

# DEPARTMENT OF HOMELAND SECURITY

## Office of Inspector General

### Evaluation of DHS' Information Security Program for Fiscal Year 2006



### Office of Information Technology

OIG-06-62

September 2006

*Office of Inspector General*

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



**Homeland  
Security**

September 25, 2006

### 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 by our office as part of our oversight responsibility to promote economy, effectiveness, and efficiency within the Department.

This report assesses 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.....	3
Results of Independent Evaluation .....	7
Recommendations.....	15
Management Comments and OIG Analysis .....	16

## Appendices

Appendix A: Purpose, Scope, and Methodology.....	18
Appendix B: Management Response to Draft Report .....	20
Appendix C: Digital Dashboard Example.....	24
Appendix D: IT Security Scorecard and C&A Remediation Progress Report .....	26
Appendix E: System Inventory and IT Security Performance.....	27
Appendix F: OIG Assessment of the Plan of Action and Milestones Process .....	30
Appendix G: OIG Assessment of the Certification and Accreditation Process .....	31
Appendix H: Agencywide Security Configuration Requirements .....	32
Appendix I: Incident Detection and Handling Procedures .....	33
Appendix J: Security Training Procedures.....	34
Appendix K: Major Contributors to this Report.....	35
Appendix L: Report Distribution .....	36

## Abbreviations

ATO	Authority to Operate
C&A	Certification and Accreditation
CBP	United States Customs and Border Protection
CIO	Chief Information Officer
CIS	United States Citizenship and Immigration Services
CISO	Chief Information Security Officer
CONOPS	Concept of Operations
CSIRC	Computer Security Incident Response Center
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center
FY	Fiscal Year
ICE	United States Immigration and Customs Enforcement

# Table of Contents/Abbreviations

---

ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
Preparedness	Directorate for Preparedness
RFID	Radio Frequency Identification
RMS	Risk Management System
SBU	Sensitive But Unclassified
S&T	Science and Technology
SOC	Security Operations Center
SP	Special Publication
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
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 (DHS) information security program and practices to comply with the Office of Management and Budget's (OMB) *Federal Information Security Management Act (FISMA) of 2002* reporting requirements.<sup>1</sup> We evaluated DHS' progress in implementing its agencywide information security program. In doing so, we specifically assessed DHS' Plan of Action and Milestones (POA&M) as well as its certification and accreditation (C&A) processes. We performed our work at both the program and the component levels.

In response to a United States House of Representatives, Committee on Appropriations report, DHS implemented a department-wide remediation plan to certify and accredit all operational systems by the end of Fiscal Year (FY) 2006.<sup>2</sup> The completion of this plan will eliminate a major factor that held the Department back from strengthening its security program in prior years.

In addition, some of the issues that we identified and recommendations made in our FY 2005 report, to assist DHS and its components in the implementation of its information program, have been addressed. Some of the measures taken include developing a process to maintain a comprehensive inventory and increasing the number of operational systems that have been certified and accredited.

Despite several improvements in DHS' information security program in the past year, DHS components, through their Information Systems Security Managers (ISSM), have not completely aligned their respective information security programs with DHS' overall policies, procedures, and practices. For example:

- All DHS systems have not been properly certified and accredited.
- All components' information security weaknesses are not included in a POA&M.
- Data in the enterprise management tool, Trusted Agent FISMA, is not complete or current.

---

<sup>1</sup> FISMA is included under Title III of the *E-Government Act* (Public Law 107-347).

<sup>2</sup> House Report 109-079 – *Department of Homeland Security Appropriations Bill, 2006*.

- 
- System contingency plans have not been tested for all systems.

While DHS has issued substantial guidance designed to create and maintain secure systems, we identified areas where the implementation of agencywide information security procedures require strengthening: (1) certification and accreditation; (2) plan of action and milestones; (3) security configurations; (4) vulnerability testing and remediation; (5) contingency plan testing; (6) incident detection, analysis, and reporting; and (7) specialized security training.

