DEPARTMENT OF HOMELAND SECURITY
Office of Inspector General

Evaluation of DHS' Information Security Program for Fiscal Year 2008

OIG-08-94

September 2008

Office of Inspector General

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

Homeland
Security

September 15, 2008

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
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
CISO	Chief Information Security Officer
DHS	Department of Homeland Security
FDCC	Federal Desktop Core Configuration
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards

Table of Contents/Abbreviations

FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center
FY	Fiscal Year
ICE	United States Immigration and Customs Enforcement
ISSM	Information Systems Security Manager
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
OIS	Office of Information Security
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
SP	Special Publication
S&T	Science and Technology
Training Office	Information Security Training, Education, and Awareness Office
TSA	Transportation Security Administration
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Services
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 of 2002* (*Public Law* 107-347, Sections 301-305). We evaluated the department's progress in implementing its agency-wide information security program. In doing so, we specifically assessed the department's Plan of Action and Milestones (POA&M), as well as its certification and accreditation (C&A) processes. We also performed an assessment 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, the department implemented a performance plan to improve on four key areas: POA&M weaknesses remediation, quality of C&A, annual testing and validation, and security program oversight. The performance plan tracks key elements that are indicative of a strong security program. In addition, the department strengthened its oversight at the components and conducted compliance reviews in the areas of C&A and configuration management. While these efforts have resulted in some improvements, components are still not executing all of the department's policies, procedures, and practices. For example, the more significant exceptions noted are:

- Systems are being accredited though key documents and key information are 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.

Management oversight of the components' implementation of the department's policies and procedures needs improvement in order for the department to ensure that all information security weaknesses are tracked and remediated, and 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 nine recommendations to the Chief Information Officer and Chief Privacy Officer. The department concurred with all 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.

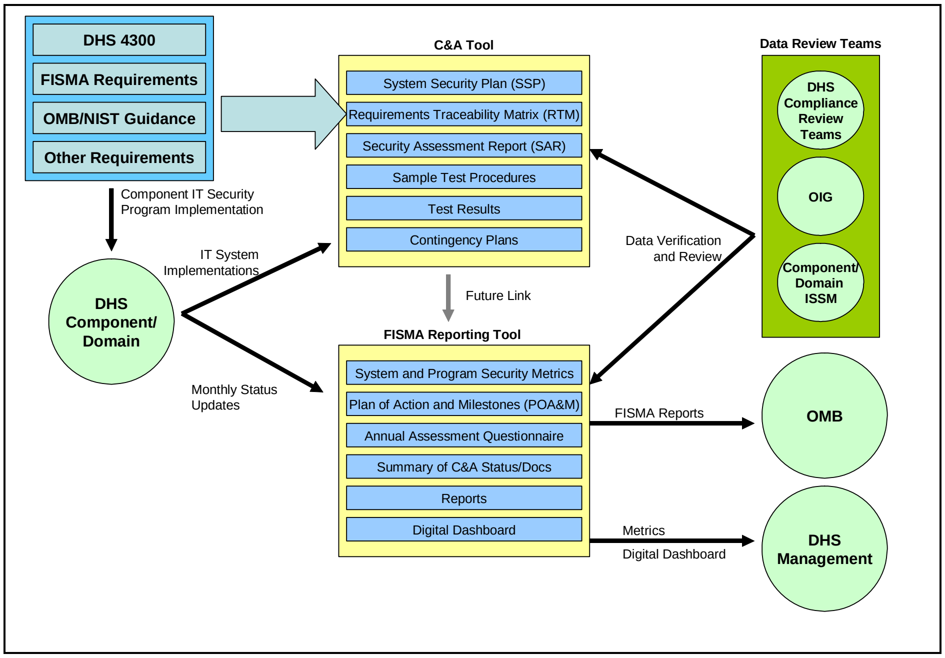
FISMA requires each federal agency to develop, document, and implement an agency-wide security program. The agency's security program should protect the information and the information systems that support the operations and assets of the agency, including those provided or managed by another agency, 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-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, on July 14, 2008. 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 Office of Information Security (OIS) 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 Review Teams
DHS Compliance Review Teams
OIG
Component/ Domain ISSM
Data Verification and Review
FISMA Reports
OMB
Metrics
Digital Dashboard
DHS Management

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

Results of Independent Evaluation

We separated the results of our evaluation into seven FISMA areas. For each area, we identified the progress that DHS has made since our Fiscal Year (FY) 2007 evaluation and those issues that need to be addressed to be more successful in the FISMA area.

OVERALL PROGRESS

- The CISO developed the *Fiscal Year 2008 DHS Information Security Performance Plan "Achieving Excellence"* to enhance its information security program. The purpose of the plan is to strengthen components' compliance with DHS' security program and to improve the department's incident response capability through the development of a robust Network Operations/Security Operations Center. The CISO developed a FISMA scorecard to manage components' compliance with the performance plan. See Appendix C for an example 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.
- DHS continues to maintain an effective process to update and manage an inventory of its agency and contractor systems on an annual basis. In addition, DHS conducted site visits to component offices outside the Washington D.C. area to determine whether there were any systems that had not been identified by the Information Systems Security Manager (ISSM) during the annual system inventory reviews.
- DHS has taken an active role in ensuring that components comply with FISMA. The CISO implemented more stringent criteria for reviewing the artifacts that components are required to upload into the department's enterprise management tool, in order to support their C&A packages. See Appendix C for FY 2008 grades assigned by the CISO.
- The CISO established a new in-depth review team. The team conducted site-visits at 10 components to determine whether DHS security requirements had been implemented on selected systems. As of July 2008, the team had reviewed 11 systems at 10 components. DHS plans to review 25 to 40 percent of its systems in FY 2009.

- The CISO established a new configuration management compliance team and randomly selected 23 systems at 7 components to evaluate their configuration management processes and determine whether DHS' baseline configuration settings had been implemented.
- The Office of Human Capital implemented a department-wide, web-based learning management system "*DHScovery*." The implementation of *DHScovery* can assist DHS in standardizing security awareness training and track employee completion of the training.

OVERALL ISSUES TO BE ADDRESSED

Despite the progress described above, the results of our review revealed that components are still not executing fully the department's policies, procedures, and practices. For example, we determined:

- Artifacts required to support the systems that have been accredited by the components were either missing key information or incomplete.
- Components have not incorporated all known security weaknesses into their POA&Ms.
- Components have not fully implemented DHS' baseline configuration settings.
- DHS does not have an automated process for maintaining and tracking its classified POA&Ms.
- Appropriate training is needed for all individuals with significant security responsibilities.
- Escalation process is needed for privacy impact assessments (PIA) that have been in the review and approval process for an extended period of time.

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 also 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. As of July 31, 2008, DHS identified 591 operational systems.
- DHS continues to maintain an effective process to update and manage its inventory on an annual basis for agency and contractor systems by reviewing the system inventory with each component.
- DHS conducts site visits to component offices outside the Washington D.C. area to determine whether there are any systems that had not been identified by the ISSM during the annual system inventory update process.

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

Certification and Accreditation Process

DHS requires components to use an enterprise-wide tool that incorporates NIST security controls required for system C&A. The C&A process requires documentation to include system security plans, risk assessments, system test and evaluation plans, security assessment reports, contingency plans, and contingency plan test results. Components are required to apply NIST Special Publication (SP) 800-53 security controls for all system C&A and self-assessments. For some of the systems that have been accredited by the components, the artifacts required to support the C&A 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 2007 FISMA report.[1]

PROGRESS

- DHS continues to require 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

[1] *Evaluation of DHS' Information Security Program for Fiscal Year 2007* (OIG-07-77, September 2007).

determination, privacy threshold analysis (PTA), and NIST SP 800-53 self-assessment.

- As of July 31, 2008, the CISO reported that 95 percent of DHS' operational systems (560/591) have been certified and accredited.
- The quality of C&A packages has improved in FY 2008, when compared to FY 2007. Specifically, only two of the 25 systems we evaluated this year had incomplete C&A packages where key security documents were missing, compared to 17 of 28 incomplete C&A packages reported in FY 2007. However, we continued to identify instances where required information was missing from security documents.

