

DEPARTMENT OF HOMELAND SECURITY
Office of Inspector General

Evaluation of DHS' Information Security
Program for Fiscal Year 2007



Office of Inspector General

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

SEP 27 2007



**Homeland
Security**

Preface

The Department of Homeland Security (DHS) Office of Inspector General 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 employees and officials of DHS, direct observations, and a review of applicable documents.

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.

A handwritten signature in black ink, appearing to read "Richard L. Skinner".

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Executive Summary	1
Background.....	2
Results of Independent Evaluation	3
Recommendations.....	13
Management Comments and OIG Analysis	13

Appendices

Appendix A:	Purpose, Scope, and Methodology.....	15
Appendix B:	Management Response to Draft Report.....	17
Appendix C:	FISMA Scorecard and C&A Steady State Scorecard for July 2007.....	22
Appendix D:	FY 2007 Monthly Component FISMA Scorecard Grades	25
Appendix E:	FISMA System Inventory and Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing	26
Appendix F:	Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory.....	28
Appendix G:	Evaluation of Agency Plan of Action and Milestones Process.....	29
Appendix H:	IG Assessment of the Certification and Accreditation Process	30
Appendix I:	IG Assessment of Agency Privacy Program and Privacy Impact Assessment Process	31
Appendix J:	Configuration Management	32
Appendix K:	Incident Reporting	33
Appendix L:	Security Awareness Training, Peer-to-Peer File Sharing, and E-Authentication Risk Assessments	34
Appendix M:	Major Contributors to this Report.....	35
Appendix N:	Report Distribution	36

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
CONOPS	Concept of Operations
DHS	Department of Homeland Security
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
NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
OIG	Office of Inspector General
OIS	Office of Information Security
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PTA	Privacy Threshold Analysis
S&T	Science and Technology
SP	Special Publication
TSA	Transportation Security Administration
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Services
USSS	United States Secret Service
US-VISIT	United States Visitor and Immigrant Status Indicator Technology



Department of Homeland Security
Office of Inspector General

Executive Summary

We conducted an independent evaluation of the Department of Homeland Security's information security program and practices to comply with the Office of Management and Budget's reporting requirements noted in the *Federal Information Security Management Act of 2002* (Public Law 107-347, Section 301-305). We evaluated the department's progress in implementing its agencywide information security program. In doing so, we specifically assessed the department's Plan of Action and Milestones, as well as its certification and accreditation processes. We performed our work at both the program and the component levels.

The department continues to improve and strengthen its security program. During the past year, the department implemented a performance plan to measure the component's progress toward full compliance with its information security program. The performance plan tracks key elements indicative of a strong, functioning security program. Monthly, the department's Chief Information Officer and Chief Information Security Officer report on and discuss component progress. Despite this oversight, components are again not executing all of the department's policies, procedures, and practices. For example:

- Systems are being accredited without key documents or missing key information.
- Plans of Action and Milestones are not being created for all information security weaknesses.
- Plans of Action and Milestones are not being monitored and resolved in a timely manner.
- Baseline security configurations are not being implemented for all systems.

Management oversight of the component's implementation of the department's policies and procedures needs to be improved to ensure the quality of the certification and accreditation process and that all information security weaknesses are tracked and remediated. Other information security program areas that need improvement include security configuration management, incident detection and analysis, and security training.

We are making five recommendations to the Chief Information Officer. The department has already begun to take actions to implement the recommendations. 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, 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.

The *E-Government Act of 2002* (Public Law 107-347, Sections 301-305) recognized the importance of information security to the economic and national security interests of the United States. 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 agencywide 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 assessments 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.

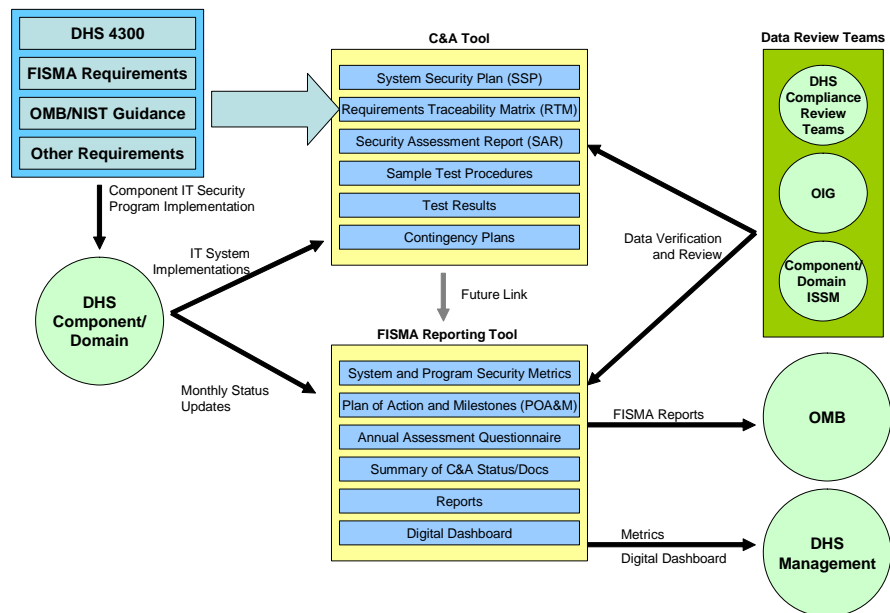
OMB issued memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, on July 25, 2007. The memorandum provides updated instructions for agency and OIG reporting under FISMA. This annual evaluation summarizes the results of our review of the Department of Homeland Security's (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 Plan of Action and Milestones (POA&Ms). In addition, DHS uses an enterprise management tool, Trusted Agent FISMA, to collect and track data related to all POA&M activities, including weaknesses identified during self-assessments, and certification and accreditation (C&A). Trusted Agent

FISMA also collects data on other FISMA metrics, such as the number of systems that have implemented DHS security configurations and the number of employees who have received information technology (IT) security training.

DHS also uses an enterprise C&A tool, Risk Management System, to automate and standardize portions of the C&A process to assist the DHS components in quickly and efficiently developing their security accreditation packages. See Figure 1 for an illustration on how the enterprise management and C&A tools are used within the department to collect, manage, and report information security metrics.

Figure 1: DHS' Enterprise Security Management Tools Usage



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) 2006 evaluation and those issues that need to be addressed to be successful in the FISMA area.

Department Oversight

DHS validates and monitors component progress through a verification process and a monthly FISMA scorecard. Improvements are needed in the level of oversight and the metrics being used to monitor component progress.