In response to our draft report, DHS concurred with our recommendations and is in the process of implementing corrective measures. DHS' 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 OMB, requires an annual review and reporting of agencies' compliance with FISMA. FISMA focuses on the program management, implementation, and evaluation of the security of unclassified and national security systems.<sup>3</sup>

The *E-Government Act of 2002* (Public Law 107-347) recognized the importance of information security to the economic and national security interests of the United States.<sup>4</sup> 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-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, on July 17, 2006. The memorandum provides updated instructions for agency and OIG reporting under FISMA. This annual evaluation summarizes, according to OMB's instructions, the results of our review of DHS' information security program and practices.

---

<sup>3</sup> The term "national security system" means any information system, including any telecommunications system, used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency:

- (i) The function, operation, or use of which involves intelligence activities; involves cryptographic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military intelligence missions (excluding a system that is to be used for routine administrative and business applications, i.e., payroll, finance, logistics, and personnel management applications), or
- (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

<sup>4</sup> Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

---

The Chief Information Security Officer (CISO) revised the baseline information technology (IT) security policies and procedures in the *DHS Sensitive Systems Policy Directive 4300A* and its companion, *DHS 4300B Sensitive Systems Handbook*, and *DHS National Security Systems Policy Directive 4300B* and its companion, *DHS 4300B National Security Systems Handbook*,<sup>5</sup> to include updated policy on certification and accreditation, wireless communication, and configuration management. Other changes included guidance for tailoring National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 controls based on the impact level established for each security objective (confidentiality, integrity, availability) and mandating that the components implement NIST SP 800-53 controls for all operational systems by March 2007. Additionally, DHS issued the *DHS Certification and Accreditation Guidance for Sensitive But Unclassified (SBU) Systems User's Manual*,<sup>6</sup> which provides the components with the necessary guidance and procedures to complete the C&A for SBU systems. Together, these policies and procedures - if fully implemented by the components - should provide DHS with an effective information security program that complies with FISMA requirements.

DHS has developed a process for reporting and capturing known security weaknesses in POA&Ms. DHS uses an enterprise management tool, Trusted Agent FISMA, to collect and track data related to all POA&M activities, including self-assessments, and certification and accreditation data. Trusted Agent FISMA also collects data on other FISMA metrics, such as the number of systems that have contingency plans, systems with contingency plans tested, systems certified and accredited, employees who have received IT security training, and incident response statistics. See Figure 1 for DHS' POA&M process.

