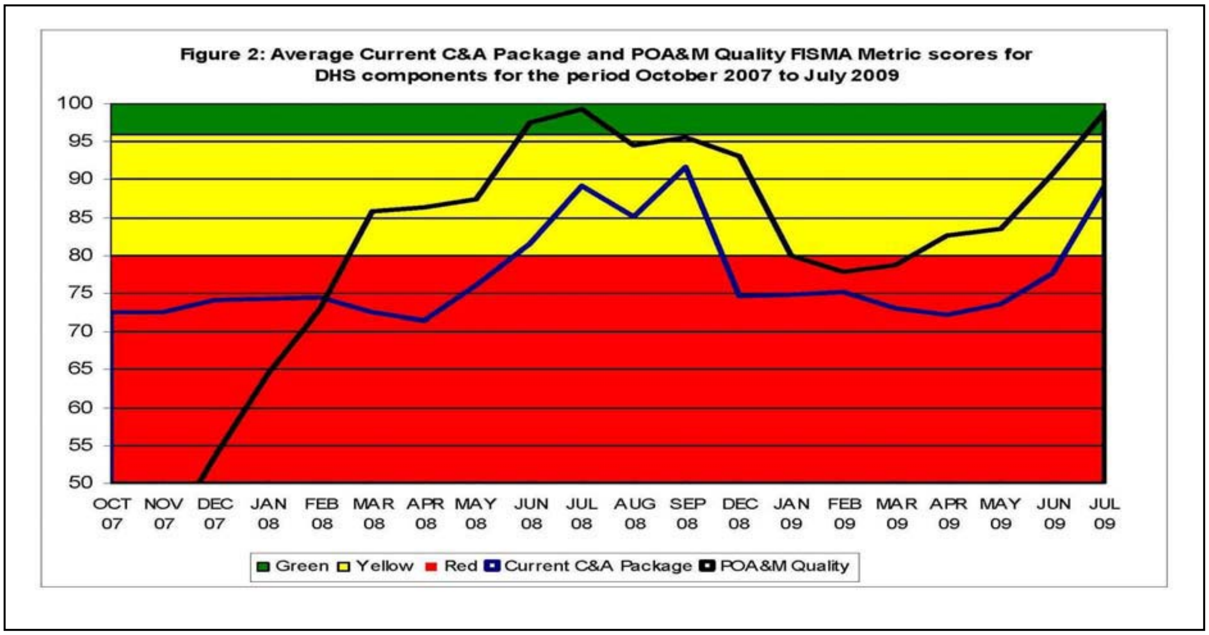


Figure 2: Average Current C&A Package and POA&M Quality FISMA Metric scores for DHS components for the period October 2007 to July 2009

In addition:

- Artifacts supporting the component systems C&A were missing key information to allow the 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 fully implemented DHS' baseline configuration settings.
- Components are not consistently maintaining and tracking their classified POA&Ms.
- Appropriate training is needed for all individuals with significant security responsibilities.
- An escalation process is needed for privacy impact assessments (PIA) that have been in the review and approval process for more than six months.

## System Inventory

DHS maintains an effective process to update and manage its systems inventory on an annual basis, including agency and contractor systems. In addition, DHS conducts site visits to identify systems that were not included in the department's annual inventory update process.

PROGRESS

- DHS continues to maintain a comprehensive inventory of its major applications and general support systems, including contractor systems. In addition, DHS updated its *FISMA System Inventory* methodology to identify the Chief Financial Officer designated systems. As of July 31, 2009, DHS identified 579 operational systems.

ISSUES TO BE ADDRESSED

- We noted that a high percentage of systems are reported by components as "under development" in DHS' enterprise management tool. As of June 30, 2009, components reported that 57 general support systems and 130 major applications are "under development." This represents 32% of DHS operational systems and may indicate that components are not accurately reporting the life cycle status of their systems to the department.
- While CBP's classified laptop system is operational, the component reported it as "under development" in DHS' enterprise management tool. CBP personnel indicated that they reported the system as "under development" because the accreditation package was classified as "secret" and could not be uploaded into DHS' enterprise management tool.
- The results of our web server audit revealed that "cbp.gov" has not been included in DHS' system inventory.[5]

See Appendices E and F for system inventory and evaluation of DHS' oversight of contractor systems and quality of system inventory.

## Certification and Accreditation Process

DHS follows the C&A process outlined in NIST Special Publication (SP) 800-37 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 C&A process requires documentation, such as system security plans, risk assessments, system test and evaluation plans, security assessment

[5] *Vulnerabilities Highlight the Need for More Effective Web Security Management* (OIG-09-101, September 2009).

reports, contingency plans, contingency plan test results, and self-assessments.

For some of the systems that have been accredited by the components, the artifacts that are required to C&A a system were either missing or incomplete. In addition, some of the self-assessments were not being properly completed by the components. We identified a similar issue in our FY 2008 FISMA report.[6]

PROGRESS

- DHS requires components to upload 11 C&A artifacts into its enterprise management tool to monitor the progress in accrediting systems. The 11 artifacts are: Authority to Operate (ATO) letter, system security plan, security assessment report, risk assessment, security test and evaluation, contingency plan, contingency plan test results, Federal Information Processing Standards (FIPS) 199 determination, E-authentication determination, privacy threshold analysis (PTA)/privacy impact assessment (PIA), and NIST SP 800-53 self-assessment.
- As of July 31, 2009, the CISO reported that 93 percent of DHS' operational systems (540/579) have been certified and accredited.
- The quality of C&A packages has improved in FY 2009, when compared to FY 2008. Specifically, we identified fewer instances where the required information was missing from security documents.

ISSUES TO BE ADDRESSED

- We selected 35 systems from 12 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 C&A a system were either missing or incomplete. Without this information, agency officials cannot make credible, risk-based decisions on whether to authorize the system to operate. Specifically:

[6] *Evaluation of DHS' Information Security Program for Fiscal Year 2008* (OIG-08-94, September 2008).

    - ➢ We identified eight instances where the FIPS-199 determination was not completed and four instances where FIPS-199 determination was outdated. The FIPS-199 determination, when applied properly during the risk assessment process, helps agency officials to select applicable controls for the information systems.
    - ➢ Twenty-five instances were identified where system security plans were missing sections that describe detailed emergency configuration changes, management plans, security controls, and incident handling procedures. In addition, we noted four instances where the system security plans were outdated. The system security plan should be current, providing an overview of the information system, and describing the security controls implemented or planned to protect the system.
    - ➢ We identified seventeen instances where contingency plans were incomplete, missing the identification of alternate processing facilities or restoration procedures. Four of the contingency plans were more than three years old. An updated contingency plan can help agency officials to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.
    - ➢ The contingency plans for two "high availability" systems had not been tested because the alternate processing facilities were not operational. Contingency plan testing identifies planning gaps and is also a training exercise to prepare recovery personnel for plan activation, which can improve plan effectiveness and overall agency preparedness. Untested plans may create a false sense of ability to recover operations in a timely manner.

- As part of the C&A review, we also evaluated the quality of completed NIST SP 800-53 self-assessments. For example, we evaluated whether the components provided support for all applicable controls as to how they were implemented. In addition, we assessed whether supporting documentation existed for all controls that were reported as "tested." Finally, we evaluated the adequacy of the justifications for any controls that were reported as "not applicable," and whether a POA&M was created for all required controls that had not been tested. Specifically:

    - ➢ We identified eighteen instances where controls, required by DHS and NIST, were missing from the self-assessments.

- ➢ We noted fifteen instances where required controls were not tested; did not include validation and verification testing; or were missing documentation to support that testing was performed. Examples of these instances were found in the areas of access control, configuration management, contingency planning, and risk assessment.

- We reported in April 2009 that the LAN-A system was certified and accredited without the required security documents.[7]

See Appendix H for our assessment of DHS' C&A process.

## **Plan of Action and Milestones Process**

DHS requires components to create and maintain POA&Ms for all known IT security weaknesses. DHS performs automated reviews on POA&Ms for accuracy and completeness and the results are provided to components on a daily basis. Despite these efforts, components are not entering and tracking all IT security weaknesses in DHS' enterprise management tool, nor is all of the data entered by the components accurate and updated in a timely manner. We identified a similar issue in our FY 2008 FISMA report.

### PROGRESS

- DHS had taken actions to evaluate classified POA&Ms maintained at FEMA, TSA, and USCG.
- Components have created POA&Ms for 135 of 140 (96%) notice of findings and recommendations (NFRs) for the weaknesses identified during the FY 2008 financial statement audit.
- Components have prioritized all unclassified POA&Ms in DHS' enterprise management tool.

### 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.

[7] *Better Monitoring and Enhanced Technical Controls Are Needed to Effectively Manage LAN-A* (OIG-09-55, April 2009).

- 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, 2009, only 320 out of 365 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 and Information Systems Security Officer (ISSOs) are responsible for ensuring that POA&M information is entered accurately and that weaknesses are mitigated timely. Component personnel cited a lack of time and staff as the explanation that their POA&Ms are not being updated regularly. For example,

    - ➢ Three components (CBP, Management, and TSA) did not create POA&Ms for findings identified in OIG audit reports issued during FY 2009.
    - ➢ Although six components (CBP, FEMA, ICE, NPPD, TSA, and USCG) followed a manual process for maintaining classified POA&Ms, not all components identified the source of the weaknesses or include the creation date, estimated completion dates, and the actual completion of the POA&Ms. In addition, there is no evidence of periodic updates, component CISO reviews, or that these weaknesses were properly prioritized.
    - ➢ Components are not creating POA&Ms for the weaknesses identified during the C&A process or from the NIST SP 800-53 self-assessments. As part of our C&A quality review, we evaluated whether POA&Ms had been created for any weakness that was identified during the C&A process, or from the NIST SP 800-53 self-assessment when controls had not been tested and where risks were not accepted. In 17 instances, POA&Ms were not created for the weaknesses identified during the C&A process.