ISSUES TO BE ADDRESSED

- Systems were being accredited without key documents or where C&A documents were missing key information. We selected 25 systems from 12 components and offices to evaluate the quality of DHS' C&A process. For two systems, the accreditation packages were incomplete as key security documents were missing. For other systems, we identified that some of the required security documents were missing key information. Without this information, agency officials cannot make credible, risk-based decisions on whether to authorize the system to operate. Specifically, we determined:
  - ➢ Five instances where the FIPS-199 determination was not completed in accordance with applicable DHS and NIST guidance.
  - ➢ Twenty-two instances where system security plans were missing sections that describe detailed emergency configuration changes, management plans, security controls, and incident handling procedures.
  - ➢ Nineteen instances where contingency plans were incomplete, missing the identification of alternate processing facilities or restoration procedures. One of the contingency plans reviewed was more than four years old.
  - ➢ Three instances where the contingency plans had not been tested. Some of the contingency plans could not be tested because the alternate processing facilities were not operational.
  - ➢ Eleven instances where some of the required critical security controls were not included in the system test and evaluation plan.

- 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 a compliance description for all applicable controls on how they were implemented. In addition, we evaluated whether supporting documentation existed for all controls that were reported as "tested". Finally, we evaluated the adequacy of justification 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. For example:
    - ➢ Twelve instances where some controls, required by DHS and NIST, were missing from the templates used.
    - ➢ Twenty three instances where some 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.

- During our configuration assessment, we identified instances where the system security plans did not accurately reflect the system boundary or a description of hardware and software installed. Without this information, agency officials cannot make credible, risk-based decisions to accredit the systems.

- Components did not follow applicable guidance when performing E-Authentication determinations. We sampled 23 systems that were reported as E-Authentication applications in DHS' enterprise management tool to determine whether the assessments were properly completed and applicable controls were implemented. For example, we found:
    - ➢ Nine systems were reported incorrectly as E-Authentication applications in DHS' enterprise management tool, when compared to the E-Authentication determination. As such, DHS may not have an accurate inventory of its E-Authentication systems.
    - ➢ Four of the 14 E-Authentication systems had inconsistent assurance levels reported in DHS' enterprise management tool when compared to the source documents. Only one of the 14 E-Authentication systems properly addressed the DHS and NIST required controls in the system test and evaluation plans and security assessment reports for the assigned E-Authentication assurance levels.

See Appendix G for the OIG assessment of DHS' C&A process.

Plan of Action and Milestones Process

DHS requires components to use its enterprise management tool to capture and track security weaknesses. The 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 2007 FISMA report.

PROGRESS

- DHS continues to conduct monthly reviews of POA&Ms for completeness and also monitors the closure rate for initial and repeat audit findings. The findings are reported to OIS and components.
- Components have created POA&Ms for 182 of 200 (91%) notice of findings and recommendations (NFRs) for the weaknesses identified during the FY 2007 financial statement audit.
- As required by DHS policy, ISSMs are to review and approve all priority 4 and priority 5 POA&Ms to ensure that the weakness is properly identified, prioritized, and that appropriate resources have been made available. Priority 4 weaknesses are assigned to initial audit findings and priority 5 weaknesses for repeat audit findings. As of June 30, 2008, there were 198 POA&Ms that were classified as priority 4 and priority 5 weaknesses, all of which had been reviewed and approved by the ISSMs.

ISSUES TO BE ADDRESSED

- DHS components have not created POA&Ms for all known security weaknesses. DHS relies on the component ISSMs and Information Systems Security Officers (ISSOs) to ensure that POA&M information is entered accurately and that weaknesses are resolved. During our review, component personnel cited a lack of time and staff as the explanation that their POA&Ms are not being updated regularly. For example, we identified:
  - Four components (Federal Emergency Management Agency [FEMA], Immigration and Customs Enforcement [ICE], Management Directorate [Management], and United States Customs and Border Protection [CBP]) did not create

    POA&Ms for findings identified in OIG audit reports issued during FY 2008.

    - Although two components (CBP and Science and Technology [S&T]) followed a manual process for maintaining classified POA&Ms, there is no evidence of periodic updates, ISSM reviews, or these weaknesses were properly prioritized. FEMA has not implemented a process for maintaining and tracking its classified POA&Ms.
    - Components are not creating a POA&M 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 13 instances, POA&Ms were not created for the weaknesses identified during the C&A process. In nine instances, POA&Ms were not created for required controls that were not tested as part of NIST SP 800-53 self-assessments.

- While weaknesses were identified by the CISO's in-depth team, components have created POA&Ms for only one of the 11 systems reviewed.

- Based on an analysis of data in DHS' enterprise management tool, as of June 30, 2008, the ISSMs and ISSOs are not maintaining current information as to the progress of security weakness remediation.

    - Component management is not updating all weaknesses where the estimated completion date has been delayed. Of the 4,245 open POA&Ms with estimated completion dates, 491 (12%) were delayed by at least 3 months (prior to April 1, 2008). Further, 252 had an estimated completion date over one year old, dating as far back as September 30, 2005. In addition, completion dates for 226 of the 252 POA&Ms have not been updated since March 2006.
    - Components are required to provide justification as to why the remediation action for a POA&M is delayed. As of June 30, 2008, 1,405 (71%) of 1,978 open POA&Ms identified as delayed did not have an explanation for the delay.

    - Resources required for the remediation of 265 (6%) of the 4,245 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.

- Not all POA&Ms are being resolved in a timely manner, including weaknesses identified as significant deficiencies. As of June 30, 2008:

    - 282 (7%) of 4,245 open POA&Ms reported had estimated completion dates that were more than 2 years after the identification of the weakness.

    - 11 open weaknesses are defined as significant deficiencies. Five of these 11 significant deficiencies were created more than 12 months ago. In addition, four of these five significant deficiencies are scheduled to take more than two years to complete the mitigation efforts.[2]

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

Configuration Management

DHS has strengthened its oversight at the components. DHS also issued a baseline configuration guide for the components to follow when configuring their Windows Vista workstations. To evaluate components' compliance with DHS baseline configuration requirements, we determined whether required configuration settings had been implemented on the (1) 25 systems selected for our C&A review, and (2) 28 systems chosen for the configuration assessment. For the C&A review, we performed testing to determine whether DHS baseline configuration settings were implemented on selected servers. During our configuration assessment, we verified whether NIST SP 800-53 controls and DHS baseline configuration settings were implemented on selected servers through interviews and observations. Results from both reviews revealed that the components have not implemented all of the required DHS baseline configuration settings. We reported a similar issue in our FY2007 FISMA report.

[2] A significant deficiency is a weakness in an organization's overall IT security program or management control structure that significantly restricts the capability of the component to carry out its mission or compromises the security of its information, information system, personnel, or other resources, operations, or assets. The risk is great enough that the organization head must be notified and immediate or near-immediate corrective action must be taken.

PROGRESS

- The CISO has strengthened its oversight of the components' implementation of DHS' baseline configuration requirements. One of the objectives of DHS' configuration management compliance team is to evaluate whether baseline configuration settings are being implemented.
- DHS issued a new baseline configuration guide for Windows Vista in May 2008.

ISSUES TO BE ADDRESSED

- DHS has not implemented the Federal Desktop Core Configuration (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. According to a DHS Procurement official, the department is in the process of drafting its standardized FDCC contract language for all IT acquisitions.
  - ➢ Adopted FDCC standard configurations and documented all deviations from FDCC. According to an official from DHS' Desktop Working Group, the department is in the process of documenting the deviations from FDCC requirements.
  - ➢ Implemented FDCC security settings on its Windows XP and Vista desktops and laptops. Further, DHS has not established an implementation date for FDCC compliance. An official from DHS' Desktop Working Group indicated that the department could not implement the settings on its Windows XP and Vista desktop and laptops until all FDCC deviations are documented.

- Components have not fully 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 fully implemented on the systems. For example, components have not fully implemented warning banners, or enforced password complexities, and audit trail policies. Note: CISO's in-depth review team identified similar findings during their assessments.

- Vulnerability assessments performed at components during our Automated Commercial Environment, Automated Targeting System, Chet Holifield Federal Building, and United States Coast Guard (USCG) network security 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, ICE, and USCG.[3]

- Components are not performing annual security testing, as required under FISMA. Some components indicated during our C&A review that vulnerability scans performed internally or by DHS Security Operations Center had satisfied this requirement.
- Components are not conducting periodic configuration management reviews to evaluate their compliance with DHS baseline settings, citing a lack of resources and tools.
- Weak internal IT controls related to financial management systems were found during the audit of the department's consolidated financial statements for FY 2007.[4] Security concerns included inadequate access controls, application controls, software development, and change controls. Note: POA&Ms have been created for 182 (91%) of 200 NFRs identified during the financial statement audit.

See Appendix I 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.