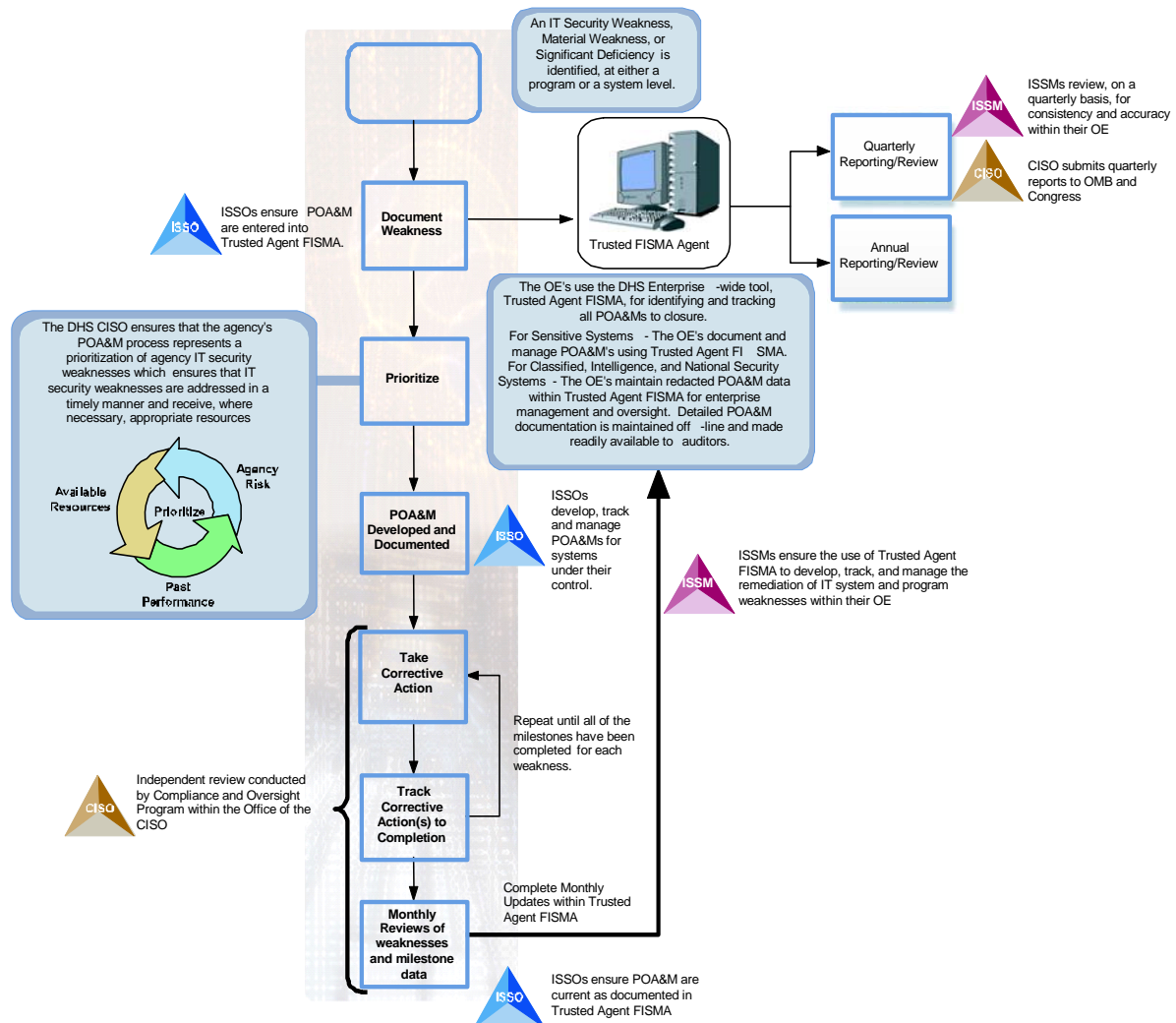
---

<sup>5</sup> The latest versions are dated June 1, 2006.

<sup>6</sup> Dated May 5, 2006.