- Based on an analysis of data in DHS' enterprise management tool, as of June 30, 2009, component CISOs and ISSOs 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 management is not updating all weaknesses where the estimated completion date has been delayed. Of the 3,918 open POA&Ms with estimated completion dates, 837 (21%) were delayed by at least 3 months (prior to April 1, 2009). Furthermore, 563 POA&Ms had an estimated completion date over one year old, dating as far back as December 31, 2005. In addition, completion dates for 226 of the 563 POA&Ms have not been updated since March 2006.
- Resources required for the remediation of 298 (8%) of the 3,918 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.
- 238 (6%) of 3,918 open POA&Ms are scheduled to take more than 2 years to mitigate the weaknesses.

- Based on our samples of the vulnerability assessment results performed by DHS SOC, CIS had not created POA&Ms for the high risk vulnerabilities that could not be mitigated timely.

See Appendix G for the evaluation of DHS' POA&M process.

## Configuration Management

To evaluate components' compliance with DHS baseline configuration requirements, we determined whether required configuration settings had been implemented on the 50 systems selected for our C&A and configuration management reviews. For the systems selected for the C&A review, we performed testing to determine whether DHS baseline configuration settings were implemented on selected servers. For the systems selected for our configuration assessment, we verified whether NIST SP 800-53 controls and DHS baseline configuration settings were implemented on selected servers. Our review also includes the results of a limited number of systems evaluated during the year, such as the LAN-A, OneNet, Los Angeles International Airport, and web server audits. Results revealed that the components have not implemented all of the required DHS baseline configuration settings. We reported a similar issue in our FY2008 FISMA report.

PROGRESS

- DHS documented the deviations from FDCC settings. In addition, components are in various stages of implementing the settings on their Windows XP and Vista desktops and laptops. Components are scheduled to complete the implementation by FY2011. Our testing results confirmed that FLETC had implemented FDCC settings on its Windows XP desktops and laptops.
- DHS updated the baseline configuration guidelines for Oracle database, Windows XP, Windows 2003 Server, Windows 2008 Server, and Windows Vista.

ISSUES TO BE ADDRESSED

- Components indicated that automated tools are needed to ensure that DHS baseline configuration settings are implemented consistently and more efficiently throughout the department.
- DHS has not implemented the FDCC requirements, as outlined in OMB Memorandums M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, March 22, 2007, and M-07-18, *Ensuring New Acquisitions Include Common Security Configurations*, June 1, 2007. For example, DHS has not incorporated the standard FDCC contract language into all IT acquisitions. CBP, CIS, FLETC, ICE and TSA have not incorporated the standard language into their IT contracts.
- The majority of components, including Management, have yet to implement FDCC security settings.
- Components have not implemented DHS baseline configuration settings on the systems reviewed. Specifically:
    - ➢ Results from our C&A and configuration reviews indicated that DHS' baseline configuration settings have not been implemented on the systems. For example, components have not implemented warning banners, enforced password complexities, or enabled audit trail policies.
    - ➢ Vulnerability assessments performed at components during our LAN-A, OneNet, Los Angeles International Airport, and web server audits identified security concerns with access control, identification and authentication, and configuration management. In these instances, components had not configured their systems based on DHS' configuration

guidelines. Components included CBP, CIS, FEMA, ICE, Management, NPPD, TSA, USCG, and USSS.[8]

- Weak internal IT controls related to financial management systems were found during the audit of the department's consolidated financial statements for FY 2008.[9] Security concerns included inadequate access controls, application controls, software development, and change controls.

See Appendix J for information regarding DHS' configuration management.

## Incident Detection, Handling, and Analysis Procedures

DHS has established adequate incident detection, handling, and analysis procedures, but has not fully implemented its vulnerability assessment program across the department.

PROGRESS

- DHS continues to implement its Vulnerability Assessment Program as the DHS SOC has full visibility to perform scans on workstations and servers at CBP, CIS, DHS HQ, FLETC, and TSA.

ISSUES TO BE ADDRESSED

- FLETC, NPPD, OIG, and S&T did not submit weekly incident reports to the DHS SOC, as required. Furthermore, the DHS SOC does not follow-up with these components to obtain the missing reports.
- 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 and ICE, and cannot perform vulnerability

[8] *Technical Security Evaluation of DHS Activities at Los Angeles International Airport* (OIG-09-01, October 2008), *Better Monitoring and Enhanced Technical Controls Are Needed to Effectively Manage LAN-A* (OIG-09-55, April 2009)*, Improved Management and Stronger Leadership Are Essential to Complete the OneNet Implementation* (OIG-09-98, September 2009), and *Vulnerabilities Highlight the Need for More Effective Web Security Management* (OIG-09-101, September 2009).

[9] *Information Technology Management Letter for the FY 2008 DHS Financial Statement Audit* (OIG-09-50, April 2009).

assessments on their workstations and servers. Finally, the DHS SOC has no access at OIG, USCG, and USSS.

See Appendix K for information regarding DHS' incident reporting.

## Security Training

DHS validates components' employee security training. The department's Information Security Training, Education, and Awareness Office (Training Office) has not developed a specific training program for employees with significant security responsibilities.

PROGRESS

- The Training Office has initiated a process requiring components to identify all personnel with significant IT security-related responsibilities.

ISSUES TO BE ADDRESSED

- The Training Office has not identified appropriate, specialized security training for employees and contractors with significant IT security responsibilities. We reported a similar issue in our FY2006, FY2007, and FY2008 FISMA reports.[10]
- DHS contractors do not have access to *DHScovery* or the standardized security awareness training offered by the system.

See Appendix L for information regarding DHS' security awareness training.

## Privacy

The Privacy Office continues to refine its PIA guidance. However, the Privacy Office continues to experience delays in reviewing and approving PIAs submitted by the components and has not implemented all requirements specified in OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007. We reported a similar issue in our FY2008 FISMA report.

[10] *Evaluation of DHS' Information Security Program for Fiscal Year 2006* (OIG-06-62, September 2006), *Evaluation of DHS' Information Security Program for Fiscal Year 2007* (OIG-07-77, September 2007), and *Evaluation of DHS' Information Security Program for Fiscal Year 2008* (OIG-08-94, September 2008).

PROGRESS

- The Privacy Office has issued new policies since our last review. For example, the Privacy Office issued:
    - *Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS* to provide step by step instructions on how to protect personal information.
    - *DHS Policy Regarding Privacy Impact Assessments Memorandum* to set forth the Privacy Officer's requirements to perform the privacy assessments.
    - *DHS Policy Regarding Fair Information Practice Principles* to reiterate that the Fair Information Practice Principles as the foundational principles for DHS' privacy policy.
    - *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons* to set forth the policy to protect the privacy information of non-U.S. persons collected, used, retained, and/or disseminated by the department.

ISSUES TO BE ADDRESSED

- DHS has not implemented all of the requirements outlined in OMB M-07-16. Specifically, DHS has not defined the consequences for users who do not comply with the policy. The Privacy Office is working in conjunction with the Office of General Counsel and the Chief Human Capital Office to develop the consequences of non-compliance policy.
- DHS' Privacy Office is experiencing delays in reviewing and approving PIAs. As of June 15, 2009, there were 99 PIAs in various stages of review; the PIAs for 3 operational systems had been outstanding for more than 230 days.

See Appendix I for DHS' Privacy Program and Privacy Impact Assessment Process.

## Recommendations

We recommend that the DHS Chief Information Officer:

**Recommendation #1**: Improve the ISO's review process to ensure that all POA&Ms, including those POA&Ms for classified systems, are complete, accurate, and current. Specifically, components must correct the POA&M deficiencies identified by the ISO review.

**Recommendation #2**: Ensure that all applicable controls are included in the security document when certifying and accrediting systems. Systems accredited with outdated documents or without all applicable controls should not be accepted.

**Recommendation #3**: 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 to ensure that DHS baseline configuration settings are implemented.

**Recommendation #4**: Expedite the implementation of a department-wide vulnerability assessment program to perform periodic testing to evaluate the security posture at all components. POA&Ms should be created for any high risk vulnerabilities that can not be mitigated timely.

**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.

We recommend that the DHS Chief Privacy Officer:

**Recommendation #7:** Establish an escalation process for any PIAs that have been in the review and approval process for an extended period of time.

**Recommendation #8:** Define the consequences of non-compliance by system users, in accordance with the requirements outlined in OMB M-07-16.

## Management Comments and OIG Analysis

DHS concurred with recommendation 1. DHS has taken actions to improve the ISO review process to ensure that all POA&Ms, including those POA&Ms for classified systems, are complete, accurate, and current. Improvements include the implementation of automated POA&M quality review checks performed daily and conducting reviews of POA&Ms to ensure that results from Annual Assessments, Information Technology Acquisition Reviews, and Enterprise Architecture Center of Excellence Reviews and OMB A-123 reviews are included.

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

DHS concurred with recommendation 2. The certification and accreditation (C&A) document templates and applicable controls are generated 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 to ensure that all applicable controls are adequately addressed. The document review team has been instructed not to accept any outdated templates or documents without applicable controls in place.

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

DHS concurred with recommendation 3. Components are required to validate 10% of their systems quarterly to ensure configuration requirements are being implemented and maintained. Additionally, the DHS FY10 Information Security Scorecard will show configuration management status based on component quarterly updates. DHS plans to complete periodic reviews of the component's process to ensure the validation is thorough and complete as part of our program review. The department also continues to research potential enterprise-level tools to support configuration management.

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

DHS concurred with recommendation 4. The DHS SOC is responsible for implementing the department-wide Vulnerability Assessment Tracking (VAT) Program. The DHS SOC has vulnerability assessment scanning capabilities within DHS Headquarters and has deployed distributed scanning servers within most of the components. Implementation of the scanners at the remaining components is in progress. The DHS VAT Program requires at least one annual baseline scan of 100% of DHS systems. POA&Ms are required to be created for any high risk vulnerabilities identified that can not be mitigated timely.

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved and will remain open until DHS provides documentation to support that all planned corrective actions are completed.
DHS concurred with recommendation 5. DHS has begun to develop a role-based training package for component CIO's implementation to ensure the required security training of individuals with significant security responsibilities. The department performs training for individuals with significant security responsibilities as part of agency-wide and component sponsored security conferences and workshops. Additionally, several components have established their own role-based training for personnel with significant security responsibilities and invite other components to participate.