[3] *Progress Has Been Made But More Work Remains in Meeting Homeland Security Presidential Directive 12 Requirements* (OIG-08-01, October 2007)*; Improved Administration Can Enhance Federal Emergency Management Agency Classified Laptop Computer Security, Unclassified Summary* (Report OIG-08-14, November 2007)*; Lessons Learned from the August 11, 2007, Network Outage at Los Angeles International Airport* (OIG-08-58, May 2008)*; Technical Security Evaluation of U.S. Immigration and Customs Enforcement Activities at the Chet Holifield Federal Building* (OIG-08-59, May 2008), and *Additional Controls Can Enhance the Security of the Automated Commercial Environment System* (OIG-08-64, June 2008).

[4] *Information Technology Management Letter for the FY 2007 DHS Financial Statement Audit* (OIG-08-77, June 2008).

PROGRESS

- DHS' Security Operations Center has performed vulnerability assessment scans at CBP, ICE, and Management.

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 Security Operations Center only has limited access at six components (CBP, FEMA, Federal Law Enforcement Training Center [FLETC], ICE, Management, and United States Citizenship and Immigration Services [USCIS]) to perform vulnerability scans on selected servers and workstations. Furthermore, some components are not submitting vulnerability assessment schedule, or testing results to DHS' Security Operations Center, as required.

See Appendix J for information regarding DHS' incident reporting.

Security Training

DHS validates employee security training at the components. 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 Office of Human Capital implemented a department-wide, web-based learning management system "*DHScovery*." The system can be used to provide standardized security awareness training and track employee completion of that training.
- DHS' Training Office conducts site visits to review and validate training records at the components.

ISSUES TO BE ADDRESSED

- The Training Office has not identified appropriate, specialized security training for employees and contractors with significant IT security responsibilities. While the Training Office validates the specialized training obtained by ISSMs and ISSOs, it relies on the components to ensure that individuals with significant security responsibilities (i.e., system administrators, database administrators, and network administrators, etc.) are properly trained. We reported a similar issue in our FY 2006 and FY2007 FISMA reports.[5]

- DHS does not have policy or procedures regarding the use of Collaborative Web Technologies. In addition, DHS does not educate users on the risks associated with the use of Collaborative Web Technologies during security awareness training.
- DHS contractors do not have access to *DHScovery* or the standardized security awareness training offered by the system.
- Some employees with significant responsibilities (i.e., database and system administrators) did not attain sufficient knowledge to perform their job functions. The results from our configuration review found that some of the administrators could not execute the commands needed to demonstrate whether controls were implemented. Their inability to execute system commands may be related to the fact that the Training Office and components have not determined the appropriate specific specialized security training needed for employees and contractors with significant IT securities responsibilities.

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

Privacy

DHS has established a PIA process. In addition, the Privacy Office continues to refine its PIA guidance. The Privacy Office is experiencing 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.

PROGRESS

- The Privacy Office has issued new policies since our last review. For example, the Privacy Office issued:
  - ➢ Privacy Technology Implementation Guide to aid technology managers and developers integrate privacy protections into operational IT systems.

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

- Privacy Incident Handling Guidance to inform the department's employees, senior officials, and contractors of their obligation to protect personally identifiable information (PII) and how to respond in the event of potential loss or compromise of PII.
- A policy to assist components in completing or preparing Systems of Records and Notices.

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 any users who do not comply with the policy.
- DHS' Privacy Office is experiencing delays in reviewing and approving PIAs. As of July 21, 2008, there were 76 PIAs in various stages of review; 20 of these PIAs had been outstanding for more than 8 months.

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

Recommendations

We recommend that the DHS Chief Information Officer:

Recommendation #1: Improve the OIS' review process to ensure that all POA&Ms, including those POA&M for classified systems, are complete, accurate, and current. The department should consider accepting the risks of the remediation actions for any low priority POA&Ms that have been delayed for more than 12 months.

Recommendation #2: Ensure that components are utilizing the department's C&A tool to generate the most current security document templates with all applicable controls when certifying and accrediting their systems. Systems accredited with outdated templates or without all applicable controls should not be accepted.

Recommendation #3: Improve its process to ensure that DHS baseline configuration requirements are implemented and maintained on all systems. The process should include testing to verify the implementation of DHS baseline configuration settings.

Recommendation #4: Identify the contingency plans for systems with high availability and with alternate processing facilities not operational. The department should consider accepting the risks for the systems with high availability and contingency plans cannot be tested for the reason that the alternate processing facilities are not operational.

Recommendation #5: Expedite the implementation of a department-wide vulnerability assessment program to perform periodic testing to evaluate the security posture at all components.

Recommendation #6: Establish appropriate training that is needed for all individuals with significant security responsibilities to perform their security functions.

Recommendation #7: Ensure the FDCC requirements outlined in OMB M-07-11 and M-07-18 are implemented expeditiously.

We recommend that the DHS Chief Privacy Officer:

Recommendation #8: Establish an escalation process for any PIAs that have been in the review and approval process for an extended period of time.

Recommendation #9: 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 begun the procurement and installation of a system to manage its classified POA&Ms. The department anticipates that this system will be operational by the first quarter of FY 2009.

We agree that the steps DHS plans to take satisfy this recommendation.

DHS concurred with recommendation 2. The department has revised its FY 2009 Information Security Performance Plan to further improve the quality of its C&A process. In addition, revised versions of the DHS C&A document templates will be implemented in the first quarter of FY 2009.

We agree that the steps DHS plans to take satisfy this recommendation.

DHS concurred with recommendation 3. The department has revised its FY 2009 Information Security Performance Plan to include additional reporting requirements regarding configuration management.

We agree that the steps DHS plans to take satisfy this recommendation.

DHS concurred with recommendation 4. DHS has begun to identify the systems with "High Availability" to determine the scope of work associated with the implementation of an alternative processing center across the department.

We agree that the steps DHS plans to take satisfy this recommendation.

DHS concurred with recommendation 5. The DHS Security Operations Center (SOC), in support of the DHS FY09 Information Security Performance Plan, has begun to establish additional metrics to evaluate the visibility needed to implement an effective department-wide Vulnerability Assessment program.

We agree that the steps DHS plans to take satisfy this recommendation.

DHS concurred with recommendation 6. DHS has begun to establish training objectives based on security roles to facilitate a more robust training program for the department. Initially, the department plans to focus on the highest risk security positions.

We agree that the steps DHS plans to take satisfy this recommendation.

DHS concurred with recommendation 7. The department has revised its FY 2009 Information Security Performance Plan to ensure compliance with FDCC requirements. Specifically, DHS has incorporated key FDCC compliance milestones into configuration management metrics. In addition, the criteria for Acquisition Reviews are being updated to incorporate FDCC requirements.

We agree that the steps DHS plans to take satisfy this recommendation.

DHS concurred with recommendation 8. DHS has implemented a weekly report to track the status of the PIAs and system of records notices. With these weekly reports, DHS can determine whether the PIAs and system of records notices are being updated by the components, reviewed by the Privacy Office, General Counsel, and OMB, or have not been assigned.

We agree that the steps DHS plans to take satisfy this recommendation.

DHS concurred with recommendation 9. DHS is working to establish the rules in accordance with OMB M-07-16. The department plans to complete the rules and incorporate them into the PII Handbook by

December 2008. Once the rules are established, the Chief Human Capital Office and General Counsel will be responsible for developing the consequences of non-compliance for system users. Upon completion of both tasks, DHS will develop a training program to educate employees, contractors, and other personnel who may be impacted by the requirement.

We agree that the steps DHS plans to take satisfy this recommendation.

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-08-21, FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, issued on July 14, 2008. We conducted our work at the program level and at DHS' major components: CBP, FEMA, ICE, Management, Operation Coordination, National Protection and Programs Directorate, S&T, TSA, USCIS, USCG, U.S. Visitor and Immigrant Status Indicator Technology, and United States Secret Service (USSS).