PROGRESS

- The CISO developed the *Fiscal Year 2007 DHS Information Security Performance Plan “Raising the Bar”* to hold the components to a higher C&A process standard, improve the POA&M process, close high-priority weaknesses, and require components to achieve full FISMA compliance.
- The CISO developed a FISMA scorecard to manage the component’s compliance with the performance plan. The FISMA scorecard provides the Chief Information Officer (CIO), the CISO, component CIOs, and component Information System Security Managers (ISSM) with an overview of each component’s compliance with six FISMA elements. The FISMA elements include annual testing, POA&M, C&A, configuration management, incident detection and response, and IT security training. See Appendix C for an example of the FISMA scorecard.
- Throughout the year, the CISO revised the department’s baseline IT security policies and procedures in the *DHS Sensitive Systems Policy Directive 4300A* and its companion, *DHS 4300A Sensitive Systems Handbook*.
- DHS issued its *DHS Security Operations Concept of Operations* (CONOPS) in May 2007. The CONOPS defines the security operations for the DHS Security Operations Center and subordinate component security operation centers. The CONOPS established the roles and responsibilities of the DHS Security Operations Center as the central reporting and coordinating body for computer security incidents.
- The CISO implemented a data review and verification process of the component performance information entered into Trusted Agent FISMA, including C&A artifacts, POA&Ms, configuration management, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 self-assessments, and IT security training.
- The CIO has taken an active role in ensuring that components comply with FISMA. The CIO sent memorandums to the leaders of four components (Federal Emergency Management Agency (FEMA), Infrastructure Operations, United States Coast Guard (USCG), and United States Citizenship and Immigration Services (USCIS)) in April 2007 voicing his concern over the status of their FISMA compliance. The CIO requested immediate attention to complete the required areas that were in need of improvement, for example, C&A, annual self-assessments, and POA&M management.

ISSUES TO BE ADDRESSED

- Certain metrics in the performance plan, used by the CISO to grade the components, need improvement in order to better reflect the true state of FISMA compliance. Areas include closure and completeness of POA&Ms, implementation and review of configuration management plans, and quality of annual testing. See Appendix D for FY 2007 grades assigned by the CISO.
- The OIS validation team does not ensure that all key C&A artifacts are completed prior to validating an Authority To Operate (ATO) letter. The team also does not ensure that POA&Ms are created for weaknesses identified in the ATO letter and other key C&A artifacts.
- The OIS validation team does not analyze POA&Ms and discuss with system officials to determine the reasonableness of delayed completion of POA&Ms or identify recurring and similar weaknesses across the department.
- The OIS validation team does not review classified systems' POA&Ms.

System Inventory

DHS maintains its system inventory. Site visits during annual component reviews help identify systems that have not been included in the department's system inventory.

PROGRESS

- DHS continues to maintain a comprehensive inventory of its major applications and general support systems, including contractor and national security systems. DHS identified 603 operational systems (as of July 31, 2007).
- DHS continues to maintain an effective process to update and manage its inventory on an annual basis for agency, contractors, and classified systems by reviewing the system inventory with each component.

ISSUES TO BE ADDRESSED

- Site visits to component offices outside the Washington D.C. area are not being performed during the annual system inventory reviews. Site visits can be used to determine if there are any systems that are not known by the ISSM and that should be included in the inventory.

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 requires components to use an enterprise-wide tool that incorporates NIST security controls to conduct their C&As. Components are required to apply NIST SP 800-53 security controls for all system certifications and self-assessments. For many 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, many of the self-assessments were not being properly completed by the components.

PROGRESS

- The CISO requires components to apply NIST SP 800-53 security controls for all system certifications and when completing annual self-assessments.
- DHS uses 11 C&A artifacts, uploaded into Trusted Agent FISMA by the components, to monitor their progress in accrediting systems. As of July 31, 2007, the CISO reported that 84% of DHS' operational systems (530/603) have been certified and accredited. The 11 artifacts are: 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), and NIST SP 800-53. A total of 68 of the 73 systems that have not been accredited belong to one component.

ISSUES TO BE ADDRESSED

- 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. We selected 28 systems with current ATOs spanning 10 components to evaluate the quality of DHS' C&A process. In 17 instances, the accreditation packages were incomplete. Specifically, systems were accredited, although some 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. For example:
 - Eight instances where system security plans were incomplete, including sections that describe detailed configuration management plans, security controls, and incident handling procedures.
 - Eleven instances where a description of the use of automated vulnerability assessment tools were not addressed.

-
- Eleven instances where the effectiveness of controls were not addressed.
 - Five instances where contingency plans were incomplete, including the identification of alternate processing facilities or restoration procedures.
 - Eight instances where there was no system test and evaluation plan or it was incomplete.
 - Three instances where there was no security assessment report or the results of the test were not in the security assessment report.
- As of July 31, 2007, 16 systems that were accredited were lacking at least one of three critical artifacts: risk assessment, system security plan, or security assessment report. Six of the 16 lacked all three of these required artifacts.
 - As of July 31, 2007, 83 systems were accredited for 1 year or less, including 23 for 6 months or less. We believe systems accredited for 6 months or less are in effect interim ATOs and should not be considered in calculating the number of systems that DHS has accepted as accredited.
 - We selected 33 systems spanning 13 components to evaluate the quality of completed NIST SP 800-53 self-assessments. We determined whether there was a compliance description for all applicable controls; supporting documentation for all controls that had been tested; justification for any controls that were not applicable (N/A); and that a POA&M was created for all required controls that had not been tested. For 21 self-assessments, there was no compliance description or supporting documentation for one or more controls that were not tested. For 11 self-assessments, there was no justification for not reviewing one or more of the required security controls.
 - During an OIG audit at FEMA (*Improved Administration Can Enhance Federal Emergency Management Agency Laptop Computer Security*, dated June 2007, OIG-07-50), we determined that its laptop computers had not been certified and accredited. FEMA had not included its approximately 32,000 laptops as part of any system.
 - The CIO identifies systems to be accredited if an ATO letter has been validated. We believe that systems with missing or deficient key C&A artifacts and systems with an ATO of 6 months or less should not be included in the number of systems the department reports as certified and accredited. Based on our reviews, the actual number of systems that should be accepted as being certified and accredited should be no higher than 486 (81% rather than the 84% reported by the CISO).

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

Plan of Action and Milestones Process

DHS components are required to use Trusted Agent FISMA to capture and track security weaknesses. The components are not entering and tracking all IT security weaknesses in Trusted Agent FISMA nor are all of the data entered by the components accurate and updated in a timely manner.

PROGRESS

- DHS conducts monthly reviews of POA&Ms for completeness and monitors the closure rate for initial and repeat audit findings. The findings are reported to OIS and components.
- POA&Ms have been created for all weaknesses identified during the FY 2006 financial statement audit.

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.
 - Three components (FEMA, National Protection and Programs Directorate (NPPD), and Science and Technology (S&T)) did not create POA&Ms for findings identified in OIG audit reports issued during FY 2007.
 - We selected 33 systems where components reported that a NIST SP 800-53 self-assessment had been completed. When a control has not been tested and the weakness is not accepted based on a risk-based decision, a POA&M should be created to remediate the weakness. In 24 instances, POA&Ms were not created for controls that were not tested.
 - We selected 28 systems, spanning 10 components, with current ATOs to evaluate the quality of the C&A documentation. In 10 instances, POA&Ms were not created for weaknesses identified during the C&A process.
- Based on an analysis of data in Trusted Agent FISMA, as of July 5, 2007, the ISSMs and ISSOs are not maintaining current information as to the progress of security weakness remediation.
 - Component management is not updating all weaknesses when the estimated completion date had been delayed. Of the 5,342 open POA&Ms that had estimated completion dates, 480 (9%) were at least 3 months past due (prior to April 5, 2007). Further, 277 had

an estimated completion date over 1 year old, dating as far back as September 30, 2005.