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

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. DHS has published the revised DHS Hardening Guide to incorporate the FDCC requirements for Windows XP and Vista.

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

DHS concurred with recommendation 7. The Privacy Office is refining its escalation policy for addressing concerns with outstanding privacy compliance documentation. Once the Chief Privacy Officer approves that policy it will be distributed to the Component Privacy Officers and privacy points of contact. The Privacy Office anticipates the publication of the policy prior to the end of the calendar year. Additionally, the Privacy Office has increased the amount of component specific training being conducted in an effort to shorten the amount of time required for a PIA to be completed.

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

DHS concurred with recommendation 8. The Chief Privacy Officer satisfied her part of the requirement outlined in OMS M-07-l6 by issuing the Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS on October 31, 2008. A memo to all employees was sent in December 2008 with a link to the rules. These are considered the "rules" associated with the requirement for "rules and consequences."

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved and will remain open until the consequences of non-compliance policy, which the Privacy Office is working on in conjunction with the Office of General Counsel and the Chief Human Capital Office to develop, is finalized.

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 and practices, based on the requirements outlined in FISMA and, using OMB Memorandum M-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, issued on August 20, 2009. We conducted our work at the program level and at DHS' major components: CBP, CIS, FEMA, FLETC, ICE, Management, NPPD, OIG, S&T, TSA, USCG, and USSS.

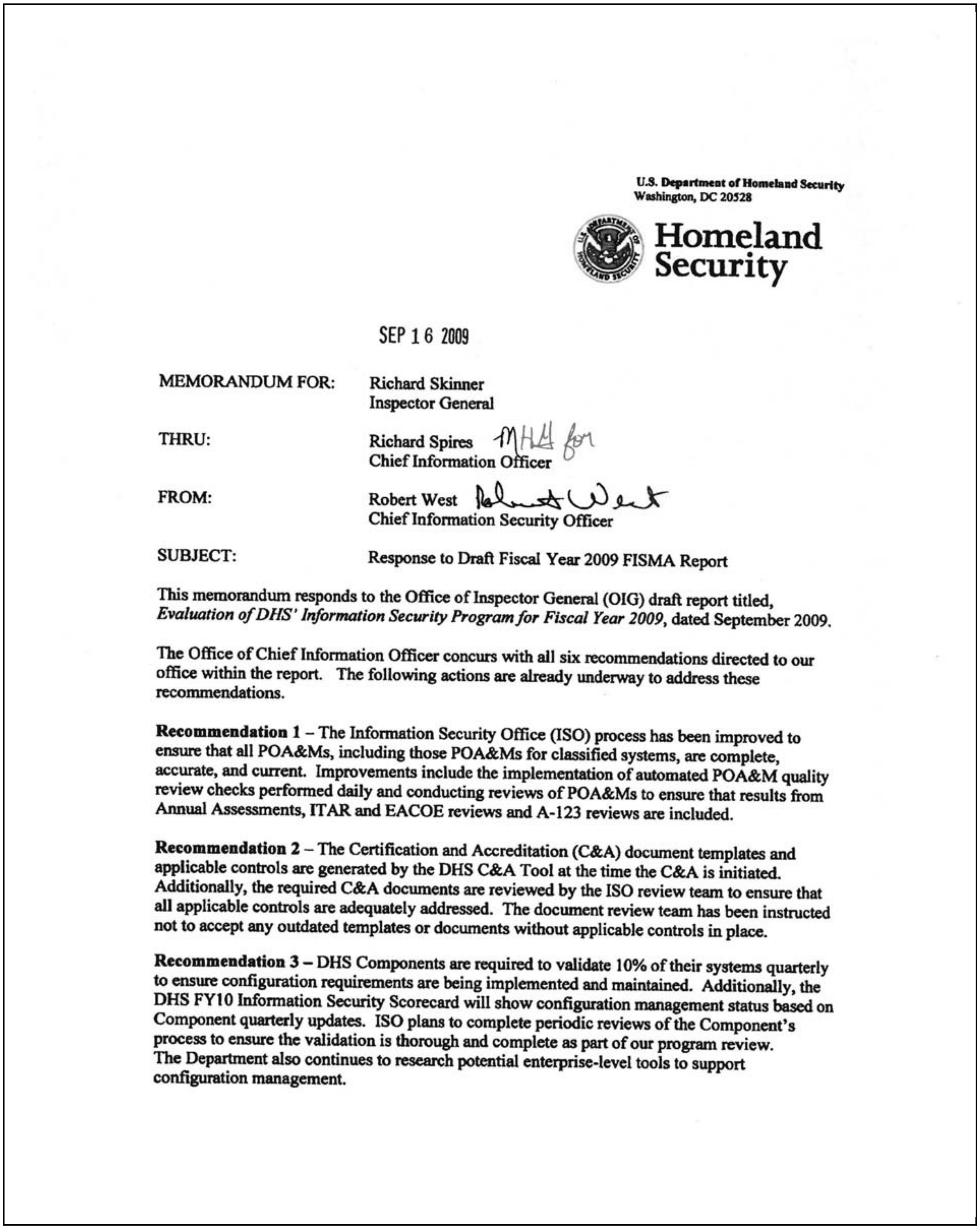
In addition to our independent evaluation, we conducted reviews of DHS' information systems and security program-related areas throughout FY 2009. This report includes the results of a limited number of systems evaluated during the year and our on-going financial statement review, including the LAN-A, OneNet, Los Angeles International Airport, and Web server audits.

As part of our evaluation of DHS' compliance with FISMA, we assessed DHS and its components' compliance with the security requirements mandated by FISMA and other federal information systems' security policies, procedures, standards, and guidelines including NIST SP 800-37, and FIPS-199. Specifically, we: (1) used last year's FISMA independent evaluation as a baseline for this year's review and assessed the progress that DHS has made in resolving weaknesses previously identified; (2) focused on reviewing DHS' POA&M process to ensure that all security weaknesses are identified, tracked, and addressed; (3) reviewed policies, procedures, and practices that DHS has implemented at the program level and at the component level; (4) evaluated processes (i.e., system inventory, C&A, security training, and incident response that DHS has implemented as part of its agency-wide information security program); and, (5) developed our independent evaluation of DHS' information security program.

We reviewed the quality of C&A packages for a sample of 35 systems at 12 components and offices: CBP, CIS, FEMA, FLETC, ICE, Management, NPPD, OIG, 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 20 systems at CBP, CIS, FEMA, FLETC, ICE, Management, NPPD, S&T, TSA, USCG, and USSS.

We conducted our evaluation between April and August 2009 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 L.

The principal OIG points of contact for the evaluation are Frank Deffer, Assistant Inspector General, Office of Information Technology at (202) 254-4100 and Edward G. Coleman, Director, Information Security Audit Division at (202) 254-5444.



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

Homeland
Security

SEP 16 2009

MEMORANDUM FOR: Richard Skinner
Inspector General

THRU: Richard Spires MHH for
Chief Information Officer

FROM: Robert West Robert West
Chief Information Security Officer

SUBJECT: Response to Draft Fiscal Year 2009 FISMA Report

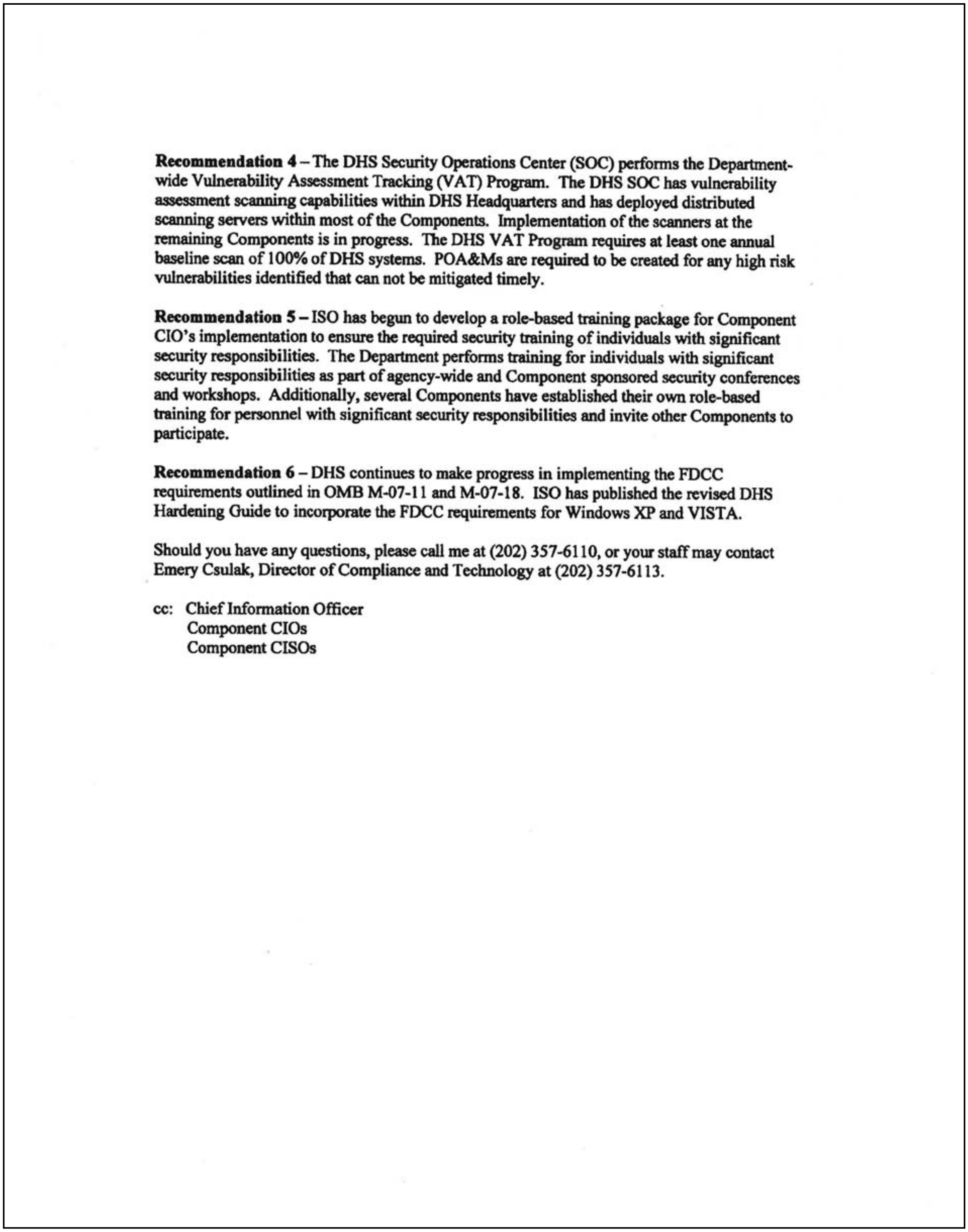
This memorandum responds to the Office of Inspector General (OIG) draft report titled, *Evaluation of DHS' Information Security Program for Fiscal Year 2009*, dated September 2009.