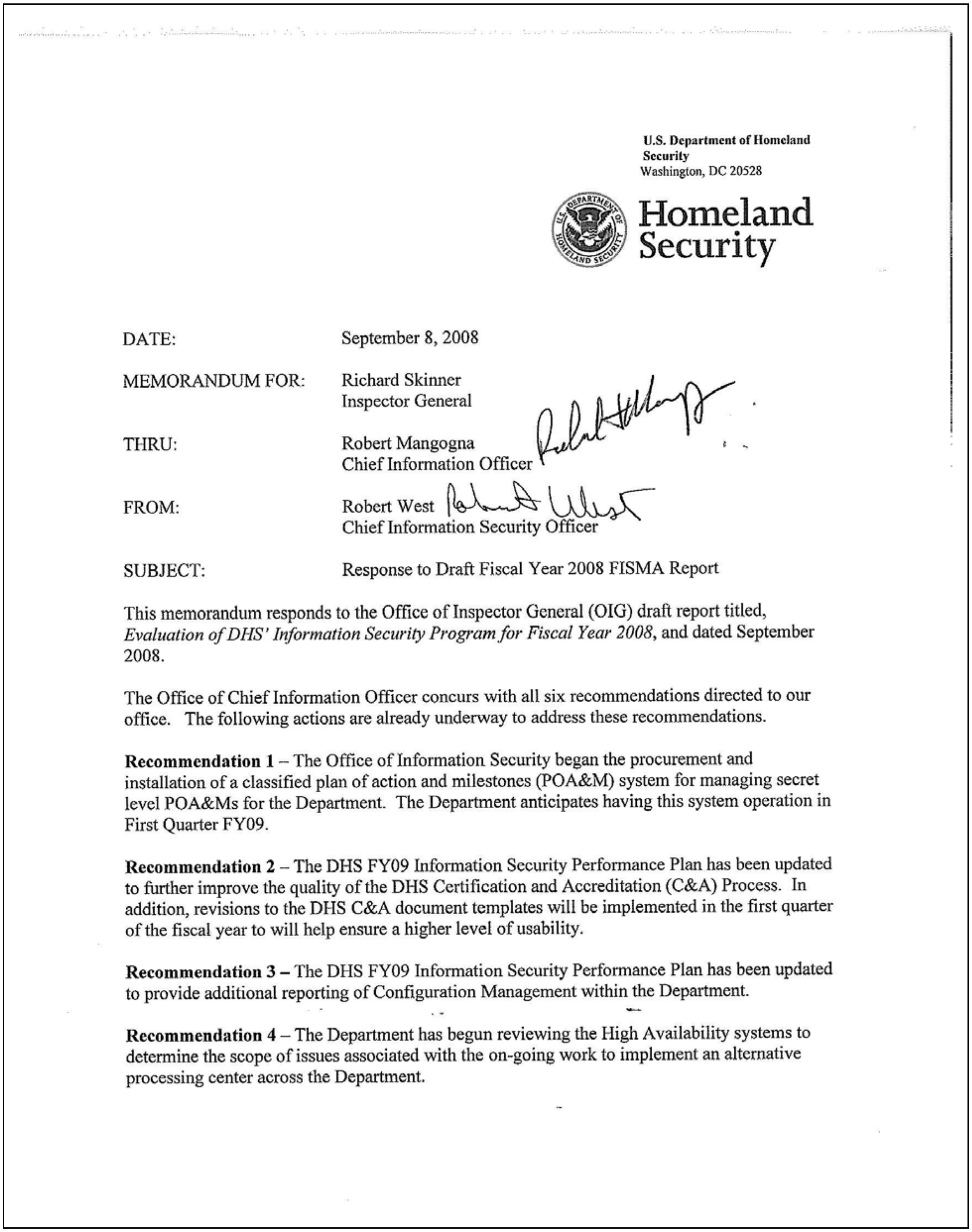
In addition to our independent evaluation, we conducted reviews of DHS' information systems and security program-related areas throughout FY 2008. This report includes the results of a limited number of systems evaluated during the year and our on-going financial statement review, including the Automated Commercial Environment, Automated Targeting System, Chet Holifield Federal Building, and USCG network security 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 the C&A packages for a sample of 25 systems at 12 components and offices: CBP, Management, FEMA, ICE, Operation Coordination, NPPD, S&T, TSA, USCIS, USCG, US-VISIT, 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 28 systems at CBP, FEMA, ICE, Management, TSA, USCG, and USCIS.

We conducted our evaluation between May and August 2008 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

DATE: September 8, 2008

MEMORANDUM FOR: Richard Skinner
Inspector General

THRU: Robert Mangogna
Chief Information Officer

FROM: Robert West
Chief Information Security Officer

SUBJECT: Response to Draft Fiscal Year 2008 FISMA Report

This memorandum responds to the Office of Inspector General (OIG) draft report titled, *Evaluation of DHS' Information Security Program for Fiscal Year 2008*, and dated September 2008.

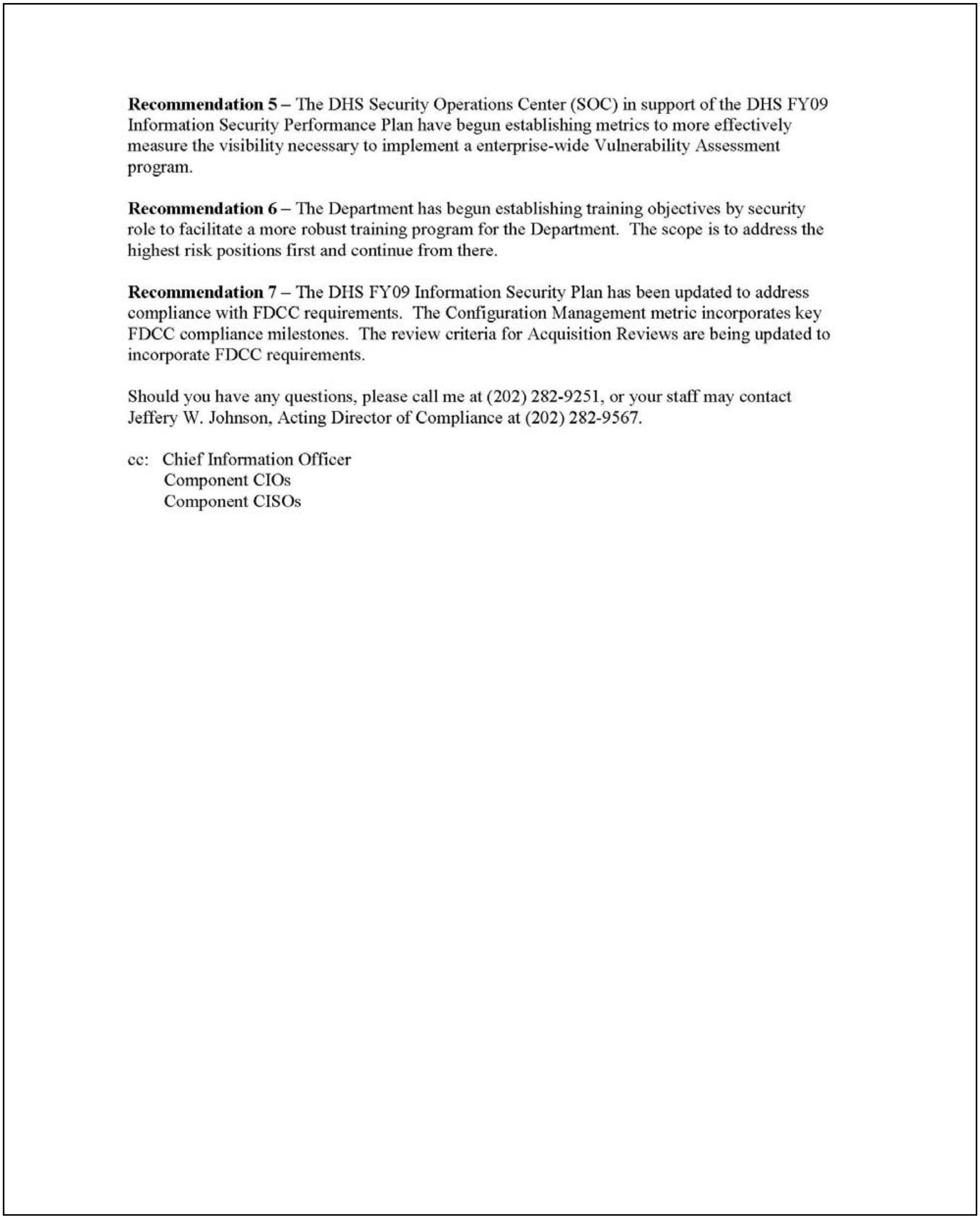
The Office of Chief Information Officer concurs with all six recommendations directed to our office. The following actions are already underway to address these recommendations.

Recommendation 1 – The Office of Information Security began the procurement and installation of a classified plan of action and milestones (POA&M) system for managing secret level POA&Ms for the Department. The Department anticipates having this system operation in First Quarter FY09.

Recommendation 2 – The DHS FY09 Information Security Performance Plan has been updated to further improve the quality of the DHS Certification and Accreditation (C&A) Process. In addition, revisions to the DHS C&A document templates will be implemented in the first quarter of the fiscal year to will help ensure a higher level of usability.

Recommendation 3 – The DHS FY09 Information Security Performance Plan has been updated to provide additional reporting of Configuration Management within the Department.

Recommendation 4 – The Department has begun reviewing the High Availability systems to determine the scope of issues associated with the on-going work to implement an alternative processing center across the Department.