- Components are required to provide reasons why a POA&M is delayed. As of July 5, 2007, 1,510 of 2,074 open POA&Ms identified as delayed did not have a reason.
- Resources required remediation for 387 of the 5,342 open POA&Ms (7%) were not identified or listed the cost of remediation as \$1. For the remaining 4,955 POA&Ms that included required resources, 296 (6%) did not specify the funding sources.
- Effective March 1, 2007, components were required to assign one of the 17 NIST SP 800-53 families of controls to each weakness. As of July 5, 2007, only 441 of the 2,179 open POA&Ms (20%) created after March 1, 2007 had a NIST SP 800-53 control assigned.
- Effective March 1, 2007, ISSMs were required 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. In addition, any weakness can be assigned to priority 4 or priority 5 by management. As of July 5, 2007, 148 of 150 priority 4 and priority 5 POA&Ms created after March 1, 2007 were not approved.
- Not all POA&Ms are being resolved in a timely manner, including weaknesses identified as a significant deficiency.
 - As of July 5, 2007, 1,447 of 5,342 open POA&Ms (27%) reported estimated completion dates that were more than 2 years after the identification of the weakness.
 - As of July 5, 2007, there were 38 open weaknesses defined as significant deficiencies. Seven POA&Ms were created over the 12 previous months. 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.

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

Configuration Management

DHS has updated its baseline software security configuration guides and are to be followed by the components when configuring their systems. A review of four systems identified that the components have not implemented all of the required software security configurations.

PROGRESS

- DHS updated its agencywide security baseline configuration guides for Windows NT/2000/2003/XP/Vista/Active Directory, Solaris, Unix, Linux, Cisco Routers, Microsoft SQL server, and Oracle database servers in May 2007.

ISSUES TO BE ADDRESSED

- Components have not fully implemented NIST SP 800-53 baseline security controls, including DHS baseline security configuration requirements, for all of their systems. Our review of four systems at two components, FEMA and United States Immigration and Customs Enforcement (ICE), in which the component reported that DHS security configurations had been implemented, disclosed that NIST SP 800-53 baseline security controls had not implemented for their systems. NIST controls that had not been implemented included those associated with access control, audit and accountability, configuration management, identification and authentication, and system and information integrity.
- The CIO does not have a verification process to validate whether components have implemented DHS baseline configuration requirements.
- Vulnerability assessments performed at components during our laptop, Plum Island Animal Disease Center, Ronald Reagan Washington National Airport, and Dulles International Airport 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 United States Customs and Border Protection (CBP), FEMA, S&T, Transportation Security Administration (TSA), and USCG.¹

¹ *Improved Administration Can Enhance U.S. Customs and Border Protection Laptop Computer Security*, dated December 2006 (OIG-07-16); *Technical Security Evaluation of DHS Activities at Dulles International Airport*, dated January 2007 (OIG-07-25); *Additional Physical, System, and Management Controls Can Enhance Security at Plum Island*, dated May 2007 (OIG-07-43); *Technical Security Evaluation of DHS Activities at Ronald Reagan Washington National Airport*, dated May 2007 (OIG-07-44); *Improved Administration Can Enhance Federal Emergency Management Agency Laptop Computer Security*, dated June 2007 (OIG-07-50).

-
- Weak internal IT controls related to financial management systems were found during the audit of the department's financial statement for FY 2006.² Security concerns included inadequate access controls, application controls, and software development and change controls. Note: POA&Ms have been created for each of the weaknesses identified.

See Appendix J for information regarding DHS' configuration management.

Incident Detection, Handling, and Analysis Procedures

DHS has improved its incident detection, handling, and analysis procedures during the last year and began performing vulnerability assessments at some components. However, the department has not fully implemented the vulnerability assessment program across the department.

PROGRESS

- DHS issued the *DHS Security Operations Concept of Operations* in May 2007.
- DHS developed detailed procedures for reporting incidents externally to law enforcement authorities.
- The DHS Computer Security Incident Response Center developed detailed procedures for reporting incidents to the United States Computer Emergency Readiness Team (US-CERT).
- DHS developed procedures to perform department-wide security incident monitoring, analysis, and notification. The DHS Security Operations Center has begun to issue security event notifications to components.
- DHS Security Operations Center has performed vulnerability assessment scans at CBP, FEMA, and DHS headquarters.

ISSUES TO BE ADDRESSED

- DHS' vulnerability assessment program has not been deployed department-wide. The program should be a comprehensive vulnerability alert, assessment, remediation, and reporting process to effectively identify computer security vulnerabilities and track mitigation efforts to resolution.
- Some components are not reporting incidents to the DHS Computer Security Incident Response Center, as required. Components are required to submit weekly incident reports. Five components - FEMA, Federal

² *Information Technology Management Letter for the FY 2006 DHS Financial Statement Audit*, dated August 2007 (OIG-07-53).

Law Enforcement Training Center (FLETC), ICE, OIG, and USCIS - did not submit reports every week during an 11-week period that we reviewed.

See Appendix K for information regarding DHS' incident reporting.

Security Training Procedures

DHS validates employee security training at the components. The Information Security Training, Education, and Awareness Office (Training Office) has not determined specific training that is needed for employees with significant security responsibilities.

PROGRESS

- The Training Office validates specialized security training for individuals identified by the components with significant IT security responsibilities.

ISSUES TO BE ADDRESSED

- DHS (CIO and Office of Human Capital) has not implemented a department-wide web-based IT security training program (learning management system) to standardize security awareness training and to track the completion of security training. The learning management system was originally planned to be implemented in FY 2004; but it was pushed back to FY 2007. Currently, the plan is to launch the system by the end of September 2007 for DHS headquarters employees only. The system is expected to be fully functional (available to all components) by September 2009. We reported a similar issue in our FY 2006 FISMA report.
- The Training Office has not established appropriate specialized security training that is needed for all 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 (including system administrators, database administrators, and network administrators, etc.) are properly trained. We reported a similar issue in our FY 2006 FISMA report.
- Some of the components' training plans were incomplete, as they did not include all of the required information and approvals. For example, seven training plans were not approved by the ISSM, seven plans did not include the number of employees and contractors who need training, and nine plans did not include the number of information systems security employees.

-
- Two components did not submit FY 2007 training plans.

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

Recommendations

We recommend that the DHS CIO:

Recommendation #1: Improve the OIS' review process to ensure that all POA&Ms, including classified systems, are complete, accurate, and current. Specifically, the closure for all POA&Ms should be monitored by OIS to ensure that security weaknesses are mitigated timely. POA&Ms should also be reviewed by OIS to identify the causes for recurring and similar weaknesses across the department and determine the reasonableness of delayed completion.