The Office of Chief Information Officer concurs with all six recommendations directed to our office within the report. The following actions are already underway to address these recommendations.

**Recommendation 1** – The Information Security Office (ISO) process has been improved to ensure that all POA&Ms, including those POA&Ms for classified systems, are complete, accurate, and current. Improvements include the implementation of automated POA&M quality review checks performed daily and conducting reviews of POA&Ms to ensure that results from Annual Assessments, ITAR and EACOE reviews and A-123 reviews are included.

**Recommendation 2** – The Certification and Accreditation (C&A) document templates and applicable controls are generated 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 review team to ensure that all applicable controls are adequately addressed. The document review team has been instructed not to accept any outdated templates or documents without applicable controls in place.

**Recommendation 3 –** DHS Components are required to validate 10% of their systems quarterly to ensure configuration requirements are being implemented and maintained. Additionally, the DHS FY10 Information Security Scorecard will show configuration management status based on Component quarterly updates. ISO plans to complete periodic reviews of the Component's process to ensure the validation is thorough and complete as part of our program review. The Department also continues to research potential enterprise-level tools to support configuration management.



**Recommendation 4** – The DHS Security Operations Center (SOC) performs the Department-wide Vulnerability Assessment Tracking (VAT) Program. The DHS SOC has vulnerability assessment scanning capabilities within DHS Headquarters and has deployed distributed scanning servers within most of the Components. Implementation of the scanners at the remaining Components is in progress. The DHS VAT Program requires at least one annual baseline scan of 100% of DHS systems. POA&Ms are required to be created for any high risk vulnerabilities identified that can not be mitigated timely.

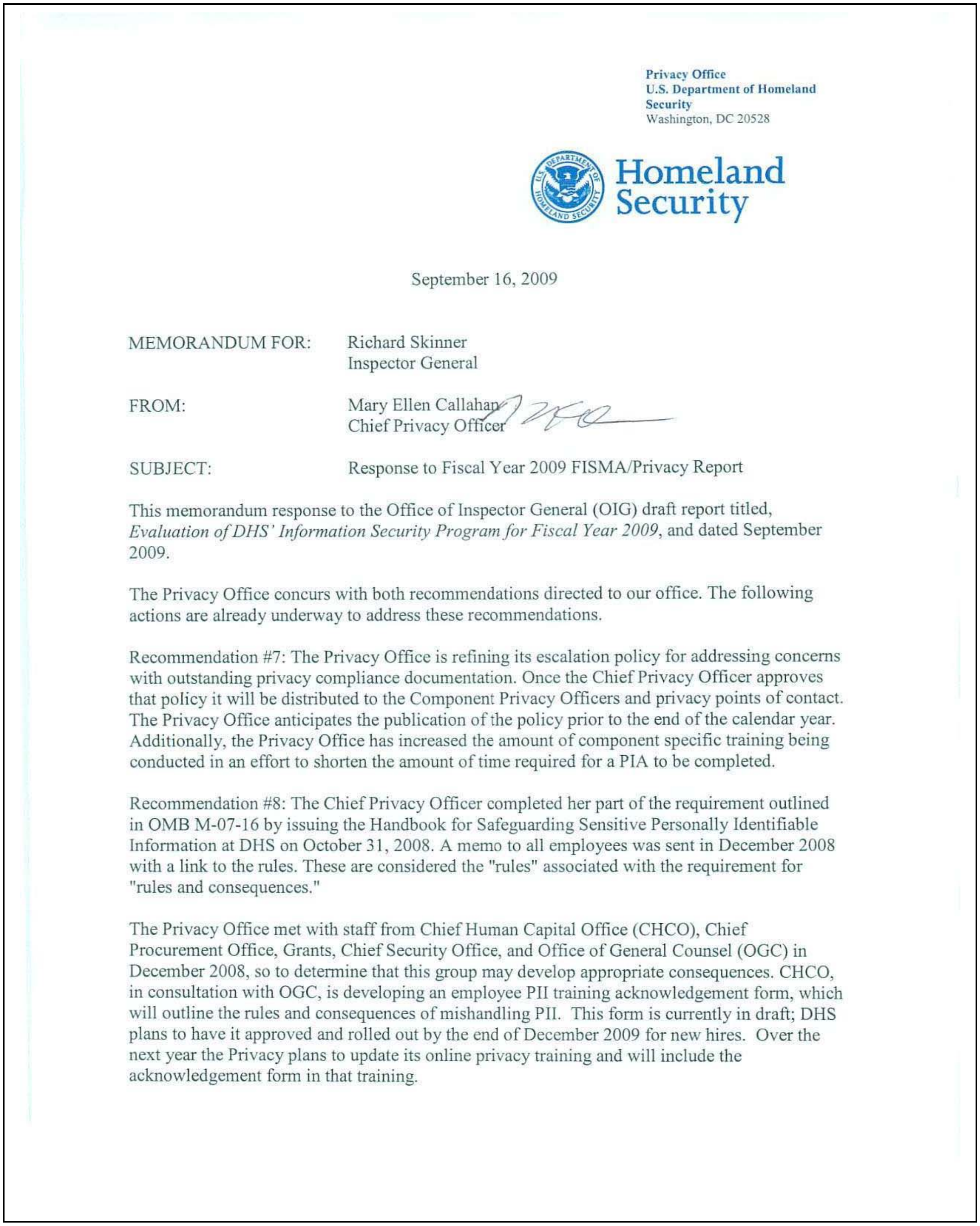
**Recommendation 5** – ISO has begun to develop a role-based training package for Component CIO's implementation to ensure the required security training of individuals with significant security responsibilities. The Department performs training for individuals with significant security responsibilities as part of agency-wide and Component sponsored security conferences and workshops. Additionally, several Components have established their own role-based training for personnel with significant security responsibilities and invite other Components to participate.

**Recommendation 6** – DHS continues to make progress in implementing the FDCC requirements outlined in OMB M-07-11 and M-07-18. ISO has published the revised DHS Hardening Guide to incorporate the FDCC requirements for Windows XP and VISTA.

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

# Appendix B
# Management Response to Draft Report



**Privacy Office**
**U.S. Department of Homeland Security**
Washington, DC 20528

Homeland Security

September 16, 2009

MEMORANDUM FOR: Richard Skinner
Inspector General

FROM: Mary Ellen Callahan
Chief Privacy Officer

SUBJECT: Response to Fiscal Year 2009 FISMA/Privacy Report

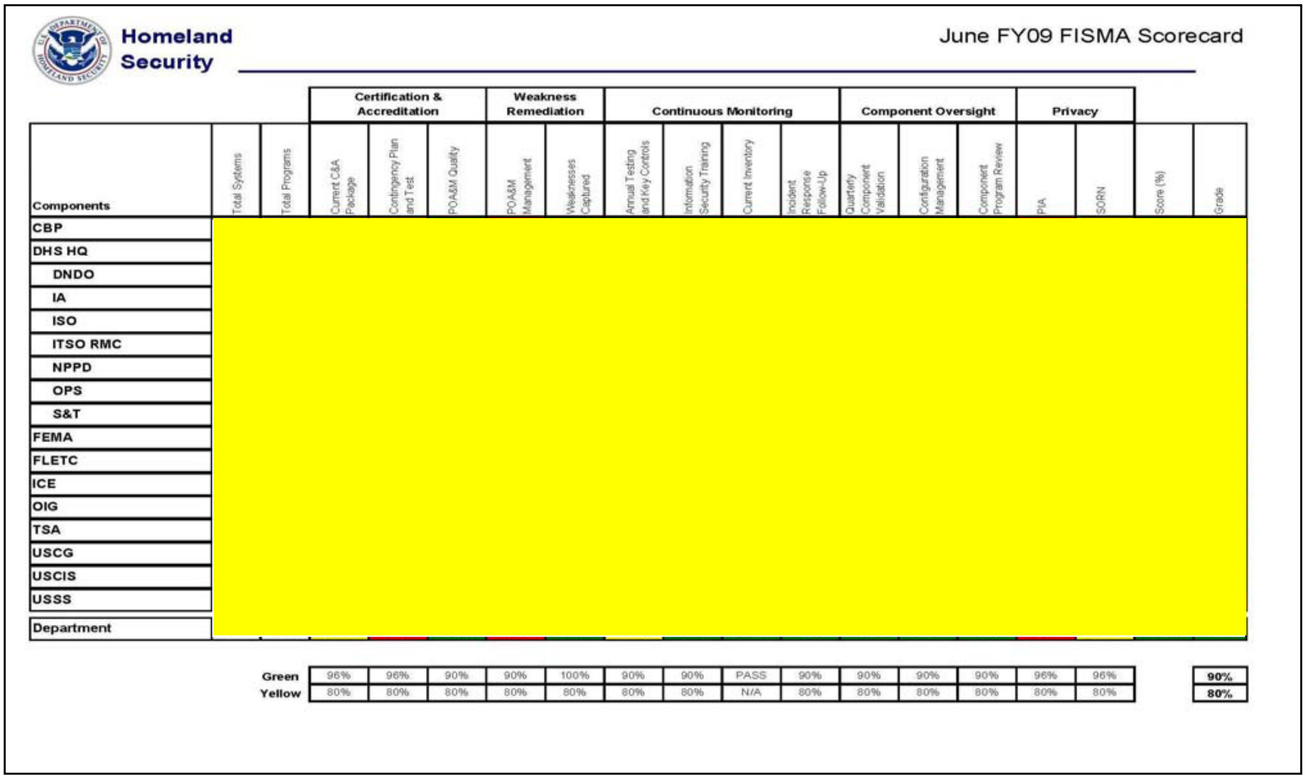
This memorandum response to the Office of Inspector General (OIG) draft report titled, *Evaluation of DHS' Information Security Program for Fiscal Year 2009*, and dated September 2009.