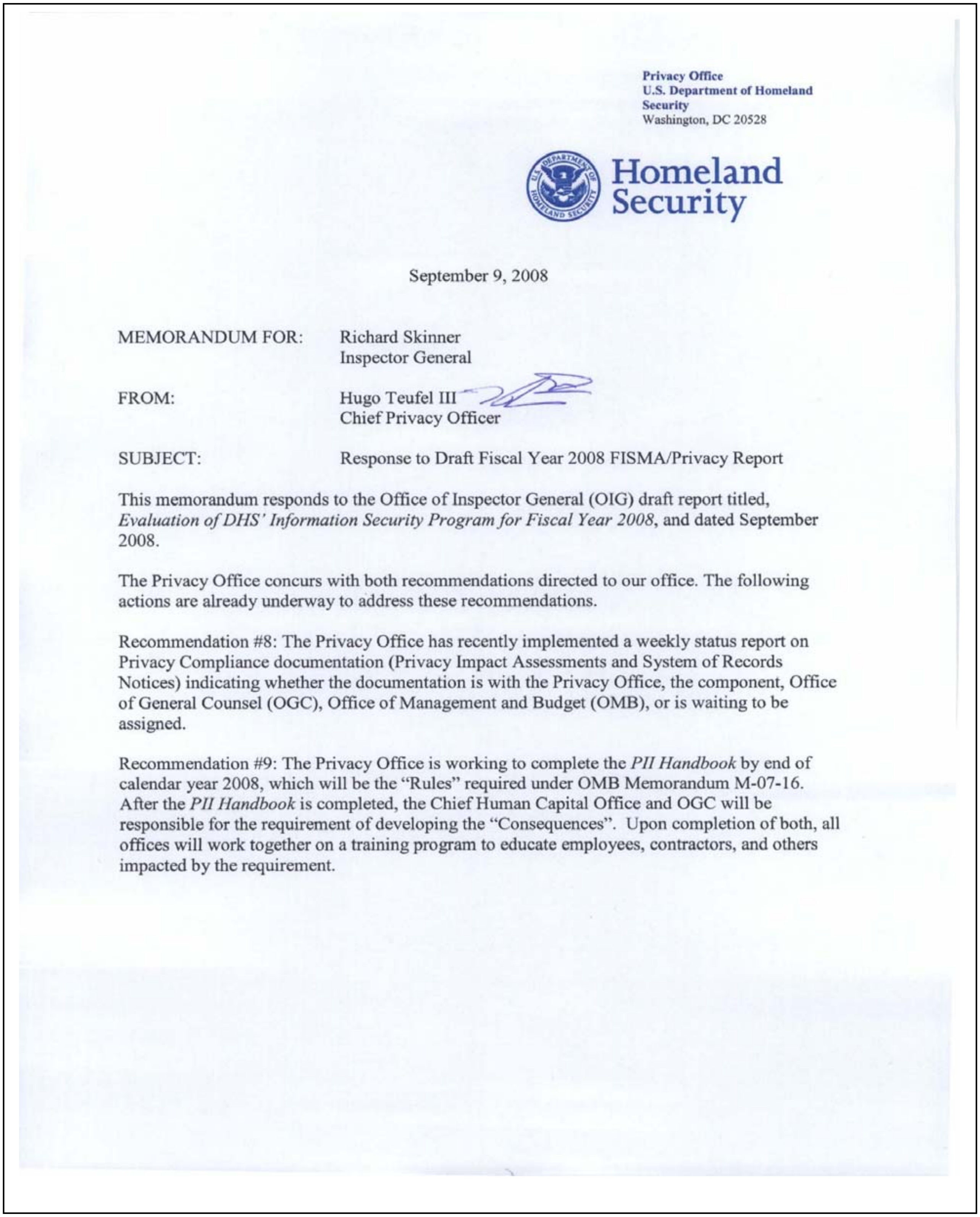
Recommendation 5 – The DHS Security Operations Center (SOC) in support of the DHS FY09 Information Security Performance Plan have begun establishing metrics to more effectively measure the visibility necessary to implement a enterprise-wide Vulnerability Assessment program.

Recommendation 6 – The Department has begun establishing training objectives by security role to facilitate a more robust training program for the Department. The scope is to address the highest risk positions first and continue from there.

Recommendation 7 – The DHS FY09 Information Security Plan has been updated to address compliance with FDCC requirements. The Configuration Management metric incorporates key FDCC compliance milestones. The review criteria for Acquisition Reviews are being updated to incorporate FDCC requirements.

Should you have any questions, please call me at (202) 282-9251, or your staff may contact Jeffery W. Johnson, Acting Director of Compliance at (202) 282-9567.

cc: Chief Information Officer
Component CIOs
Component CISOs



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

Homeland Security

September 9, 2008

MEMORANDUM FOR: Richard Skinner
Inspector General

FROM: Hugo Teufel III
Chief Privacy Officer

SUBJECT: Response to Draft Fiscal Year 2008 FISMA/Privacy Report

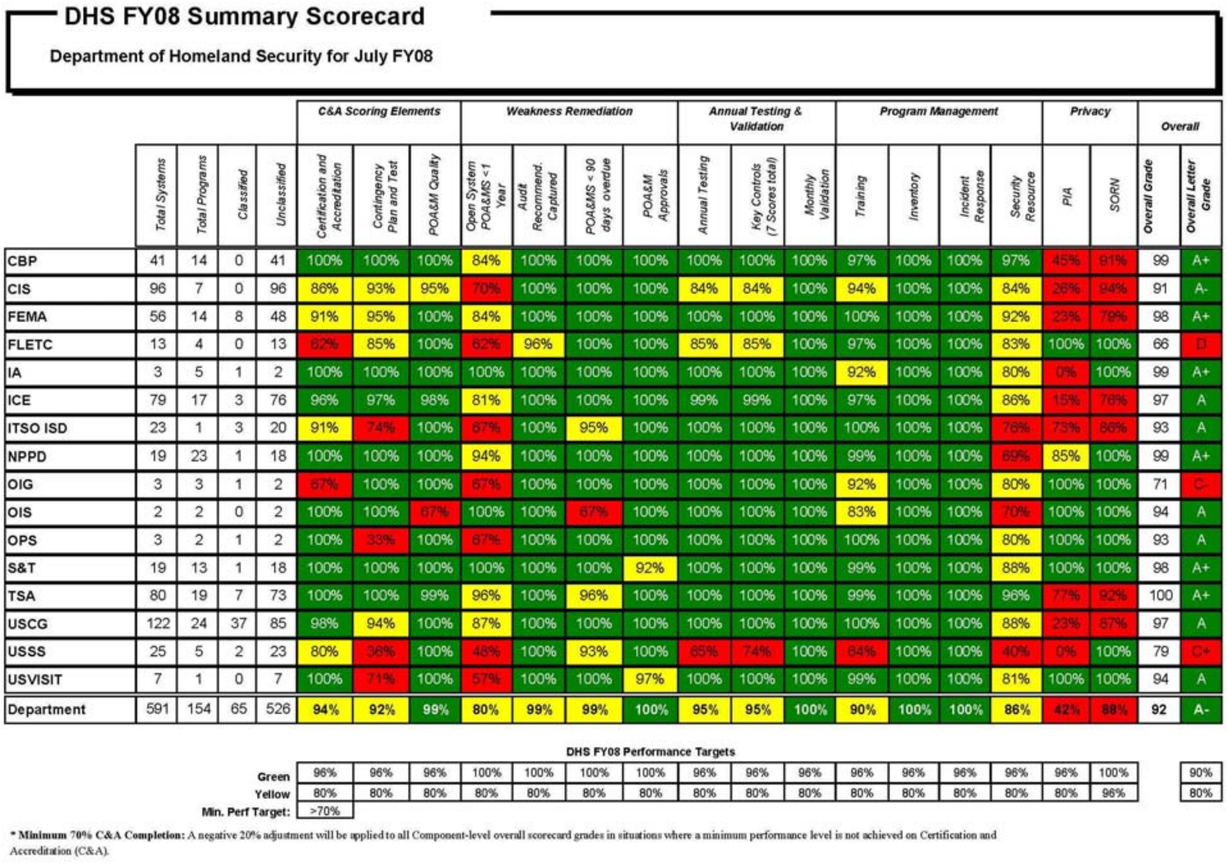
This memorandum responds to the Office of Inspector General (OIG) draft report titled, *Evaluation of DHS' Information Security Program for Fiscal Year 2008*, and dated September 2008.