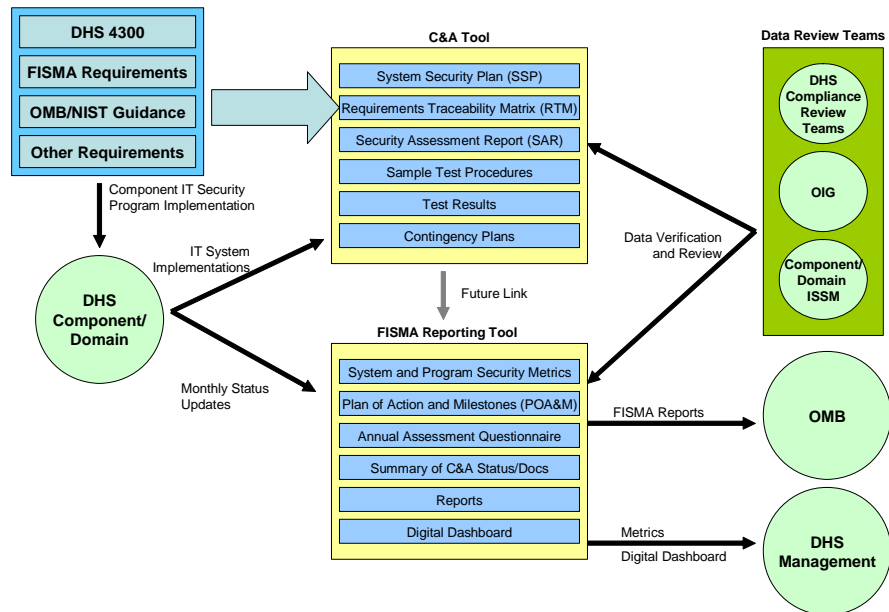
Figure 1: DHS' POA&M Process



Source: DHS 4300A Sensitive Systems Handbook – Attachment H - POA&M Process Guide

DHS also uses an enterprise C&A tool, Risk Management System (RMS), to automate and standardize portions of the C&A process to assist the DHS components to quickly and efficiently develop security accreditation packages. See Figure 2 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 2: DHS' Enterprise Security Management Tools Usage



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

DHS developed the *FY 2006 DHS Information Security Certification and Accreditation (C&A) Remediation Plan* to meet the Department’s goal of 100 percent C&A of all IT systems by September 30, 2006. The objective of the plan is to provide agencywide information security procedures to report on the progress of the C&A efforts within the Department. To manage the components’ compliance with the C&A remediation plan, the CISO developed a “digital dashboard,” which uses red, yellow, and green indicators to reflect the status of each component’s percentage of compliance.<sup>7</sup> The information used to develop the digital dashboard comes from data in Trusted Agent FISMA. See Appendix C for an example of the digital dashboard. A *Department-wide IT Security Scorecard and C&A Remediation Progress Report* was also developed to track the progress of the components and the Department in meeting its goal. See Appendix D for the July 2006 report.

<sup>7</sup> These metrics include the average C&A remediation scores of all inventory systems for each component. Remediation scoring concerns validated artifacts that are weighted according to their importance. Documents include a valid authority to operate letter, risk assessment, system security plan, security test and evaluation plan, security assessment report, contingency plan, contingency plan test results, FIPS 199 security categorization determination, e-authentication, privacy threshold analysis, and security self-assessment.

---

## Results of Independent Evaluation

We separated the results of our evaluation into six FISMA reporting areas. For each area, we identified progress that DHS has made since our FY 2005 evaluation and issues that need to be addressed to be successful in the FISMA area.

### System Inventory and IT Security Performance

DHS has established procedures to adequately maintain its system inventory and has also issued updated guidance to the components regarding many aspects of its IT security program including C&A and contingency planning.

#### PROGRESS

- DHS has a comprehensive inventory of its major applications and general support systems, including contractor and national security systems. DHS identified 692 operational systems (as of September 15, 2006).
- DHS has developed an effective process to update and maintain its inventory on an annual basis for agency, contractors, and classified systems.
- DHS has performed self-assessments on 198 (96 percent) of its contractor systems as of September 15, 2006.
- DHS updated its Rules of Behavior in the DHS Handbook to include the prohibition of peer-to-peer file sharing or software for the purpose of sharing files.

#### ISSUES TO BE ADDRESSED

- System contingency plans have not been tested for 301 (44 percent) of systems as of September 15, 2006.
- DHS cannot totally rely on all of the standard reports generated from Trusted Agent FISMA. The Chief Information Officer (CIO) has to validate some data (numbers of systems reviewed, number of systems for which security controls have been tested and evaluated in the last year) in the “System Inventory and IT Security Performance” report before providing it to OMB.

See Appendix E for specific System Inventory and IT Security Performance data.

---

## Plan of Action and Milestones Process

Although DHS has issued guidance and implemented a tool to capture and track weaknesses, improvements continue to be needed in the components' implementation of the POA&M process. The components are not including all IT security weaknesses in the tool nor is all of the data entered accurate and updated timely.