The Privacy Office concurs with both recommendations directed to our office. The following actions are already underway to address these recommendations.

Recommendation #7: The Privacy Office is refining its escalation policy for addressing concerns with outstanding privacy compliance documentation. Once the Chief Privacy Officer approves that policy it will be distributed to the Component Privacy Officers and privacy points of contact. The Privacy Office anticipates the publication of the policy prior to the end of the calendar year. Additionally, the Privacy Office has increased the amount of component specific training being conducted in an effort to shorten the amount of time required for a PIA to be completed.

Recommendation #8: The Chief Privacy Officer completed her part of the requirement outlined in OMB M-07-16 by issuing the Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS on October 31, 2008. A memo to all employees was sent in December 2008 with a link to the rules. These are considered the "rules" associated with the requirement for "rules and consequences."

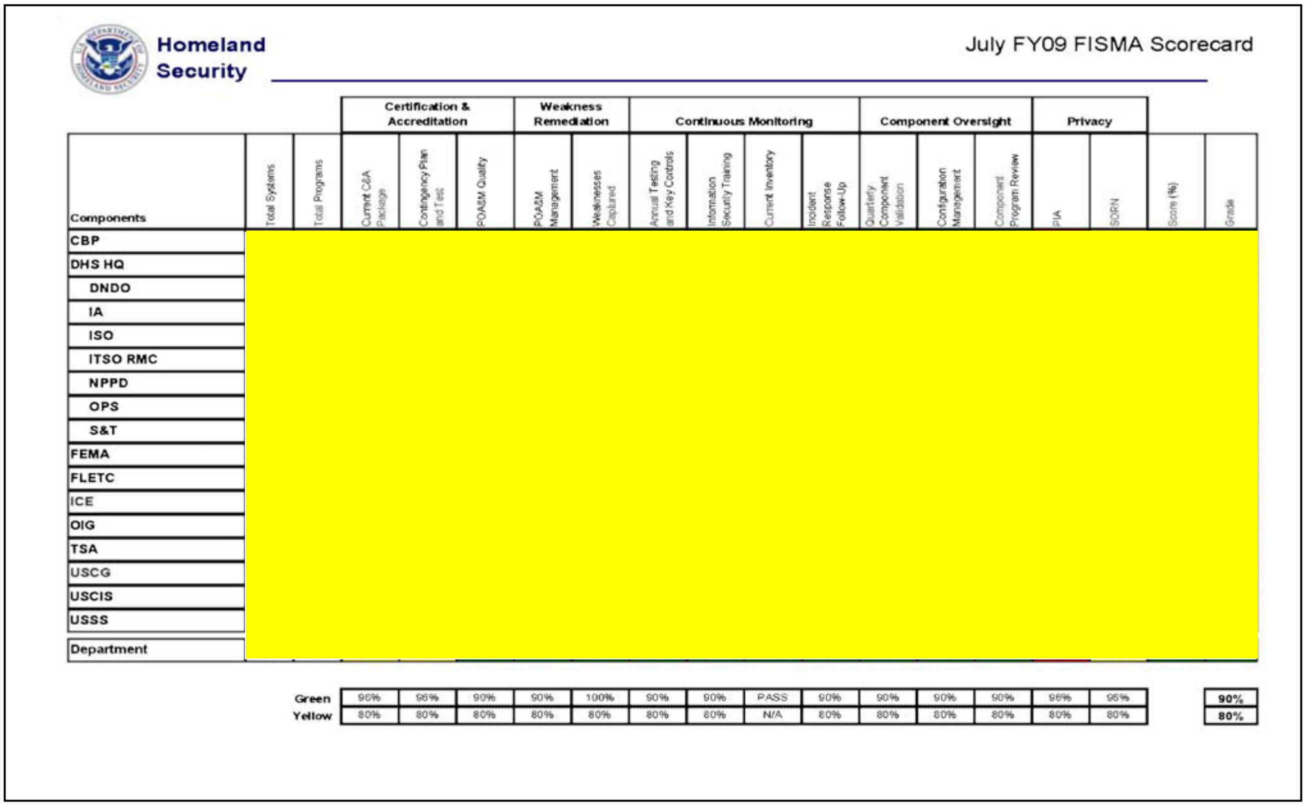
The Privacy Office met with staff from Chief Human Capital Office (CHCO), Chief Procurement Office, Grants, Chief Security Office, and Office of General Counsel (OGC) in December 2008, so to determine that this group may develop appropriate consequences. CHCO, in consultation with OGC, is developing an employee PII training acknowledgement form, which will outline the rules and consequences of mishandling PII. This form is currently in draft; DHS plans to have it approved and rolled out by the end of December 2009 for new hires. Over the next year the Privacy plans to update its online privacy training and will include the acknowledgement form in that training.



Homeland Security

June FY09 FISMA Scorecard

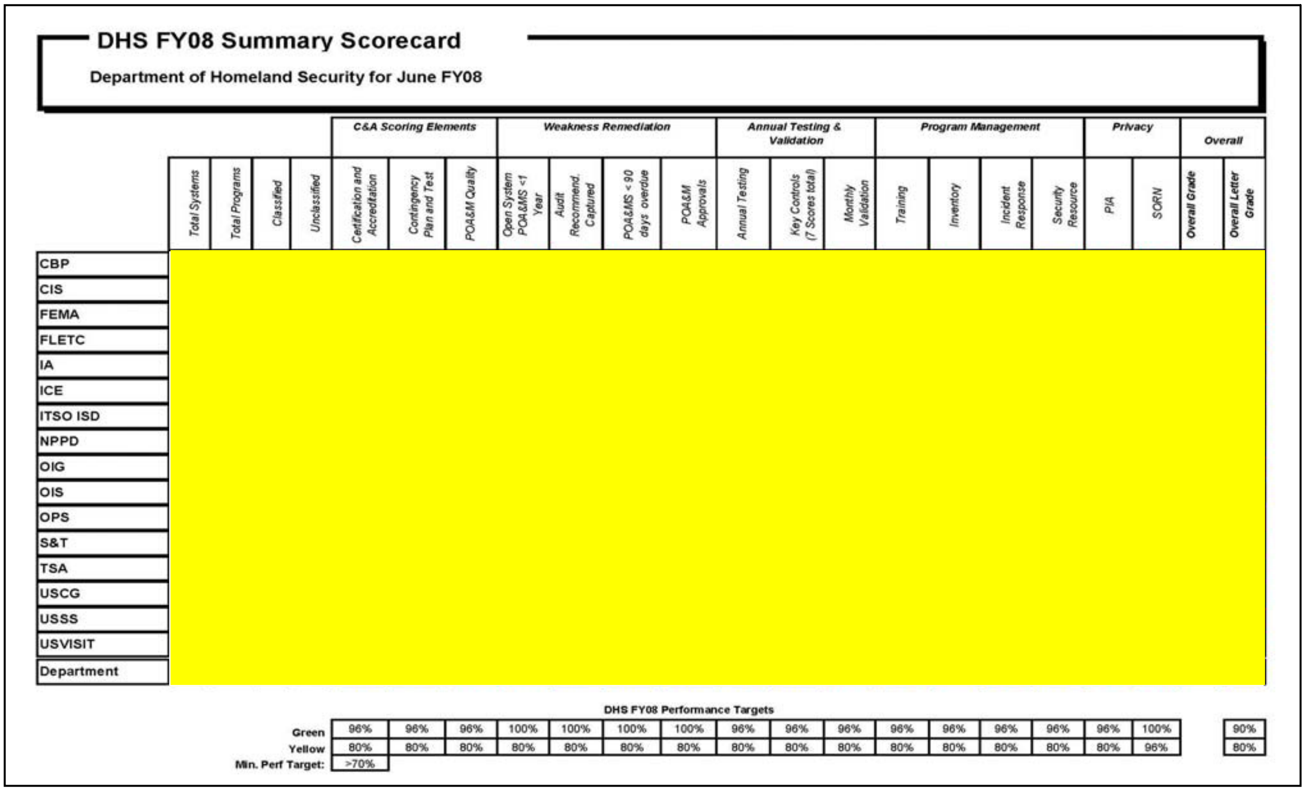
| | | | Certification & Accreditation | | | Weakness Remediation | | Continuous Monitoring | | | | Component Oversight | | | Privacy | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Components | Total Systems | Total Programs | Current C&A Package | Contingency Plan and Test | POA&M Quality | POA&M Management | Weaknesses Captured | Annual Testing and Key Controls | Information Security Training | Current Inventory | Incident Response Follow-Up | Quarterly Component Validation | Configuration Management | Component Program Review | PIA | SORN | Score (%) | Grade |
| CBP | | | | | | | | | | | | | | | | | | |
| DHS HQ | | | | | | | | | | | | | | | | | | |
| DNDO | | | | | | | | | | | | | | | | | | |
| IA | | | | | | | | | | | | | | | | | | |
| ISO | | | | | | | | | | | | | | | | | | |
| ITSO RMC | | | | | | | | | | | | | | | | | | |
| NPPD | | | | | | | | | | | | | | | | | | |
| OPS | | | | | | | | | | | | | | | | | | |
| S&T | | | | | | | | | | | | | | | | | | |
| FEMA | | | | | | | | | | | | | | | | | | |
| FLETC | | | | | | | | | | | | | | | | | | |
| ICE | | | | | | | | | | | | | | | | | | |
| OIG | | | | | | | | | | | | | | | | | | |
| TSA | | | | | | | | | | | | | | | | | | |
| USCG | | | | | | | | | | | | | | | | | | |
| USCIS | | | | | | | | | | | | | | | | | | |
| USSS | | | | | | | | | | | | | | | | | | |
| Department | | | | | | | | | | | | | | | | | | |
| | | Green | 96% | 96% | 90% | 90% | 100% | 90% | 90% | PASS | 90% | 90% | 90% | 90% | 96% | 96% | | 90% |
| | | Yellow | 80% | 80% | 80% | 80% | 80% | 80% | 80% | N/A | 80% | 80% | 80% | 80% | 80% | 80% | | 80% |