Recommendation #2: Improve the OIS' review process to ensure that all C&A documents are properly prepared before a system is accepted by the CISO as an accredited system. Systems accredited by the Designated Accrediting Authority should not be accepted unless all required artifacts are complete and weaknesses are incorporated into POA&Ms.

Recommendation #3: Establish a process to ensure that configuration requirements are implemented and maintained on all systems.

Recommendation #4: Implement a department-wide vulnerability assessment program to perform periodic testing to evaluate DHS' security posture.

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

Management Comments and OIG Analysis

DHS concurred with recommendation 1. The department significantly improved component POA&M oversight in FY 2007. The department's FY 2008 performance plan will incorporate additional requirements to address classified systems and unreasonable POA&M delays.

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

DHS concurred with recommendation 2. The department achieved significant improvements in producing key accreditation documentation in FY 2007. The department's FY 2008 performance plans will incorporate additional requirements to address artifact completeness and further identify weaknesses in POA&Ms.

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

DHS concurred with recommendation 3. The department's FY 2008 performance plan will incorporate additional requirements to address a monitoring process for configuration requirements at the system level, and for validating that components are completing annual vulnerability scans.

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

DHS concurred with recommendation 4. The DHS Security Operations Center has begun performing component vulnerability assessments and will continue to perform them in FY 2008.

We agree that the steps DHS has taken, and plans to take satisfy this recommendation.

DHS concurred with recommendation 5. The department provides specialized training at its DHS Security Conference. The department's FY 2008 performance plan will incorporate additional requirements to track individuals and establish appropriate training.

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-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, issued on July 25, 2007. We conducted our work at the program level and at DHS' major components: CBP, DHS Management, FEMA, FLETC, ICE, OIG, NPPD, S&T, TSA, USCG, USCIS, 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 2007. This report includes results of a limited number of systems evaluated during our past and on-going financial statement review, laptop security, Plum Island Animal Disease Center, and technical evaluations at two airports 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 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 agencywide 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 28 systems and 33 NIST SP 800-53 self-assessments at 13 components: CBP, DHS Management, FEMA, FLETC, ICE, NPPD, OIG, S&T, TSA, USCG, USCIS, USSS, and United States Visitor and Immigrant Status Indicator Technology (US-VISIT), to ensure that all of the required documents were completed prior to being accredited.

We conducted our evaluation between June and August 2007 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 M.

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 Audits Division at (202) 254-5444.

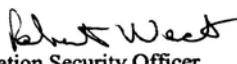
U.S. Department of Homeland
Security
Washington, DC 20528



**Homeland
Security**

September 19, 2007

MEMORANDUM FOR: Richard Skinner
Inspector General

FROM: Robert West 
Chief Information Security Officer

SUBJECT: Response to Draft Fiscal Year 2007 FISMA Report

This memorandum responds to the Office of Inspector General (OIG) draft report titled, *Evaluation of DHS' Information Security Program for Fiscal Year 2007*, Dated September 2007.

The Chief Information Security Officer (CISO) response is comprised of two attachments:

- A. Response to OIG Recommendations
- B. Response to OIG Report to the Office of Management and Budget (OMB)

Should you have any questions, please call me at (202) 282-9251, or your staff may contact Wayne Bavry, Director of Compliance at (202) 282-9506.

cc: Chief Information Officer
Component CIOs
Component ISSMs

(2) Attachments as stated

Recommendation 1: *Improve the OIS' review process to ensure that all POA&Ms, including classified systems, are complete, accurate, and current. Specifically, the closure for all POA&Ms should be monitored by OIS to ensure that security weaknesses are mitigated timely. POA&Ms should also be reviewed by OIS to identify the causes for recurring and similar weaknesses across the department and determine the reasonableness of delayed completed.*

OCIO Response

Concur. The Department significantly improved Component POA&M oversight for SBU Systems in FY07. The Department provided monthly scorecards for POA&Ms that focused on completeness, as well as closure of new and repeat audit findings. DHS reviewed the status of POA&Ms for 527 (83 %) systems and programs at least on a monthly basis. POA&M scorecards were distributed to the Information System Security Managers (ISSM) and detailed completeness reports were distributed to Component POA&M managers every month. In FY07, 88% of audit findings were incorporated into a POA&M. As of August 1, 2007 all open POA&Ms for SBU systems were prioritized in accordance with guidance contained in DHS 4300A Attachment H. As noted by the OIG, the Department also worked with Components to ensure POA&Ms were developed for all weaknesses identified in financial statement audits. The Department's FY08 Performance Plan will incorporate additional requirements to address classified systems and unreasonable POA&M delays.

Recommendation 2: *Improve the OIS' review process to ensure that all C&A documents are properly prepared before a system is accepted by the CISO as an accredited system. Systems accredited by the Designated Accrediting Authority should not be accepted unless all required artifacts are complete and weaknesses are incorporated into POA&Ms.*

OCIO Response

Concur. While the formal authority to accredit a system relies in the hands of the Designated Accrediting Authority (DAA), OIS has 1) established metrics to monitor Component C&A compliance, and 2) published criteria which raised the bar in FY07 to ensure C&A documents met departmental standards. As illustrated in the following table, the Department has achieved significant improvements in producing key accreditation documentation:

Key Accreditation Documentation	FY 2005	FY 2006	FY 2007
C&A	43%	85%	84% ¹
Controls Testing	52%	87%	96%
Contingency Plan Testing	9%	60%	84%

The Department's FY08 Performance Plan will incorporate additional requirements to address artifact completeness and further identify test weaknesses in POA&Ms.

¹ One Component failed to provide completed C&A packages for 26% of their systems. This significantly reduced the Department's total for accredited systems. The DHS CIO directed the Component CIO to increase compliance. The Component CIO affected a management personnel change, in the middle of the FISMA reporting cycle, and Component improvements are expected in FY08.

Recommendation 3: *Establish a process to ensure that configuration requirements are implemented and maintained on all systems.*

OCIO Response

Concur. In FY07, OIS deployed a compliance team to review configuration management (CM) processes at a Component level. The completion of these on-site reviews was incorporated into the Component's FY07 CM scorecard. The reviews focused on assessing Component-wide practices, usage of DHS configuration guides, as well as the Component's change management and continuous monitoring processes. The Department's FY08 Performance Plan will incorporate additional requirements to address a monitoring process for configuration requirements at the system level, and for validating Components are completing annual vulnerability scans.

Recommendation 4: *Implement a department-wide vulnerability assessment program to perform periodic testing to evaluate DHS' security posture.*

OCIO Response

Concur. As noted by the OIG, the DHS Security Operations Center (SOC) is currently performing Component vulnerability assessments.