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

Recommendation #8: The Privacy Office has recently implemented a weekly status report on Privacy Compliance documentation (Privacy Impact Assessments and System of Records Notices) indicating whether the documentation is with the Privacy Office, the component, Office of General Counsel (OGC), Office of Management and Budget (OMB), or is waiting to be assigned.

Recommendation #9: The Privacy Office is working to complete the *PII Handbook* by end of calendar year 2008, which will be the "Rules" required under OMB Memorandum M-07-16. After the *PII Handbook* is completed, the Chief Human Capital Office and OGC will be responsible for the requirement of developing the "Consequences". Upon completion of both, all offices will work together on a training program to educate employees, contractors, and others impacted by the requirement.

Appendix C
FISMA Scorecard and C&A Steady State Scorecard for July 2008



DHS FY08 Summary Scorecard

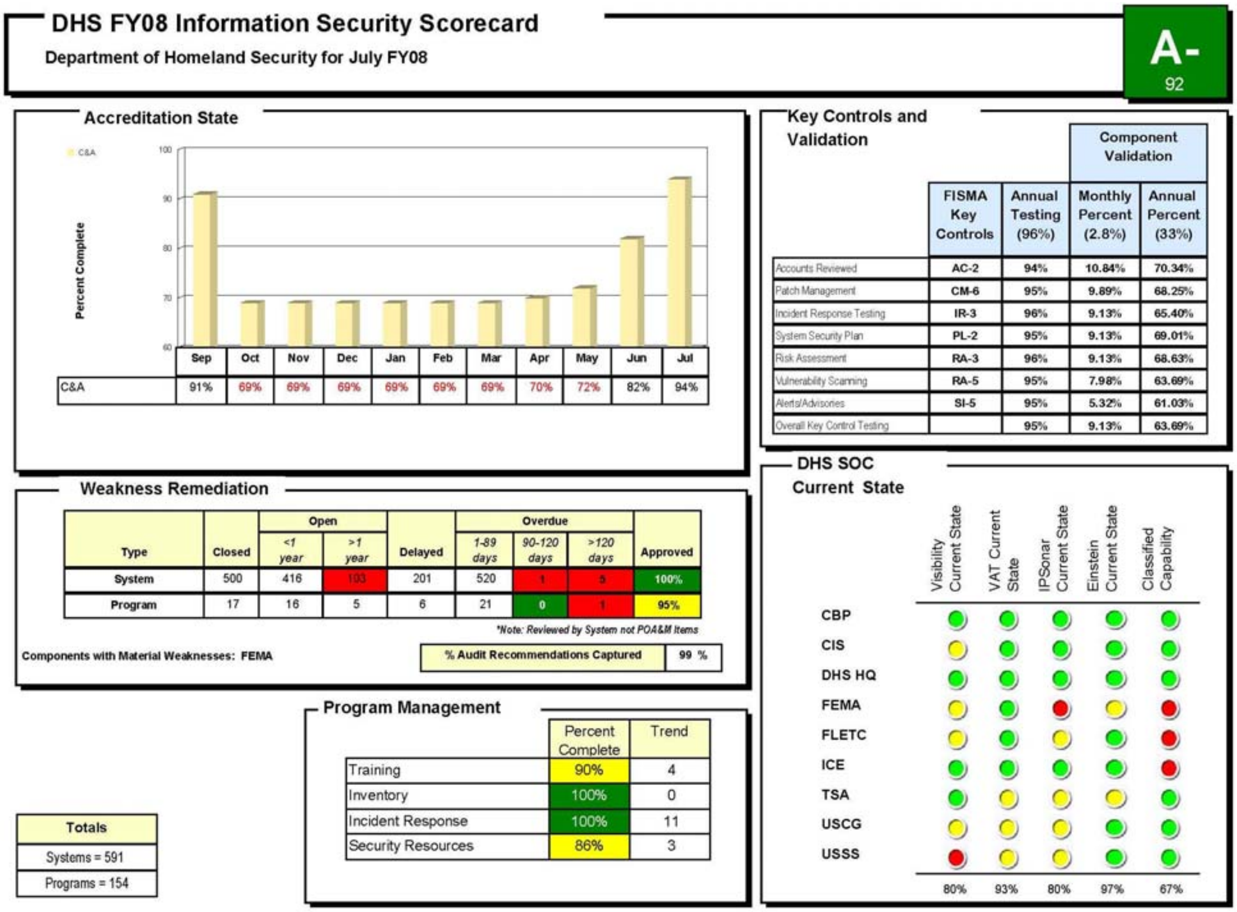
Department of Homeland Security for July FY08

					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	41	14	0	41	100%	100%	100%	84%	100%	100%	100%	100%	100%	100%	97%	100%	100%	97%	45%	91%	99	A+
CIS	96	7	0	96	86%	93%	95%	70%	100%	100%	100%	84%	84%	100%	94%	100%	100%	84%	26%	94%	91	A-
FEMA	56	14	8	48	91%	95%	100%	84%	100%	100%	100%	100%	100%	100%	100%	100%	100%	92%	23%	79%	98	A+
FLETC	13	4	0	13	62%	85%	100%	62%	96%	100%	100%	85%	85%	100%	97%	100%	100%	83%	100%	100%	66	D
IA	3	5	1	2	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	92%	100%	100%	80%	0%	100%	99	A+
ICE	79	17	3	76	96%	97%	98%	81%	100%	100%	100%	99%	99%	100%	97%	100%	100%	86%	15%	76%	97	A
ITSO ISD	23	1	3	20	91%	74%	100%	67%	100%	95%	100%	100%	100%	100%	100%	100%	100%	76%	73%	86%	93	A
NPPD	19	23	1	18	100%	100%	100%	94%	100%	100%	100%	100%	100%	100%	99%	100%	100%	69%	85%	100%	99	A+
OIG	3	3	1	2	67%	100%	100%	67%	100%	100%	100%	100%	100%	100%	92%	100%	100%	80%	100%	100%	71	C-
OIS	2	2	0	2	100%	100%	67%	100%	100%	67%	100%	100%	100%	100%	83%	100%	100%	70%	100%	100%	94	A
OPS	3	2	1	2	100%	33%	100%	67%	100%	100%	100%	100%	100%	100%	100%	100%	100%	80%	100%	100%	93	A
S&T	19	13	1	18	100%	100%	100%	100%	100%	100%	92%	100%	100%	100%	99%	100%	100%	88%	100%	100%	98	A+
TSA	80	19	7	73	100%	100%	99%	96%	100%	96%	100%	100%	100%	100%	99%	100%	100%	96%	77%	92%	100	A+
USCG	122	24	37	85	98%	94%	100%	87%	100%	100%	100%	100%	100%	100%	100%	100%	100%	88%	23%	87%	97	A
USSS	25	5	2	23	80%	36%	100%	48%	100%	93%	100%	65%	74%	100%	64%	100%	100%	40%	0%	100%	79	C+
USVISIT	7	1	0	7	100%	71%	100%	57%	100%	100%	97%	100%	100%	100%	99%	100%	100%	81%	100%	100%	94	A
Department	591	154	65	526	94%	92%	99%	80%	99%	99%	100%	95%	95%	100%	90%	100%	100%	86%	42%	88%	92	A-

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%																

* **Minimum 70% C&A Completion:** A negative 20% adjustment will be applied to all Component-level overall scorecard grades in situations where a minimum performance level is not achieved on Certification and Accreditation (C&A).



DHS FY08 Information Security Scorecard

Department of Homeland Security for July FY08

A-
92

Accreditation State

	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul
C&A	91%	69%	69%	69%	69%	69%	69%	70%	72%	82%	94%

Key Controls and Validation

			Component Validation	
	FISMA Key Controls	Annual Testing (96%)	Monthly Percent (2.8%)	Annual Percent (33%)
Accounts Reviewed	AC-2	94%	10.84%	70.34%
Patch Management	CM-6	95%	9.89%	68.25%
Incident Response Testing	IR-3	96%	9.13%	65.40%
System Security Plan	PL-2	95%	9.13%	69.01%
Risk Assessment	RA-3	96%	9.13%	68.63%
Vulnerability Scanning	RA-5	95%	7.98%	63.69%
Alerts/Advisories	SI-5	95%	5.32%	61.03%
Overall Key Control Testing		95%	9.13%	63.69%

Weakness Remediation

Type	Closed	Open		Delayed	Overdue			Approved
		<1 year	*>1 year*		*1-89 days*	*90-120 days*	*>120 days*	
System	500	416	103	201	520	1	5	100%
Program	17	16	5	6	21	0	1	95%

***Note: Reviewed by System not POA&M Items**

Components with Material Weaknesses: FEMA

% Audit Recommendations Captured	99 %

Program Management

	Percent Complete	Trend
Training	90%	4
Inventory	100%	0
Incident Response	100%	11
Security Resources	86%	3

Totals
Systems = 591
Programs = 154

DHS SOC Current State

	Visibility Current State	VAT Current State	IPSonar Current State	Einstein Current State	Classified Capability
CBP	🟢	🟢	🟢	🟢	🟢
CIS	🟡	🟢	🟢	🟢	🟢
DHS HQ	🟢	🟢	🟢	🟢	🟢
FEMA	🟡	🟢	🔴	🟡	🔴
FLETC	🟡	🟢	🟡	🟢	🔴
ICE	🟢	🟢	🟢	🟢	🔴
TSA	🟢	🟡	🟡	🟡	🟢
USCG	🟡	🟡	🟡	🟢	🟢
USSS	🔴	🟡	🟡	🟢	🟢
	80%	93%	80%	97%	67%

Question 1: FISMA System Inventory

1. As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

In the table below, identify the number of agency and contractor information systems, and the number reviewed, by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized). Extend the worksheet onto subsequent pages if necessary to include all Component/Bureaus.

Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

2. For the Total Number of Systems reviewed by the IG 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)**		**a. Number of systems certified and accredited (a)**		**b. Number of systems for which security controls have been tested and reviewed in the last year**		**c. Number of systems for which contingency plans have been tested in accordance with policy**	
Bureau Name	**FIPS 199 Risk 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		3		0	0	3	3	100%	3	100%	3	100%
	Moderate		6		0	0	6	6	100%	6	100%	6	100%
	Sub-total	**40**	**9**	**1**	**0**	**41**	**9**	**9**	100%	**9**	100%	**9**	100%
CIS	Moderate		5		4	0	9	7	78%	7	78%	7	78%
	Sub-total	**60**	**5**	**36**	**4**	**96**	**9**	**7**	78%	**7**	78%	**7**	78%
FEMA	High		1		2	0	3	3	100%	3	100%	3	100%
	Moderate		2		3	0	5	5	100%	5	100%	5	100%
	Sub-total	**35**	**3**	**21**	**5**	**56**	**8**	**8**	100%	**8**	100%	**8**	100%
FLETC	**Sub-total**	**9**	**0**	**4**	**0**	**13**	**0**	**0**	0%	**0**	0%	**0**	0%
I&A	**Sub-total**	**2**	**0**	**1**	**0**	**3**	**0**	**0**	0%	**0**	0%	**0**	0%
ICE	High		1		0	0	1	1	100%	1	100%	1	100%
	Moderate		3		3	0	6	6	100%	5	83%	6	100%
	Low		0		1	0	1	1	100%	1	100%	1	100%
	Sub-total	**32**	**4**	**47**	**4**	**79**	**8**	**8**	100%	**7**	88%	**8**	100%

		Question 1						**Question 2**					
		a. Agency Systems		**b. Contractor Systems**		**c. Total Number of Systems (Agency and Contractor systems)**		**a. Number of systems certified and accredited (a)**		**b. Number of systems for which security controls have been tested and reviewed in the last year**		**c. Number of systems for which contingency plans have been tested in accordance with policy**	
ITSO ISD	High		2		1	0	3	3	100%	3	100%	3	100%
	Moderate		1		1	0	2	2	100%	2	100%	1	50%
	Sub-total	**9**	**3**	**14**	**2**	**23**	**5**	**5**	100%	**5**	100%	**4**	80%
NPPD	High		0		1	0	1	1	100%	1	100%	1	100%
	Sub-total	**7**	**0**	**12**	**1**	**19**	**1**	**1**	100%	**1**	100%	**1**	100%
OIG	**Sub-total**	**3**	**0**	**0**	**0**	**3**	**0**	**0**	0%	**0**	0%	**0**	0%
OIS	**Sub-total**	**1**	**0**	**1**	**0**	**2**	**0**	**0**	0%	**0**	0%	**0**	0%
OPS	High		1		0	0	1	1	100%	1	100%	1	100%
	Sub-total	**2**	**1**	**1**	**0**	**3**	**1**	**1**	100%	**1**	100%	**1**	100%
S&T	Moderate		0		1	0	1	1	100%	1	100%	1	100%
	Low		0		1	0	1	1	100%	1	100%	1	100%
	Sub-total	**7**	**0**	**12**	**2**	**19**	**2**	**2**	100%	**2**	100%	**2**	100%
TSA	High		1		2	0	3	3	100%	3	100%	3	100%
	Moderate		2		2	0	4	4	100%	4	100%	4	100%
	Low		1		0	0	1	1	100%	1	100%	1	100%
	Sub-total	**51**	**4**	**29**	**4**	**80**	**8**	**8**	100%	**8**	100%	**8**	100%
USCG	High		0		1	0	1	1	100%	1	100%	1	100%
	Moderate		3		2	0	5	5	100%	5	100%	4	80%
	Low		2		1	0	3	3	100%	3	100%	3	100%
	Sub-total	**93**	**5**	**29**	**4**	**122**	**9**	**9**	100%	**9**	100%	**8**	89%
USSS	Moderate		1		0	0	1	1	100%	1	100%	0	0%
	Sub-total	**24**	**1**	**1**	**0**	**25**	**1**	**1**	100%	**1**	100%	0	0%
US-VISIT	Moderate		1		0	0	1	1	100%	1	100%	1	100%
	Sub-total	**1**	**1**	**6**	**0**	**7**	**1**	**1**	100%	**1**	100%	**1**	100%
Agency Totals	**High**	**0**	**9**	**0**	**7**	**0**	**16**	**16**	100%	**16**	100%	**16**	100%
	Moderate	**0**	**24**	**0**	**16**	**0**	**40**	**38**	95%	**37**	93%	**35**	88%
	Low	**0**	**3**	**0**	**3**	**0**	**6**	**6**	100%	**6**	100%	**6**	100%
	Total	**376**	**36**	**215**	**26**	**591**	**62**	**60**	97%	**59**	95%	**57**	92%

Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory		
3.a.	**The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.** Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self-reporting by contractors does not meet the requirements of law. Self-reporting by another federal agency, for example, a federal service provider may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance. Response Categories: - Rarely- for example, approximately 0-50% of the time - Sometimes- for example, approximately 51-70% of the time - Frequently- for example, approximately 71-80% of the time - Mostly- for example, approximately 81-95% of the time - Almost Always- for example, approximately 96-100% of the time	- Almost Always- for example, approximately 96-100% of the time
3.b.	**The agency has developed a complete inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.** Response Categories: - The inventory is approximately 0-50% complete - The inventory is approximately 51-70% complete - The inventory is approximately 71-80% complete - The inventory is approximately 81-95% complete - The inventory is approximately 96-100% complete	- The inventory is approximately 96-100% complete
3.c.	**The IG generally agrees with the CIO on the number of agency-owned systems. Yes or No.**	Yes
3.d.	**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 or No.**	Yes
3.e.	**The agency inventory is maintained and updated at least annually.**	Yes
3.f	**If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please identify the known missing systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the system as presented in your FY2008 Exhibit 53 (if known), and indicate if the system is an agency or contractor system.**	

Component/Bureau	System Name	Exhibit 53 UPI (must be 23-digit)	Agency or Contractor system?

Number of known systems missing from inventory:	

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. Evaluate the degree to which each statement reflects the status in your agency by choosing from the responses provided. If appropriate or necessary, include comments in the area provided.

For each statement in items 4.a. through 4.f., select the response category that best reflects the agency's status.

Response Categories:

- Rarely- for example, approximately 0-50% of the time
- Sometimes- for example, approximately 51-70% of the time
- Frequently- for example, approximately 71-80% of the time
- Mostly- for example, approximately 81-95% of the time
- Almost Always- for example, approximately 96-100% of the time

4.a.	**The POA&M is an agency-wide process, incorporating all known IT security weaknesses 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.**	- Almost Always- for example, approximately 96-100% of the time (a)
4.b.	**When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&M for their system(s).**	- Mostly- for example, approximately 81-95% of the time (b)
4.c.	**Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly).**	- Mostly- for example, approximately 81-95% of the time (c)
4.d.	**Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.**	- Almost Always- for example, approximately 96-100% of the time (d)
4.e.	**IG findings are incorporated into the POA&M process.**	- Mostly- for example, approximately 81-95% of the time (e)
4.f.	**POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.**	- Mostly- for example, approximately 81-95% of the time (f)

POA&M comments:

(a) DHS requires all known IT security weaknesses to be included in DHS' enterprise management tool.