Homeland Security

July FY09 FISMA Scorecard

| | | | Certification & Accreditation | | | Weakness Remediation | | Continuous Monitoring | | | | Component Oversight | | | Privacy | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Components | Total Systems | Total Programs | Current C&A Package | Contingency Plan and Test | POA&M Quality | POA&M Management | Weaknesses Captured | Annual Testing and Key Controls | Information Security Training | Current Inventory | Incident Response Follow-Up | Quarterly Component Validation | Configuration Management | Component Program Review | PIA | SORN | Score (%) | Grade |
| CBP | | | | | | | | | | | | | | | | | | |
| DHS HQ | | | | | | | | | | | | | | | | | | |
| DNDO | | | | | | | | | | | | | | | | | | |
| IA | | | | | | | | | | | | | | | | | | |
| ISO | | | | | | | | | | | | | | | | | | |
| ITSO RMC | | | | | | | | | | | | | | | | | | |
| NPPD | | | | | | | | | | | | | | | | | | |
| OPS | | | | | | | | | | | | | | | | | | |
| S&T | | | | | | | | | | | | | | | | | | |
| FEMA | | | | | | | | | | | | | | | | | | |
| FLETC | | | | | | | | | | | | | | | | | | |
| ICE | | | | | | | | | | | | | | | | | | |
| OIG | | | | | | | | | | | | | | | | | | |
| TSA | | | | | | | | | | | | | | | | | | |
| USCG | | | | | | | | | | | | | | | | | | |
| USCIS | | | | | | | | | | | | | | | | | | |
| USSS | | | | | | | | | | | | | | | | | | |
| Department | | | | | | | | | | | | | | | | | | |
| | | Green | 96% | 96% | 90% | 90% | 100% | 90% | 90% | PASS | 90% | 90% | 90% | 90% | 96% | 96% | | 90% |
| | | Yellow | 80% | 80% | 80% | 80% | 80% | 80% | 80% | N/A | 80% | 80% | 80% | 80% | 80% | 80% | | 80% |



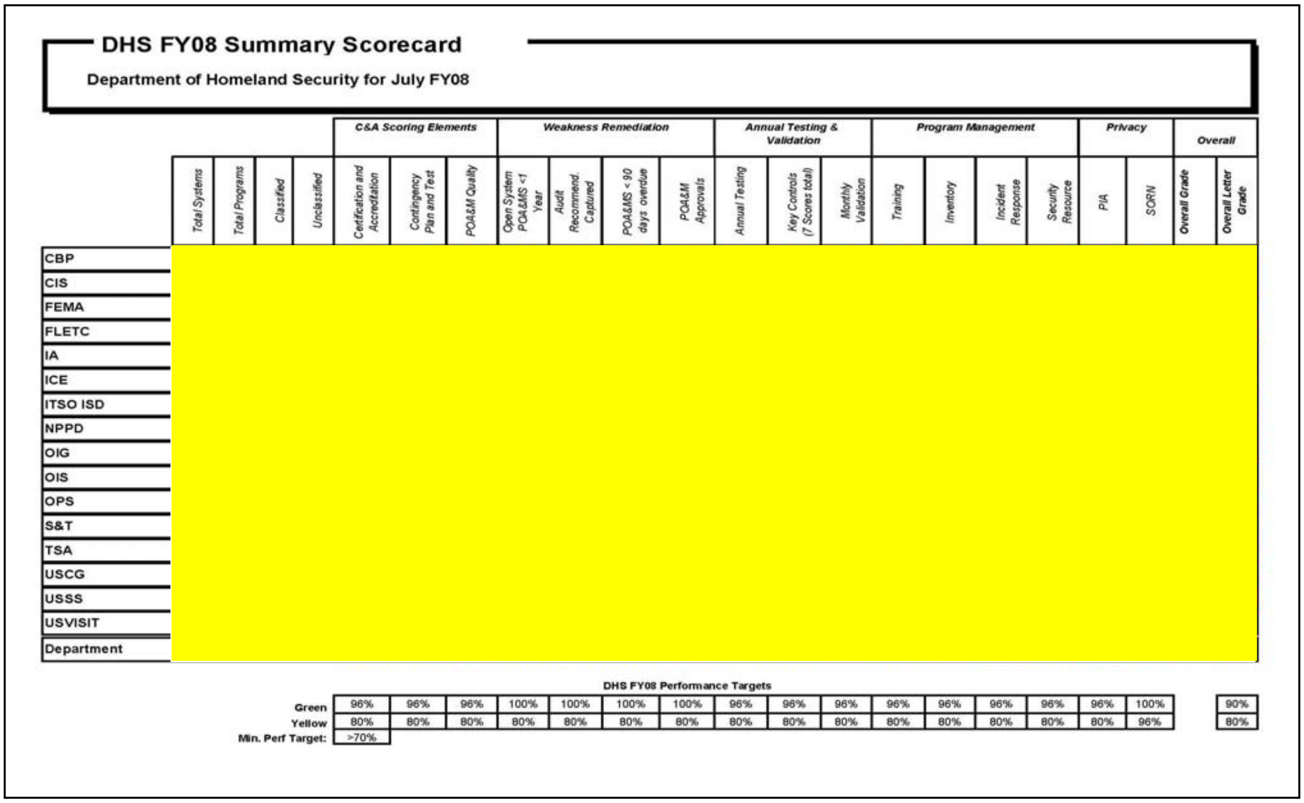
## DHS FY08 Summary Scorecard

Department of Homeland Security for June FY08

| | | | | | C&A Scoring Elements | | | Weakness Remediation | | | | Annual Testing & Validation | | | Program Management | | | | Privacy | | Overall | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Total Systems | Total Programs | Classified | Unclassified | Certification and Accreditation | Contingency Plan and Test | POA&M Quality | Open System POA&MS <1 Year | Audit Recommend. Captured | POA&MS < 90 days overdue | POA&M Approvals | Annual Testing | Key Controls (7 Scores total) | Monthly Validation | Training | Inventory | Incident Response | Security Resource | PIA | SORN | Overall Grade | Overall Letter Grade |
| CBP | | | | | | | | | | | | | | | | | | | | | | |
| CIS | | | | | | | | | | | | | | | | | | | | | | |
| FEMA | | | | | | | | | | | | | | | | | | | | | | |
| FLETC | | | | | | | | | | | | | | | | | | | | | | |
| IA | | | | | | | | | | | | | | | | | | | | | | |
| ICE | | | | | | | | | | | | | | | | | | | | | | |
| ITSO ISD | | | | | | | | | | | | | | | | | | | | | | |
| NPPD | | | | | | | | | | | | | | | | | | | | | | |
| OIG | | | | | | | | | | | | | | | | | | | | | | |
| OIS | | | | | | | | | | | | | | | | | | | | | | |
| OPS | | | | | | | | | | | | | | | | | | | | | | |
| S&T | | | | | | | | | | | | | | | | | | | | | | |
| TSA | | | | | | | | | | | | | | | | | | | | | | |
| USCG | | | | | | | | | | | | | | | | | | | | | | |
| USSS | | | | | | | | | | | | | | | | | | | | | | |
| USVISIT | | | | | | | | | | | | | | | | | | | | | | |
| Department | | | | | | | | | | | | | | | | | | | | | | |

DHS FY08 Performance Targets

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Green | 96% | 96% | 96% | 100% | 100% | 100% | 100% | 96% | 96% | 96% | 96% | 96% | 96% | 96% | 96% | 100% | | 90% |
| Yellow | 80% | 80% | 80% | 80% | 80% | 80% | 80% | 80% | 80% | 80% | 80% | 80% | 80% | 80% | 80% | 96% | | 80% |
| Min. Perf Target: | >70% | | | | | | | | | | | | | | | | | |



## DHS FY08 Summary Scorecard

Department of Homeland Security for July FY08

| | | | | | C&A Scoring Elements | | | Weakness Remediation | | | | Annual Testing & Validation | | | Program Management | | | | Privacy | | Overall | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Total Systems | Total Programs | Classified | Unclassified | Certification and Accreditation | Contingency Plan and Test | POA&M Quality | Open System POA&MS <1 Year | Audit Recommend. Captured | POA&MS < 90 days overdue | POA&M Approvals | Annual Testing | Key Controls (7 Scores total) | Monthly Validation | Training | Inventory | Incident Response | Security Resource | PIA | SORN | Overall Grade | Overall Letter Grade |
| CBP | | | | | | | | | | | | | | | | | | | | | | |
| CIS | | | | | | | | | | | | | | | | | | | | | | |
| FEMA | | | | | | | | | | | | | | | | | | | | | | |
| FLETC | | | | | | | | | | | | | | | | | | | | | | |
| IA | | | | | | | | | | | | | | | | | | | | | | |
| ICE | | | | | | | | | | | | | | | | | | | | | | |
| ITSO ISD | | | | | | | | | | | | | | | | | | | | | | |
| NPPD | | | | | | | | | | | | | | | | | | | | | | |
| OIG | | | | | | | | | | | | | | | | | | | | | | |
| OIS | | | | | | | | | | | | | | | | | | | | | | |
| OPS | | | | | | | | | | | | | | | | | | | | | | |
| S&T | | | | | | | | | | | | | | | | | | | | | | |
| TSA | | | | | | | | | | | | | | | | | | | | | | |
| USCG | | | | | | | | | | | | | | | | | | | | | | |
| USSS | | | | | | | | | | | | | | | | | | | | | | |
| USVISIT | | | | | | | | | | | | | | | | | | | | | | |
| Department | | | | | | | | | | | | | | | | | | | | | | |