### PROGRESS

- DHS made numerous enhancements to Trusted Agent FISMA to make it a more useful tool to manage its security program. Enhancements included improved capability to prioritize POA&M weaknesses and additional management reports to validate the integrity of the information entered.
- DHS conducted component site visits and Trusted Agent FISMA training which included detailed reviews of the POA&M process, to ensure the quality and completeness of the component's POA&M data. DHS conducts quarterly reviews and reports its findings to the DHS Compliance and Oversight Office and components.

### ISSUES TO BE ADDRESSED

- DHS' components have not created POA&Ms for all known security weaknesses. As of June 8, 2006, 388 (55 percent) of the operational systems had a POA&M in Trusted Agent FISMA. DHS requires components to create at least one POA&M for every system. We reviewed 27 operational systems that had not been accredited and found 18 that did not have at least one POA&M (lack of a completed C&A).
- 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. Based on an analysis of data in Trusted Agent FISMA as of June 8, 2006, the ISSMs and ISSOs are not maintaining current information as to the progress of security weakness remediation. The Office of the CISO cannot effectively manage its security program without key information being maintained accurately.
  - Component management was not updating all weaknesses when the estimated completion date had been delayed. Four hundred and seventy-seven (477) of the 3,566 open POA&Ms (13 percent) had estimated completion dates that were at least 3 months past due (prior to March 8, 2006), including 37 that had an estimated completion date over 1 year old.

- 
- Twenty-eight open POA&Ms, which included 18 POA&Ms designated as high or medium criticality, did not have an estimated completion date entered in the system.
  - Two thousand four hundred and sixty-two (2,462) of the 3,566 open POA&Ms (69 percent) did not include the resources required for remediation. For the remaining 1,104 POA&Ms that included required resources, 438 (40 percent) listed the cost of remediation as 1 dollar. The total estimated cost of remediation for the 1,104 POA&Ms is approximately \$90.2 million. Because this amount represents less than one third of all open POA&Ms, the actual cost to remediate all weaknesses cannot be accurately budgeted by the components or the Department.
- Not all POA&Ms are being resolved in a timely manner. As of June 8, 2006, 182 of 3,566 open POA&Ms (5 percent), which included 91 designated as high criticality, reported estimated completion dates that were more than 2 years after the identification of the weakness.
  - Some missing or incomplete data identified during DHS' quarterly reviews of the components POA&Ms have not been corrected. Examples that were identified included systems with an authority to operate (ATO) but no POA&Ms and weaknesses without resources or milestones. Many of the systems with incomplete or missing data identified during the March 2006 review were also identified during the June 2006 review.
  - The CISO has not begun to use POA&M priority levels to ensure the timely resolution of critical weaknesses.

See Appendix F for the OIG Assessment of the POA&M Process.

### **Certification and Accreditation Process**

DHS requires components to use a department-wide tool that incorporates NIST security controls to conduct their C&As. In using this tool, components are required to apply NIST SP 800-53 security controls for all system certifications begun after June 1, 2006. However, for many of the systems reviewed, the artifacts that are required to support the C&A were either missing or incomplete.

### **PROGRESS**

- DHS issued *Certification and Accreditation Guidance for SBU Systems* to provide step-by-step instructions to the components to perform system C&A.

- 
- DHS developed a C&A Remediation Plan designed to have 100 percent of its systems certified and accredited and contingency plans tested in FY 2006.
  - DHS requires 11 C&A artifacts to be uploaded into Trusted Agent FISMA to monitor components' progress in meeting its C&A remediation plan goal.<sup>8</sup> In addition, the CISO established a process to independently review and validate the artifacts in Trusted Agent FISMA.
  - The CISO monitors components' progress through monthly scorecard reports. See Appendix D for the July 2006 report.
  - Components are required to apply NIST SP 800-53 security controls for all system certifications begun after June 1, 2006.
  - DHS has updated RMS to incorporate NIST SP 800-53 and Federal Information Processing Standard (FIPS) Publication 200 security controls.
  - Beginning in February 2006, the DHS Privacy Office is responsible for validating Privacy Threshold Assessments and Privacy Impact Assessments for all systems.
  - As of August 14, 2006, 77 percent of DHS' operational systems have been certified and accredited and obtained an ATO. This is an improvement over FY 2005 when 32 percent of the Department's systems had been certified and accredited.
  - Many ISSMs have formal and informal processes in place to review C&A documentation for their systems.