(b) DHS requires components to create POA&M for all IT security weaknesses. However, our review determined that POA&Ms were not created for all identified IT security weaknesses. Specifically, 217 (84%) of 259 of all recommendations cited in OIG audit reports (including Notice of Findings and Recommendations [NFRs]) had corresponding POA&Ms in DHS' enterprise management tool.

(c) DHS components are required to update all information in their POA&Ms at least monthly. Of the 4,245 open POA&M in DHS' enterprise management tool, 491 (12%) have estimated completion dates that are at least three months past due. Furthermore, there are 252 (6%) POA&M that have estimated completion dates that are at least 12 months past due.

(d) The CIO regularly performs quality reviews (automated) on all POA&Ms to ensure that information entered into DHS' enterprise management tool is accurate, reasonable, and complete. In addition, the CIO prepares a monthly report to help monitor the components' progress.

(e) DHS requires all OIG findings be included in each component's POA&M. We determined that 217 (84%) of 259 of all recommendations cited in OIG audit reports (including NFRs) had corresponding POA&Ms in DHS' enterprise management tool.

(f) DHS has prioritized all POA&M (IT security weaknesses) in DHS' enterprise management tool. However, there are 11 significant weaknesses that were reported at seven components. Five of the 11 significant weaknesses were created over 12 months ago (before June 30, 2007). Of these five POA&M, four were scheduled to take more than two years to remediate. In addition, of the 4,245 open POA&M in DHS' enterprise management tool, there are 491 POA&M that are three months past due and 252 POA&M that are 12 months past due. Furthermore, we determined that many of the POA&M are not completed as originally scheduled. For example, our query results determined that 1,978 (47%) out of 4,245 open POA&M have been delayed.

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. Provide narrative comments as appropriate.

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, "Standards for Security Categorization of Federal Information and Information Systems" (February 2004) to determine a system impact level, as well as associated NIST document used as guidance for completing risk assessments and security plans.

5.a.	**The IG rates the overall quality of the Agency's certification and accreditation process as:** Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Good	
5.b	**The IG's quality rating included or considered the following aspects of the C&A process:** (check all that apply)	Security plan	X
		System impact level	X
		System test and evaluation	X
		Security control testing	X
		Incident handling	X
		Security awareness training	X
		Configurations/patching	X
		Other: privacy impact assessment, risk assessment, contingency plan, contingency plan testing, security assessment report	

C&A process comments:

(a) DHS has implemented a good C&A process. DHS uses a department-wide tool that incorporates NIST security controls to certify and accredit all systems. The CIO requires all components to use this tool. Components are required to apply NIST SP 800-53 security controls for all system certifications. However, for many systems, the artifacts that are required to certify and accredit a system were either missing or incomplete. Our review of 25 C&A packages at 12 components and offices found two instances in which accreditation packages were incomplete. In addition, we identified that other systems were accredited, though some key security documents were missing information that is required to meet all applicable DHS, OMB, and NIST guidelines.

Question 6-7: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process

6. **Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D Question #5 (SAOP reporting template), including adherence to existing policy, guidance, and standards.** Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Good

Comments:

DHS has established a PIA process. The Privacy Office requires a privacy threshold analysis (PTA) for all systems to determine whether a PIA is needed. PTAs are specifically developed to identify which systems in the DHS information systems inventory collect or use personally identifiable information (PII), which systems require a PIA, and which need a Privacy Act System of Records Notice. The PIA guidance provides information on when a PIA must be conducted, how associated analysis should be performed, and how the PIA document should be written. Further, the Privacy Office continues to refine its policies since our last review, such as Privacy Technology Implementation Guide (PTIG), and Privacy Incident Handling Guidance (PIHG).

The Privacy Office has a backlog in reviewing and approving PIAs. As of July 21, 2008, there were 76 PIAs in various stages of review.

7. **Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-07-16, "*Safeguarding Against and Responding to the Breach of Personally Identifiable Information*".** Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Satisfactory

Comments:

DHS has implemented the majority of M-07-16 requirements. For example, the Privacy Office has issued a breach notification policy, developed an implementation plan to eliminate the unnecessary collection and use of social security numbers, and drafted a plan to review and to reduce holding of PII.

DHS has not outlined the consequences of non-compliance in its rules of behavior.

	Question 8: Configuration Management	
8.a.	**Is there an agency-wide security configuration policy? Yes or No.**	Yes
	Comments: DHS has included in its agency-wide policy a requirement that all components ensure that the installation of hardware and software products meet requirements specified in applicable DHS secure baseline configuration guides. DHS has developed configuration guides for all major hardware and software systems being used by its components.	
8.b.	**Approximate the extent to which applicable information systems implement security configurations available from the National Institute of Standards and Technology's website at http://checklists.nist.gov.** **Response categories:** - Rarely- for example, approximately 0-50% of the time - Sometimes- for example, approximately 51-70% of the time - Frequently- for example, approximately 71-80% of the time - Mostly- for example, approximately 81-95% of the time - Almost Always- for example, approximately 96-100% of the time	See comment (a)
8c	**Indicate which aspect of Federal Desktop Core Configuration (FDCC) have been implemented as of this report**:	
	c.1 Agency has adopted and implemented FDCC standard Configuration and has documented deviations. **Yes or No**	No (b)
	c.2 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 or No	No (c)
	c.3 All Windows XP and VISTA computing systems have implemented the FDCC security settings. Yes or No.	No (d)

Comments:

(a) Many of the components use standard configurations for their systems, but have not fully implemented DHS' baseline configuration guides. As part of our C&A and configuration reviews, we identified that DHS' baseline configuration settings have not been fully implemented on all of the systems selected. Results of vulnerability assessments during the fiscal year have identified additional security concerns, including inadequate password controls and patches that had not been installed.

(b) DHS is in the process of documenting deviations from FDCC settings.

(c) DHS is in the process of drafting its standard FDCC contract language for all IT acquisitions.

(d) DHS cannot implement the settings on its Windows XP and Vista desktops and laptops until the department completes documenting deviations from FDCC.

Question 9: Incident sReporting

Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided below.

9.a.	**The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.**	Yes
9.b.	**The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov)**	Yes
9.c.	**The agency follows documented policies and procedures for reporting to law enforcement. Yes or No.**	Yes

Comments:

Question 10: Security Awareness Training	
Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities? Response Categories: - Rarely- or approximately 0-50% of employees - Sometimes- or approximately 51-70% of employees - Frequently- or approximately 71-80% of employees - Mostly- or approximately 81-95% of employees - Almost Always- or approximately 96-100% of employees	- Mostly, or, approximately 81-95% of employees
Comments: The Training Office is validating components' training data to ensure that the components provide IT security awareness training to their employees. The Training Office has not determined what training is needed for individuals with significant IT security responsibilities (including network, database, and system administrators).	

Question 11: Collaborative Web Technologies and Peer-to-Peer File Sharing	
A. Does the agency explain policies regarding the use of collaborative web technologies in IT security awareness training, ethics training, or any other agency-wide training? Yes or No.	No
B. Does the agency explain policies regarding the use of peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training? Yes or No.	Yes

Question 12: E-Authentication Risk Assessments	
12. a. Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with the NIST Special Publication 800-63, "Electronic Authentication Guidelines"? Yes or No.	Yes (a)
12.b. If the response is "No", then please identify the systems in which the agency has not implemented the e-authentication guidance and indicate if the agency has a planned date of remediation.	

(a) We sampled 23 systems that were reported as E-Authentication applications in DHS' enterprise management tool to determine whether the assessments were properly completed and applicable controls were implemented. For example, we found nine systems were reported incorrectly as E-Authentication applications in DHS' enterprise management tool, when compared to the determination. As such, DHS may not have an accurate inventory of its E-Authentication systems. In addition, 4 of the 14 E-Authentication systems had inconsistent assurance levels reported in DHS' enterprise management tool when compared to the source documents. Only one of the 14 E-Authentication systems properly addressed the DHS and NIST required controls in the system test and evaluation plans and security assessment reports for the assigned E-Authentication assurance levels.

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
Charles Twitty, IT Auditor
Kristina Hayden, Program Analyst
Nazia Khan, IT Specialist
Thomas Rohrback, IT Specialist
Peter Spano, Management/Program Assistant
Meghan Sanborn, Referencer

Advanced Technology Division

John Molesky, Information Security Engineer
Jordan Dixon, Information Security Engineer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Assistant Secretary for Legislative 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
Director, Privacy Compliance
Chief Information Officer Audit Liaison
Chief Information Security Officer Audit Liaison
Privacy Office Audit Liaison
Component CIOs
Component ISSMs

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, call the Office of Inspector General (OIG) at (202) 254-4199, 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.