DHS FY08 Performance Targets

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Green | 96% | 96% | 96% | 100% | 100% | 100% | 100% | 96% | 96% | 96% | 96% | 96% | 96% | 96% | 96% | 100% | | 90% |
| Yellow | 80% | 80% | 80% | 80% | 80% | 80% | 80% | 80% | 80% | 80% | 80% | 80% | 80% | 80% | 80% | 96% | | 80% |
| Min. Perf Target: | >70% | | | | | | | | | | | | | | | | | |

**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 within in accordance with policy.**

| | | **Question 1** | | | | | | | | **Question 2** | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | **a.<br>Agency Systems** | | **b.<br>Contractor Systems** | | **c.<br>Systems Used by the Agency but Owned by Another Agency** | | **d.<br>Total Number of Systems (Agency and Contractor systems)<br>(Column A + Column B)** | | **a.<br>Number of systems certified and accredited** | | **b.<br>Number of systems for which security controls have been tested and reviewed in the past year** | | **c.<br>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 | 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 | 18 | 10 | 1 | 0 | 0 | 0 | 19 | 10 | 10 | 100% | 10 | 100% | 10 | 100% |
| | Moderate | 30 | 3 | 1 | 0 | 0 | 0 | 31 | 3 | 3 | 100% | 3 | 100% | 3 | 100% |
| | Low | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 100% | 1 | 100% | 1 | 100% |
| | Undefined | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | **Sub-total** | **48** | **13** | **3** | **1** | **1** | **1** | **51** | **14** | **14** | **100%** | **14** | **100%** | **13** | **93%** |
| **DNDO** | High | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | Moderate | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | Low | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | **Sub-Total** | **1** | **0** | **0** | **0** | **0** | **0** | **1** | **0** | **0** | **0%** | **0** | **0%** | **0** | **0%** |
| **FEMA** | High | 14 | 7 | 5 | 2 | 0 | 0 | 19 | 9 | 9 | 100% | 8 | 89% | 7 | 78% |
| | Moderate | 14 | 2 | 14 | 3 | 0 | 0 | 28 | 5 | 4 | 80% | 4 | 80% | 5 | 100% |
| | Low | 5 | 1 | 4 | 0 | 0 | 0 | 9 | 1 | 1 | 100% | 1 | 100% | 1 | 100% |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Sub-total** | **33** | **10** | **23** | **5** | **0** | **0** | **56** | **15** | **14** | **93%** | **13** | **87%** | **13** | **87%** |
| **FLETC** | High | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | Moderate | 7 | 2 | 2 | 1 | 0 | 0 | 9 | 3 | 3 | 100% | 3 | 100% | 3 | 100% |
| | Low | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | Undefined | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | **Sub-total** | **8** | **2** | **2** | **1** | **0** | **0** | **10** | **3** | **3** | **100%** | **3** | **100%** | **3** | **100%** |
| **I&A** | High | 1 | 0 | 1 | 0 | 0 | 0 | 2 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | Moderate | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | Low | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | **Sub-total** | **2** | **0** | **1** | **0** | **0** | **0** | **3** | **0** | **0** | **0%** | **0** | **0%** | **0** | **0%** |
| **ICE** | High | 9 | 3 | 14 | 3 | 0 | 0 | 23 | 6 | 5 | 83% | 1 | 17% | 6 | 100% |
| | Moderate | 16 | 2 | 24 | 2 | 0 | 0 | 40 | 4 | 4 | 100% | 1 | 25% | 4 | 100% |
| | Low | 7 | 0 | 5 | 0 | 0 | 0 | 12 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | **Sub-total** | **32** | **5** | **43** | **5** | **0** | **0** | **75** | **10** | **9** | **90%** | **2** | **20%** | **10** | **100%** |
| **ISO** | High | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | Moderate | 0 | 0 | 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% | 0 | 0% |
| | **Sub-total** | **1** | **0** | **1** | **0** | **0** | **0** | **2** | **0** | **0** | **0%** | **0** | **0%** | **0** | **0%** |
| **RMC** | High | 6 | 3 | 8 | 2 | 0 | 0 | 4 | 5 | 5 | 100% | 1 | 20% | 3 | 60% |
| | Moderate | 4 | 2 | 4 | 1 | 0 | 0 | 8 | 3 | 3 | 100% | 3 | 100% | 2 | 67% |
| | Low | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | Undefined | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | **Sub-total** | **11** | **5** | **13** | **3** | **0** | **0** | **24** | **8** | **8** | **100%** | **3** | **38%** | **5** | **63%** |
| **NPPD** | High | 2 | 0 | 6 | 4 | 0 | 0 | 8 | 4 | 4 | 100% | 3 | 75% | 3 | 75% |
| | Moderate | 5 | 0 | 10 | 0 | 0 | 0 | 15 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | Low | 1 | 1 | 1 | 0 | 0 | 0 | 2 | 1 | 1 | 100% | 1 | 100% | 1 | 100% |
| | **Sub-total** | **8** | **1** | **17** | **4** | **0** | **0** | **25** | **5** | **5** | **100%** | **4** | **80%** | **4** | **80%** |
| **OIG** | High | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | Moderate | 0 | 0 | 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% | 0 | 0% |
| | **Sub-total** | **2** | **0** | **0** | **0** | **0** | **0** | **2** | **0** | **0** | **0%** | **0** | **0%** | **0** | **0%** |
| **OPS** | High | 1 | 0 | 1 | 0 | 0 | 0 | 2 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | Moderate | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Low | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | **Sub-total** | **2** | **0** | **1** | **0** | **0** | **0** | **3** | **0** | **0** | **0%** | **0** | **0%** | **0** | **0%** |
| **S&T** | High | 2 | 0 | 1 | 0 | 0 | 0 | 3 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | Moderate | 4 | 2 | 5 | 1 | 0 | 0 | 9 | 3 | 3 | 100% | 3 | 100% | 3 | 100% |
| | Low | 1 | 0 | 5 | 0 | 0 | 0 | 6 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | **Sub-total** | **7** | **2** | **11** | **1** | **0** | **0** | **18** | **3** | **3** | **100%** | **3** | **100%** | **3** | **100%** |
| **TSA** | High | 15 | 3 | 8 | 2 | 0 | 0 | 23 | 5 | 5 | 100% | 5 | 100% | 5 | 100% |
| | Moderate | 29 | 3 | 15 | 0 | 0 | 0 | 44 | 3 | 3 | 100% | 3 | 100% | 3 | 100% |
| | Low | 5 | 0 | 2 | 0 | 0 | 0 | 7 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | Undefined | 7 | 3 | 0 | 0 | 0 | 0 | 7 | 3 | 3 | 100% | 2 | 67% | 3 | 100% |
| | **Sub-total** | **56** | **9** | **25** | **2** | **0** | **0** | **81** | **11** | **11** | **100%** | **10** | **91%** | **11** | **100%** |
| **USCG** | High | 37 | 7 | 5 | 3 | 0 | 0 | 42 | 10 | 10 | 100% | 8 | 80% | 9 | 90% |
| | Moderate | 44 | 6 | 17 | 3 | 0 | 0 | 61 | 9 | 6 | 67% | 4 | 44% | 9 | 100% |
| | Low | 12 | 0 | 4 | 2 | 0 | 0 | 16 | 2 | 1 | 50% | 1 | 50% | 2 | 100% |
| | **Sub-total** | **93** | **13** | **26** | **8** | **0** | **0** | **119** | **21** | **17** | **81%** | **13** | **62%** | **20** | **95%** |
| **USCIS** | High | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | Moderate | 61 | 3 | 32 | 7 | 0 | 0 | 93 | 10 | 10 | 100% | 10 | 100% | 10 | 100% |
| | Low | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | **Sub-total** | **61** | **3** | **35** | **7** | **0** | **0** | **96** | **10** | **10** | **100%** | **10** | **100%** | **10** | **100%** |
| **USSS** | High | 9 | 3 | 0 | 0 | 0 | 0 | 9 | 3 | 3 | 100% | 2 | 67% | 3 | 100% |
| | Moderate | 3 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | Low | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0% | 0 | 0% | 0 | 0% |
| | **Sub-total** | **13** | **3** | **0** | **0** | **0** | **0** | **13** | **3** | **3** | **100%** | **2** | **67%** | **3** | **100%** |
| **Agency Totals** | **High** | **117** | **36** | **51** | **16** | **0** | **0** | **168** | **52** | **51** | **98%** | **38** | **73%** | **46** | **88%** |
| | **Moderate** | **219** | **25** | **125** | **18** | **0** | **0** | **344** | **43** | **39** | **91%** | **34** | **79%** | **42** | **98%** |
| | **Low** | **33** | **2** | **25** | **3** | **0** | **0** | **58** | **5** | **4** | **80%** | **4** | **80%** | **5** | **100%** |
| | **Undefined** | **9** | **3** | **0** | **0** | **1** | **1** | **9** | **3** | **3** | **100%** | **2** | **67%** | **3** | **100%** |
| | **Total** | **378** | **66** | **201** | **37** | **1** | **1** | **579** | **103** | **97** | **94%** | **78** | **76%** | **96** | **93%** |

Appendix F
Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory

| | |
|---|---|
| **Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory** | |
| | **Response:** |
| **Does the agency have policies for oversight of contractors?** Yes/No<br>If the answer above is Yes, Is the policy implemented? | **Yes**<br>**Yes** (a) |
| **The agency has a materially correct inventory of major information systems (including national security systems) operated by or under the control of such agency.** Yes/No | **Yes** |
| **Does the agency maintain an inventory of interfaces between the agency systems and all other systems, such as those not operated by or under the control of the agency?** Yes/No | **Yes** |
| **Does the agency require agreements for interfaces between systems it owns or operates and other systems not operated by or under the control of the agency?** Yes/No | **Yes** (b) |
| **The IG generally agrees with the CIO on the number of agency-owned systems.** Yes/No | **Yes** |
| **The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency.** Yes/No | **Yes** |
| **The agency inventory is maintained and updated at least annually.** Yes/No | **Yes** |

**If the IG does not indicate that the agency has a materially correct inventory, please identify any known missing major systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the systems as presented in the FY 2009 Exhibit 300 (if known), and indicate if the system is an agency or contractor system.**

| Component/Bureau | System Name | Exhibit 300 Unique Project Identifier (UPI) | Agency or Contractor System? |
|---|---|---|---|
| CBP | WWW.CBP.GOV | | Agency System Owned by Another Agency |
| | | | |
| | | | |
| **Number of known systems missing from the inventory:** | **1 System Missing** | | |

(a) Implementation of policy for contractor owned or operated systems needs improvement. During our C&A review and web server audit, we identified instances where components did not ensure that the required vulnerability assessments or configuration setting reviews are performed by the contractors.