Recommendation 5: *Establish appropriate training that is needed for all individuals with significant security responsibilities.*

OCIO Response

Concur. In FY07, OIS reviewed all major Component training plans and 94% of the plans were compliant with DHS requirements. At the 2007 DHS Security Conference eleven (11) tracks were presented to focus specialized training:

#	Track Title	DHS 2007 Security Conference / Training Topics (65)
1	Introductory ISSO Roles and Responsibilities	Introduction/Security Basics Certification and Accreditation Overview NIST SP 800-60 & FIPS 199 Classification System Security Plan Introduction IT Security Risk Assessment Introduction Understanding NIST 800-53 DHS C&A Artifacts ISAs, MOUs, and SLAs
2	Experienced ISSO Roles and Responsibilities	Integrating Security into the SDLC Continuous Monitoring POA&M Process Management DHS FISMA Systems Inventory Methodology
3	C&A for Designated Accreditation Authorities (DAAs) and Program Managers	Certification and Accreditation Overview Risk Assessment Processes for DAAs and PMs SCI System Certification and Accreditation
4	DHS Security Management Tools	RMS Introduction TAF Introduction 508 Accessibility Requirement for TAF POA&M Development and Management Using TAF RMS Advanced Training TAF 800-53 Support (Reports and Data Integrity) Security Management Tools Laboratory

Appendix B
 Management Response to Draft Report

#	Track Title	DHS 2007 Security Conference / Training Topics (65)
5	IT Security for CFO Designated Financial Systems	IT Audit Management Methodology: Process and Procedures Roles and Responsibilities for IT General Controls Assessing Managerial and Operational Controls 4300A Requirements and TAF Procedures for Key Controls New Requirements for Testing Key Controls Testing Key Controls for Effectiveness Evaluating IT Control Exceptions and Their Impact on a Federal Financial Statement Audit Financial System NFR Management and Scorecards
6	Security Essentials	Online/Offline Privacy Social Engineering Techniques Using Portable Electronic Devices Security Personal Password Management
7	Information Security Policy and Architecture	Operating System and Equipment Hardening Guidance DHS Security Architecture, Volume 3 Update DHS Security Policy 4300 Update Federal Regulations and Guidance Updates
8	Security Assessments	Overview of NIST SP 800-53A Assessing Managerial and Operational Controls Assessment: Lessons Learned Wireless Security Penetration and Prevention Assessing Microsoft Windows Assessing UNIX Assessing Network Devices (Routers, Switches, Firewalls)
9	Identity Management	e-Passport Public Key Directory Validation Service Reader Solution Identity Management 101 Directories and Identity Management Using SSO and HSPD-12 Technologies in Your Environment External Facing DHS Identify Management Initiatives Smart Card Basics – Standards, Logical Access, Physical Access Biometrics Basics
10	Operations and Security	DHS Network Security and Infrastructure Vulnerability Testing Laboratory Sys Admin vs the Hacker – Securing Windows 2003 DHS SOC Capabilities and Responsibilities Insider Threat and Information Security Security Operations Center (SOC) Online Training
11	Privacy	Privacy Incident Response Privacy Documentation: PIAs, PTAs, SORNs Privacy Technical Requirement Guidelines Privacy Policy Guidance Using New Technologies to Enforce Privacy Policy

Conference briefings are published on the DHS OCISO home page for year-round access. This training is the basis for defining DHS specific curriculum requirements. The Department's FY08 Performance Plan will incorporate additional requirements to address the OIG recommendations to track individuals and establish appropriate training, based on DHScovery as well as Security Line of Business support for platform / device training for systems, databases and networks.

OIG Reporting to OMB		
OIG Ref	Description	OCISO Response
Appendix E Certification and Accreditation		
Question 2a	Number of Systems certified and accredited (a).	For consistency, the C&A Table "Percent of Total" column should reflect both totals: 74% / 48% as shown in the "Total Number" column.
Question 2a	Comment.	The Department does require all systems to have all artifacts in place at the time of accreditation.
Appendix G Evaluation of Plan of Action and Milestone (POA&M) Process		
Question 4d	Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	The OIG comment regarding the review of classified POA&Ms represents only 12% of the total number of systems at DHS, which indicates 88% compliance. This score should be changed from Frequently, 71-80% to Mostly, 81%-95% of the time. The new "delay reasonableness" criteria identified by the OIG, as a recommendation for future improvement, should not be used to further reduce the overall score based on the current practice of monthly reviews.
Question 4f	POA&M process prioritizes IT security weakness to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	The CIO Office does prioritize security weaknesses. The priority in FY07 was to address specific audit and recurring findings (Priority 4 and Priority 5). The OIG comments for deficiencies which in many cases were rated lower at Priority 3 and Priority 2 is valid but does not reflect that the priority on such weaknesses were lower but implemented. This score should be changed from Mostly, 85-91% of the time to Almost always, 96-100% of the time.

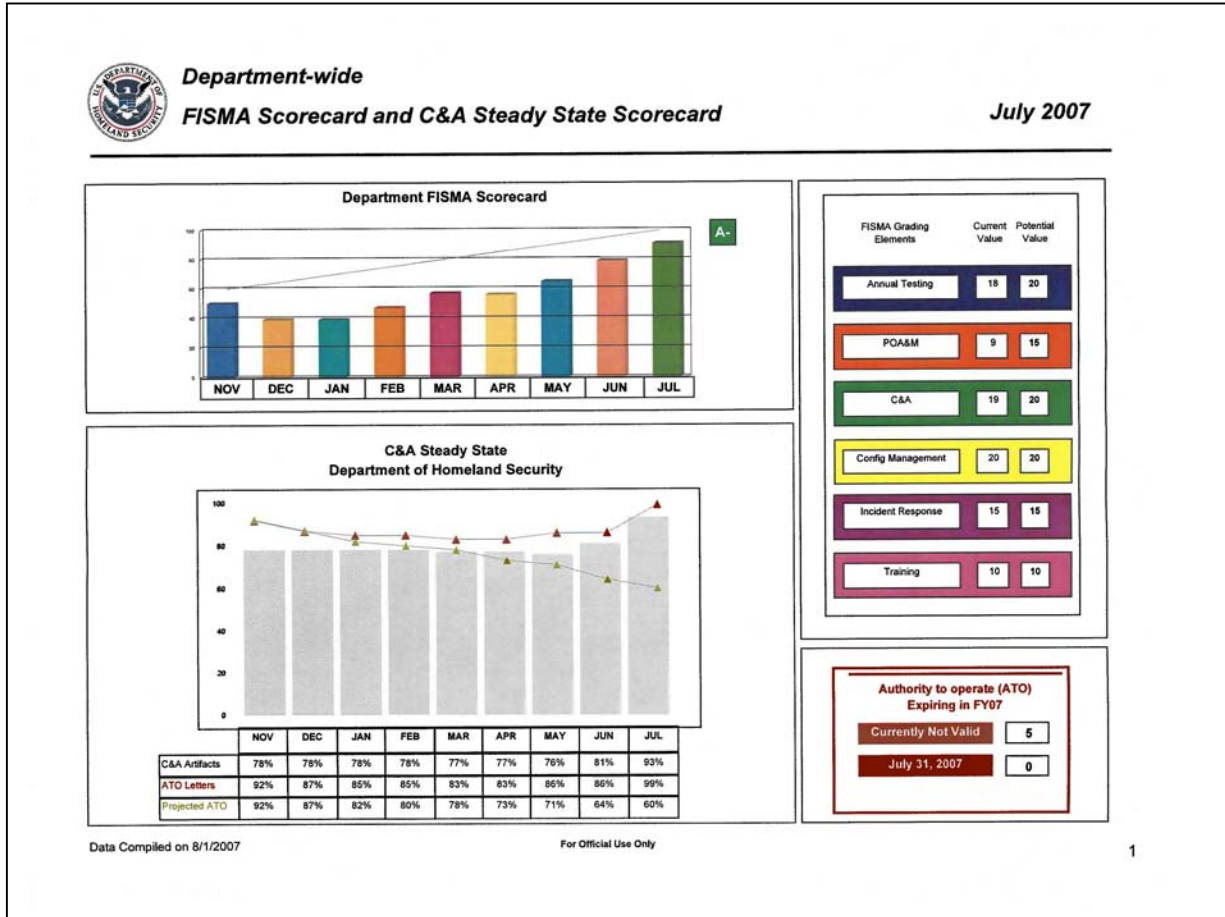
OIG comments:

Question 2a: We are only showing the percent of systems reviewed that we believe should be considered accredited.

Question 4d: Since the review of POA&M activities is a factor, we considered the lack of POA&M review for reasonableness and recurring weaknesses in determining our score.

Question 4f: Since the reason for prioritizing weaknesses is to address them in a timely manner, we factored in the lack of timely resolution of significant weaknesses in determining our score.

Appendix C
 FISMA Scorecard and C&A Steady State Scorecard for July 2007



Appendix C
 FISMA Scorecard and C&A Steady State Scorecard for July 2007



**Department-Wide
 FISMA Scorecard and C&A Steady State Scorecard**

July 2007

	Systems			FISMA Grading Elements						Overall Grading	
	Unclass	Class	Total	Annual Test	POAAM	C&A	Config Mgt	Incident Rep	Training	Total	Grade
CBP	43	0	43	13	8	19	20	15	10	85	B
CIS	93	0	93	20	11	20	20	15	9	95	A
FEMA	45	8	56	18	7	19	20	15	10	89	B+
FLETC	11	0	11	18	6	20	20	15	10	89	B+
IA	2	1	3	20	15	20	20	15	8	96	A
ICE	86	12	98	18	15	19	20	15	10	97	A
INF	16	3	19	20	13	17	20	15	9	94	A
INPPD	16	1	17	20	13	20	20	15	10	98	A+
OIG	2	1	3	6	12	16	20	15	10	79	C+
OPS	2	1	3	20	15	20	20	15	10	100	A+
S&T	18	2	20	20	15	20	20	15	10	100	A+
TSA	62	9	71	20	15	20	20	15	10	100	A+
USCG	84	39	123	20	11	20	20	15	10	96	A
USSS	33	2	35	20	15	20	20	15	9	99	A+
USVISIT	8	0	8	18	15	17	20	15	10	95	A
Department	524	79	603	19	9	19	20	15	10	91	A
			Target	20	15	20	20	15	10	100	

Data Compiled on 8/1/2007

For Official Use Only

2

Appendix C
 FISMA Scorecard and C&A Steady State Scorecard for July 2007



**Department-Wide
 FISMA Scorecard and C&A Steady State Scorecard**

July 2007

Component	POA&M Quality								Priority 5 Closure <i>Includes Repeat Audit Findings</i>				Priority 4 Closure <i>Includes Initial Audit Findings</i>				Total
	Number		Passed			%	Score	5 Points		%		4 Points		Score	15 Points		
	Total	Sys	Prog	Total	Sys	Prog		Total	Closed	Closed	Score	Total	Closed			Closed	Score
CBP	45	43	2	45	43	2	100%	6	26	18	69%	1	53	40	75%	1	8
CIS	76	75	1	74	74	0	97%	6	0	0	100%	5	16	3	19%	0	11
FEMA	44	43	1	42	41	1	95%	4	29	17	59%	1	78	71	91%	2	7
FLETC	10	9	1	8	8	0	80%	1	0	0	100%	5	45	11	24%	0	6
IA	2	2	0	2	2	0	100%	6	0	0	100%	5	0	0	100%	4	15
ICE	86	80	6	86	80	6	100%	6	0	0	100%	5	14	14	100%	4	15
INF	20	18	2	18	16	2	90%	4	0	0	100%	5	4	4	100%	4	13
NPPD	18	17	1	16	15	1	89%	4	0	0	100%	5	0	0	100%	4	13
OIG	2	2	0	2	2	0	100%	6	0	0	100%	5	6	4	67%	1	12
OPS	1	1	0	1	1	0	100%	6	0	0	100%	5	0	0	100%	4	15
S&T	16	16	0	16	16	0	100%	6	0	0	100%	5	0	0	100%	4	15
TSA	66	61	5	64	59	5	97%	6	13	13	100%	5	101	101	100%	4	15
USCG	75	72	3	75	72	3	100%	6	40	36	90%	3	99	94	95%	2	11
USSS	37	33	4	37	33	4	100%	6	0	0	100%	5	10	10	100%	4	15
USVISIT	9	8	1	9	8	1	100%	6	0	0	100%	5	12	12	100%	4	15
Department	507	480	27	495	470	25	98%	6	108	84	78%	1	438	364	83%	2	9

Required Scores - July 2007								
POA&M Quality	Percentage Points		Priority 5 Closure	Percentage Points		Priority 4 Closure	Percentage Points	
Greater than	95%	6	Greater than	95%	5	Greater than	95%	4
Greater than	80%	4	Greater than	80%	3	Greater than	80%	2
Greater than	70%	1	Greater than	50%	1	Greater than	50%	1
Less than or = to	70%	0	Less than or = to	50%	0	Less than or = to	50%	0

Data Compiled on 8/1/2007

For Official Use Only

3

Appendix D
 FY 2007 Monthly Component FISMA Scorecard Grades

Federal Information Security Management Act Monthly Scorecards for DHS Components

Component Name	November '06	December '06	January '07	February '07	March '07	April '07	May '07	June '07	July '07
CBP	F	F	F	C-	C	B	B+	A-	B
CIS	F	F	F	F	F	F	F	F	A
FEMA	F	F	D	F	C+	C	C+	B-	B+
FLETC	F	F	C-	C-	A-	A-	A-	B	B+
IA	F	F	F	D-	D	D	B+	A	A
ICE	F	F	F	C-	D	C	C+	A	A
Infrastructure	F	F	F	D	D	A-	A	A-	A
NPPD	F	C-	C-	B-	B	A	A	A	A+
OIG	F	F	B	C+	C+	B-	B-	C	C+
OPS	F	F	C-	A-	A	A-	A	A	A+
S&T	F	F	F	B-	B	B-	A	A-	A+
TSA	B+	A	A	A	A	A	A	A	A+
USCG	F	F	F	F	F	F	F	C	A
USSS	F	F	F	D-	B-	C+	B-	B-	A+
US-VISIT	F	F	C+	A	A-	A	A	A	A-

Appendix E

FISMA System Inventory and Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

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		3	3/2	67%	3	100%	2	67%
	Moderate		3		0		3	3/2	67%	3	100%	2	67%
	Low		1		0		1	1	100%	1	100%	1	100%
	Sub-total	41	7	2	0	43	7	7/5	71%	7	100%	5	71%
USCIS	Moderate		6		12		18	4/2	11%	6	33%	17	94%
	Low		0		2		2	1	50%	1	50%	2	100%
	Sub-total	59	6	34	14	93	20	5/3	15%	7	35%	19	95%
FEMA	High		8		0		8	7/5	63%	7	88%	4	50%
	Moderate		0		1		1	1/0	0%	1	100%	0	0%
	Not Categorized		2		0	0	2	0	0%	0	0%	0	0%
	Sub-total	38	10	18	1	56	11	8/5	45%	8	73%	4	36%
FLETC	Moderate		3		0		3	3	100%	3	100%	2	67%
	Low		1		0		1	1/0	0%	1	100%	0	0%
	Sub-total	9	4	2	0	11	4	4/3	75%	4	100%	2	50%
IA	Sub-total	3	0	0	0	3	0	0	0%	0	0%	0	0%
Oper Coord	Sub-total	2	0	1	0	3	0	0	0%	0	0%	0	0%

Appendix E

FISMA System Inventory and Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

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
ICE	High		3		1		4	4/3	75%	3	75%	4	100%
	Moderate		3		2		5	4/3	60%	5	100%	2	40%
	Low		1		1		2	2	100%	2	100%	2	100%
	Sub-total		40	7	58	4	98	11	10/8	73%	10	91%	8
Infrastructure	High		0		1		1	1/0	0%	1	100%	1	100%
	Moderate		1		1		2	2	100%	2	100%	1	50%
	Sub-total		5	1	14	2	19	3	3/2	67%	3	100%	2
NPPD	High		1		1		2	2/1	50%	2	100%	1	50%
	Moderate		1		2		3	3/2	67%	3	100%	3	100%
	Low		0		1		1	1/0	0%	1	100%	0	0%
	Sub-total		6	2	11	4	17	6/3	50%	6	100%	4	67%
OIG	High		1		0		1	1	100%	1	100%	1	100%
	Sub-total		3	1	0	0	3	1	100%	1	100%	1	100%
S&T	Moderate		4		0		4	3	75%	3	75%	2	50%
	Low		1		2		3	1	33%	1	33%	1	33%
	Sub-total		11	5	9	2	20	7	4	57%	4	57%	3
TSA	High		0		1		1	1	100%	1	100%	1	100%
	Moderate		0		1		1	1	100%	1	100%	1	100%
	Low		0		1		1	1	100%	1	100%	1	100%
	Sub-total		47	0	24	3	71	3	3	100%	3	100%	3
USCG	High		2		0		2	2/0	0%	2	100%	1	50%
	Moderate		3		1		4	3/1	25%	4	100%	2	50%
	Low		1		0		1	1/0	0%	1	100%	1	100%
	Sub-total		96	6	27	1	123	7	6/1	14%	7	100%	4
USSS	High		2		0		2	2/1	50%	2	100%	1	50%
	Moderate		1		0		1	1/0	0%	1	100%	0	0%
	Sub-total		34	3	1	0	35	3	3/1	33%	3	100%	1
US-VISIT	Low		0		1		1	1	100%	1	100%	0	0%
	Sub-total		2	0	6	1	8	1	100%	1	100%	0	0%
Agency Totals	High	136	20	58	4	194	24	23/14	58%	22	92%	16	67%
	Moderate	210	25	118	20	328	45	42/19	42%	32	71%	32	71%
	Low	49	5	31	8	80	13	11/7	54%	10	77%	8	62%
	Not Categorized	1	2	0	0	1	2	0	0%	0	0%	0	0%
	Total	396	52	207	32	603	84	62/40	48%	64	76%	56	67%

Comments: (a) Per CISO procedures, the number of systems certified and accredited is based on a validated ATO letter, not on the adequacy of the documents required. If in our determination, the systems should not have been accredited based upon the quality of the artifacts, the revised number is shown next to the original total. The percent of total is based on the OIG's count of systems accredited.

Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory	
In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.	
<p>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.</p> <p>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.</p> <p>Response Categories:</p> <ul style="list-style-type: none"> - 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 	<p>- Almost Always- for example, approximately 96-100% of the time ^(a)</p>
<p>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.</p> <p>Response Categories:</p> <ul style="list-style-type: none"> - 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 	<p>- Approximately 96-100% complete</p>
<p>3.c. The IG generally agrees with the CIO on the number of agency-owned systems. Yes or No.</p>	<p>Yes</p>
<p>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.</p>	<p>Yes</p>
<p>3.e. The agency inventory is maintained and updated at least annually.</p>	<p>Yes</p>

Comments:

(a) DHS requires contractor systems to be evaluated in the same manner as agency owned systems. As of July 31, 2007, NIST SP 800-53 self-assessments have been performed for all operational contractor systems. This response is a result of DHS' reported performance metrics. The OIG has not evaluated the quality of assessments performed.

Question 4: Evaluation of Agency Plan of Action and Milestones (POA&M) Process	
<p>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.</p> <p>For each statement in items 4.a. through 4.f., select the response category that best reflects the agency's status.</p> <p>Response Categories:</p> <ul style="list-style-type: none"> - 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.	<p>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.</p> <p style="text-align: right;">- Almost Always, for example, approximately 96-100% of the time ^(a)</p>
4.b.	<p>When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).</p> <p style="text-align: right;">- Sometimes, for example, approximately 51-70% of the time ^(b)</p>
4.c.	<p>Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly).</p> <p style="text-align: right;">- Mostly- for example, approximately 81-95% of the time ^(c)</p>
4.d.	<p>Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.</p> <p style="text-align: right;">- Sometimes, for example, approximately 51-70% of the time ^(d)</p>
4.e.	<p>IG findings are incorporated into the POA&M process.</p> <p style="text-align: right;">- Mostly, for example, approximately 81-95% of the time ^(e)</p>
4.f.	<p>POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.</p> <p style="text-align: right;">- Mostly- for example, approximately 81-95% of the time ^(f)</p>
<p>POA&M process comments:</p> <p>(a) DHS requires all known IT security weaknesses be included in Trusted Agent FISMA.</p> <p>(b) DHS requires components to create POA&Ms for all IT security weaknesses. However, there were instances during our review of the C&A process and NIST SP 800-53 self-assessments where POA&Ms were not created for all weaknesses identified or controls not tested. In addition, many of the POA&Ms did not contain all required information, such as resources required for remediation.</p> <p>(c) DHS components are required to update all information in their POA&Ms at least monthly. However, as of July 5, 2007, 9% of open POA&Ms had estimated completion dates that were at least 3 months past due (prior to April 5, 2007), including 277 that had estimated completion dates more than 1 year old.</p> <p>(d) The CIO conducts monthly reviews of the POA&Ms for status and completion and issues reports to the components. However, the CIO does not review POA&Ms for classified systems and does not analyze POA&Ms to determine the reasonableness of delayed completion of POA&Ms or identify recurring or similar weaknesses across the department.</p> <p>(e) DHS requires all OIG findings be included in each component's POA&M. We determined that 88% of findings were incorporated into a POA&M.</p> <p>(f) DHS prioritizes its IT security weaknesses. However, 7 of 38 open significant weaknesses (18%) were created more than 12 months ago and 8 of the 38 (21%) did not have resources identified.</p>	