(b) During our C&A quality review, we found that some memorandum of agreements (MOAs) were out-dated or have yet to be established.

| **Question 4: Evaluation of Agency Plan of Action and Milestones (POA&M) Process** | |
|---|---|
| **Assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestones (POA&M) process, providing explanatory detail in the area provided.** | **Response:** |
| **Has the Agency developed and documented an adequate policy that establishes a POA&M process for reporting IT security deficiencies and tracking the status of remediation efforts?** Yes/No | **Yes** (a) |
| **Has the Agency fully implemented the policy?** Yes/No | **Yes**(b) |
| **Is the Agency currently managing and operating a POA&M process?** Yes/No | **Yes** (c) |
| **Is the agency's POA&M process an agency-wide process, incorporating all known IT security weakness, including IG/external audit findings associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency?** Yes/No | **Yes** (d) |
| **Does the POA&M process prioritize IT security weakness to help ensure significant IT security weaknesses are corrected in a timely manner and receive appropriate resources?** Yes/No | **No** (e) |
| **When an IT security weakness is identified, do program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s)?** Yes/No | **Yes** |
| **For Systems Reviewed:**<br>**a. Are deficiencies tracked and remediated in a timely manner?** Yes/No<br>**b. Are the remediation plans effective for correcting the security weakness?** Yes/No<br>**c. Are the estimated dates for remediation reasonable and adhered to?** Yes/No | **a. Yes**<br>**b. Yes**<br>**c. Yes** (f) |
| **Do Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly)?** Yes/No | **Yes** (g) |
| **Does the Agency CIO centrally track, maintain, and independently review/validate POA&M activities on at least a quarterly basis?** Yes/No | **Yes** (h) |

(a) DHS requires components to create and manage POA&Ms for all known IT security weaknesses.

(b) As of June 30, 2009, DHS has 3,918 open POA&Ms. However, POA&Ms have not been created for all weaknesses identified during the C&A process. Components are not consistently maintaining and tracking their classified POA&Ms.

(c) DHS is managing and operating a POA&M process on its unclassified systems. However, components are not consistently maintaining, tracking, or prioritizing their classified POA&Ms.

(d) POA&Ms have not been created for all OIG audit findings. Components have created POA&Ms for 162 out of 179 (91%) recommendations cited in OIG audit reports (including Notice of Findings and Recommendations).

(e) For classified POA&Ms, components have not identified the source of the weakness or included the milestones of the POA&Ms. In addition, there is no evidence of periodic updates, component CISO reviews, or that these weaknesses were properly prioritized.

(f) Out of the 3,918 open POA&Ms, there are 837 POA&MS that are three months past due and 563 POA&MS that are 12 months past due. Our review also determined that 1,859 out of 3,918 (47%) open POA&Ms have been delayed.

(g) DHS requires that all POA&M information be updated at least monthly. However, POA&Ms have not been updated on a regular basis. For example, 1,488 out of 3,918 (38%) open POA&Ms have not been updated within the last 90 days.

(h) The CIO regularly performs daily quality reviews (automated) on all POA&Ms to ensure that information entered into the enterprise management system is accurate, reasonable, and complete. However, components are not entering and tracking all IT security weaknesses in DHS' enterprise management tool, nor is all of the data entered by the components accurate and updated in a timely manner.

# Appendix H
# IG Assessment of the Certification and Accreditation Process

| | | |
|---|---|---|
| **Question 5: IG Assessment of the Certification and Accreditation Process** | | |
| **Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems (May 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199 (February 2004), Standards for Security Categorization of Federal Information and Information Systems, to determine a system impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans. Provide explanatory detail in the area provided.** | | **Response:** |
| **Has the Agency developed and documented an adequate policy for establishing a certification and accreditation process that follows the NIST framework?** Yes/No | | **Yes** (a) |
| **Is the Agency currently managing and operating a C&A process in compliance with its policies?** Yes/No | | **Yes** |
| **For systems reviewed, does the C&A process adequately provide: (check all that apply)** | Appropriate risk categories | **X** |
| | Adequate risk assessments | **X** |
| | Selection of appropriate controls | **X** |
| | | **X** |
| | Regular monitoring of system risks and the adequacy of controls | **X** |
| **For systems reviewed, is the Authorizing Official presented with complete and reliable C&A information to facilitate an informed system Authorization to Operate decision based on risks and controls implemented?** Yes/No | | **Yes** (b) |

(a) DHS bases its certification and accreditation (C&A) process on NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* for its unclassified systems. Components are required to follow Department of Defense (DoD) Information Assurance Certification and Accreditation Process when certifying and accrediting its classified systems.

(b) Based on our review of 35 systems across 12 components, artifacts that are required to C&A a system were either missing or incomplete.

| **Question 6: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process** | |
|---|---|
| **Provide a qualitative assessment of the agency's process, as discussed in Section D, for protecting privacy-related information, including adherence to existing policy, guidance and standards. Provide explanatory information in the area provided.** | **Response:** |
| **Has the Agency developed and documented adequate policies that comply with OMB guidance in M-07-16, M-06-15, and M-06-16 for safeguarding privacy-related information?** Yes/No | **Yes (a)** |
| **Is the Agency currently managing and operating a privacy program with appropriate controls in compliance with its policies?** Yes/No | **Yes** |
| **Has the Agency developed and documented an adequate policy for Privacy Impact Assessments?** Yes/No/NA | **Yes** |
| **Has the Agency fully implemented the policy and is the Agency currently managing and operating a process for performing adequate privacy impact assessments?** Yes/No/NA | **Yes** |

(a) DHS has not implemented all of the requirements outlined in OMB M-07-16. Specifically, DHS has not defined the consequences for any users who do not comply with the policy. The Privacy Office is working in conjunction with the Office of General Counsel and the Chief Human Capital Office to develop the consequences of non-compliance policy.

| Question 7: Configuration Management | |
|---|---|
| | **Response:** |
| **Is there an agency-wide security configuration policy?** Yes/No | **Yes** |
| **What tools, techniques is your agency using for monitoring compliance?** | **Tenable Security Center** |
| **Indicate the status of the implementation of FDCC at your agency :**<br>**- Agency has documented deviations from FDCC standard configuration.** Yes/No | **Yes** |
| **- New Federal Acquisition Regulation 2007-004 language, which modified "Part 39—Acquisition of Information Technology", is included in all contracts related to common security settings.** Yes/No. | **No (a)** |

(a) DHS has not incorporated the standard FDCC contract language into all IT acquisitions. CBP, FLETC, ICE and TSA have not incorporated the standard language into their IT contracts. While CIS indicated that they had incorporated the language into their IT acquisitions, we could not identify the FDCC standard language in the contracts sampled.

| **Question 8: Incident Reporting** | |
|---|---|
| | **Response:** |
| **How often does the agency comply documented policies and procedures for identifying and reporting incidents internally?** Answer will be a percentage range | **90-100%** |
| **How often does the agency comply with documented policies and procedures for timely reporting of incidents to US CERT?** Answer will be a percentage range | **90-100%** |
| **How often does the agency comply documented policy and procedures for reporting to law enforcements?** Answer will be a percentage range | **90-100%** |

| Question 9: Security Awareness Training | |
|---|---|
| | **Response:** |
| **Has the agency ensured IT security awareness training of all users with log in privileges, including contractors and those employees with significant IT security responsibilities?** Provide explanatory detail in the space provided. | **Yes. (a)** |
| **Has the Agency developed and documented an adequate policy for identifying all general users, contractors, and system owners/employees who have log in privileges, and providing them with suitable IT security awareness training?** Yes/No/NA | **Yes** |
| **Report the following for your agency:**<br>Total number of people with log in privileges to agency systems | **Unable to Determine** (b) |
| **Number of people with log in privileges to agency systems that received information security awareness training during the past fiscal year, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program" (October 2003).** | **Unable to Determine** |
| **Total number of employees with significant information security responsibilities.** | **2,701** |
| **Number of employees with significant security responsibilities that received specialized training, as described in NIST Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model" (April 1998)** | **2,535** |

| Question 10: Peer-to-Peer File Sharing | |
|---|---|
| | **Response:** |
| **Does the agency explain policies regarding the use peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training?** Yes/No | **Yes** |

(a) DHS requires all employees and contractors to take security awareness training at least annually.
(b) As of August 1, 2009, DHS has a total of 262,049 employees and contractors at various components. DHS does not maintain a centralized list of users with log in privileges. Components are responsible for creating and maintaining user accounts for its employees and contractors. As such, we are unable to determine the number of users with log in privileges.

**Information Security Audit Division**

Edward G. Coleman, Director
Chiu-Tong Tsang, Audit Manager
Barbara Bartuska, Audit Manager
Mike Horton, Information Technology Officer
Maria L. Rodriguez, Team Lead
Aaron Zappone, Program Analyst
Thomas Rohrback, IT Specialist
Michael Kim, IT Auditor
David Bunning, IT Specialist
Joseph Landas, Management/Program Assistant
Lauren Badley, Management/Program Assistant

Pamela Chambliss-Williams, Referencer

## 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,<br>
  Attention: Office of Investigations - Hotline,<br>
  245 Murray Drive, SW, Building 410,<br>
  Washington, DC 20528.

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