Question 5: IG Assessment of the Certification and Accreditation Process																		
<p>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.</p> <p>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.</p>																		
<p>The IG rates the overall quality of the Agency's certification and accreditation process as:</p> <p>5.a. Response Categories:</p> <ul style="list-style-type: none"> - Excellent - Good - Satisfactory - Poor - Failing 	<p>- Satisfactory ^(a)</p>																	
<p>The IG's quality rating included or considered the following aspects of the C&A process: (check all that apply)</p> <p>5.b.</p>	<table border="1"> <tr><td>Security plan</td><td style="text-align: center;">X</td></tr> <tr><td>System impact level</td><td style="text-align: center;">X</td></tr> <tr><td>System test and evaluation</td><td style="text-align: center;">X</td></tr> <tr><td>Security control testing</td><td style="text-align: center;">X</td></tr> <tr><td>Incident handling</td><td style="text-align: center;">X</td></tr> <tr><td>Security awareness training</td><td style="text-align: center;">X</td></tr> <tr><td>Configurations/patching</td><td style="text-align: center;">X</td></tr> <tr><td>Other: privacy impact assessment, risk assessment, contingency plan, contingency plan testing, security assessment report</td><td></td></tr> </table>	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		
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																		
<p>C&A process comments:</p> <p>(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 28 C&A packages at 10 components found 17 instances in which accreditation packages were incomplete. Specifically, systems were accredited, although some security documents were missing key information that is required to meet all applicable DHS, OMB, and NIST guidelines.</p>																		

Question 6: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process	
<p>6.a. Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D II.4 (Senior Agency Official for Privacy reporting template), including adherence to existing policy, guidance, and standards.</p> <p>Response Categories:</p> <ul style="list-style-type: none"> - Excellent - Good - Satisfactory - Poor - Failing <p>Comments:</p> <p>DHS has taken steps to continually improve its PIA guidance. The most recent guidance issued by the Privacy Office increased the emphasis on describing the privacy analysis that should take place in making a system design decision that affects privacy. The Privacy Office requires a PTA for all systems to determine if a PIA is required. The PTA was specifically designed to identify which systems in the DHS information system inventory collect or use personally identifiable information (PII), which systems require a PIA, and which need a Privacy Act System of Records Notice. The Privacy Office has further refined the PTA over the past 2 years and it is now a key aspect of the privacy compliance process. 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. The Privacy Office requires more detail requirements than required by OMB.</p>	<p>Good</p>
<p>6.b. Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-06-15, "Safeguarding Personally Identifiable Information" since the most recent self-review, including the agency's policies and processes, and the administrative, technical, and physical means used to control and protect personally identifiable information (PII).</p> <p>Response Categories:</p> <ul style="list-style-type: none"> - Excellent - Good - Satisfactory - Poor - Failing <p>Comments:</p> <p>DHS has taken actions to integrate privacy considerations into the DHS decision-making process by establishing an advisory committee, holding public workshops, and participating in policy development. The Chief Privacy Officer and CIO issued a memorandum in June 2006 to all DHS employees and contractors reinforcing their obligations to safeguard PII. In September 2006, DHS updated its IT security policies to cover the technical safeguards in identifying the requirements surrounding the protection of PII. In 2007; the Privacy Office issued guidance regarding the use of social security numbers at DHS; and the collection, use, retention, and dissemination of information on non-U.S. citizens. In June 2007, the Under Secretary for Management and Chief Privacy Officer requested that all DHS components perform self-assessments of the handling of PII by August 15, 2007, and provide privacy and IT security awareness training to all employees and contractors by September 15, 2007. The Privacy Office is also continually refining the PTA process to identify systems that maintain PII.</p>	<p>Good</p>

Question 7: Configuration Management	
<p>7.a. Is there an agency-wide security configuration policy? Yes or No.</p> <p>Comments: DHS has included in its agency-wide policy the requirement that all components ensure that the installation of hardware and software products meet the 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.</p>	Yes
<p>7.b. Approximate the extent to which applicable information systems apply common security configurations established by NIST.</p> <p>Response categories:</p> <ul style="list-style-type: none"> - 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)

Comments:

- (a) Many of the components use standard configurations for their systems, but have not fully implemented DHS' baseline configuration guides. In addition, while the CIO has performed procedural and documentation reviews at each component to determine whether configuration management processes are in place, no testing has been performed to determine whether components are in compliance with DHS baseline configurations (or other system configuration guides). Results of vulnerability assessments during the fiscal year have identified security concerns, including inadequate password controls, patches not installed, and configuration settings that are not in agreement with DHS baseline configurations.

Question 8: Incident Reporting	
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.	
8.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.
	Yes ^(a)
8.b.	The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov)
	Yes
8.c.	The agency follows documented policies and procedures for reporting to law enforcement. Yes or No.
	Yes
<p>Comments:</p> <p>(a) While DHS requires components to submit weekly incident reports, during an 11-week period in FY 2007, five major components (FEMA, FLETC, ICE, OIG, USCIS) did not submit reports every week.</p>	

Question 9: Security Awareness Training

<p>Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities?</p> <p>Response Categories:</p> <ul style="list-style-type: none"> - 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 	<p>Mostly, or, approximately 81-95% of employees</p>
---	--

Comments:
 The Training Office is validating components training data to ensure that the components provide IT security awareness training to its employees. The Training Office has begun validating training for employees with significant IT security responsibilities, however, all employees, including contractors, with significant IT security responsibilities, have not been identified. In addition, the Training Office has not established appropriate training that is needed for all individuals with significant IT security responsibilities (including network, database and system administrators).

Question 10: Peer-to-Peer File Sharing

<p>Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training? Yes or No.</p>	<p>Yes</p>
--	-------------------

Comments:
 Two components did not explain DHS' policy regarding peer-to-peer file sharing risks during its IT security awareness training.

Question 11: E-Authentication Risk Assessments

<p>The agency has completed system e-authentication risk assessments. Yes or No.</p>	<p>Yes</p>
---	-------------------

Information Security Audit Division

Edward G. Coleman, Director
Jeff Arman, Audit Manager
Chiu-Tong Tsang, Senior IT Auditor
Maria Rodriguez, Senior IT Auditor
Charles Twitty, IT Auditor
Swati Mahajan, IT Specialist
Amanda Strickler, IT Specialist
Tom Rohrback, Management/Program Assistant
Steve Ressler, Referencer

Advanced Technology Division

Richard Saunders, Director
Ginger Doetsch, Senior Security Engineer
Blake Bommelje, IT Specialist

Department of Homeland Security

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