#### ISSUES TO BE ADDRESSED

- We selected 35 systems spanning 10 components (including 29 systems with current ATOs) to evaluate the quality of DHS' C&A process. In 27 instances, the accreditation packages were incomplete. The C&A process requires documentation of system security plans, risk assessments, system test and evaluation plans, security assessment reports, contingency plans, and contingency plan test results. Specifically, systems were accredited, although some security documents were missing key information that is required to meet applicable DHS, OMB, and NIST guidelines. Without this information, agency officials cannot make credible risk-based decisions on whether to authorize the system to operate. For example, we identified the following:

---

<sup>8</sup> The 11 artifacts are: ATO letter, system security plan, security assessment report, risk assessment, security test and evaluation, contingency plan, contingency plan test results, FIPS 199 determination, e-authentication determination, privacy threshold analysis, and NIST 800-26.

- 
- Eleven instances where system security plans were incomplete as sections that describe operational and technical controls and incident handling procedures were missing;
  - Twenty instances where the use of automated vulnerability assessment tools were not documented in the risk assessments;
  - Nine instances where the alternate processing facilities were not identified in the contingency plans for systems that were categorized as high impact;
  - Eight instances where the contingency plans were not tested or the results were not documented; and
  - Fifteen instances where there were no documented test results from the system test and evaluation plan or the residual risks were not identified in the security assessment report.
- We identified deficiencies in artifacts that had been validated by DHS. For example, systems with expired ATO or Interim ATO were validated by DHS and accepted as a current ATO. In addition, an e-authentication workbook was improperly validated as support for performing a FIPS-199 categorization. We also identified instances where the dates reported in Trusted Agent FISMA were not the same as the dates in the supporting artifacts.
  - Twenty-eight systems were accredited without at least one of three critical artifacts: risk assessment, system security plan, or security assessment report. Four of the 28 lacked all three of the required artifacts.
  - Six United States Citizenship and Immigration Services (CIS) systems in which one or more of the security objectives (confidentiality, integrity, availability) in the FIPS 199 worksheet did not match what was reported in the system security plan. The DHS CIO has not issued detailed guidance to the components on how to categorize systems based on the types of data being captured, processed, or maintained. Therefore, there is little assurance that the accreditations by the components were based on an accurate review of risks and controls needed.
  - Based on guidance provided by the CISO to the components, 80 systems were accredited for 1 year or less (including 24 for 6 months or less). These systems should not be considered in calculating the number of systems that DHS has accredited.

See Appendix G for the OIG Assessment of the C&A Process.

---

## Agencywide Security Configuration Requirements

Although DHS has updated its baseline software security configuration guides, the components have not implemented all of the required software security configurations.

### PROGRESS

- DHS updated its agencywide security baseline configuration guides for Windows 2000/2003/XP, Solaris, HP-UX, Linux, Cisco Routers, and Oracle database servers in May 2006.
- An analysis of three baseline configuration guides (Windows, Oracle, and Cisco) disclosed that they provide a sufficient level of detail to adequately secure basic installations of these systems.

### ISSUES TO BE ADDRESSED

- Baseline configuration guides had not been developed for all software systems in use at DHS (for example, Windows NT, Windows Active Directory).
- DHS policy does not require that components use guidelines published by other agencies (such as NIST, National Security Agency, and Defense Information Systems Agency) for systems where DHS has not developed its own baseline configuration guides.
- Components have not fully implemented DHS baseline security configuration requirements for all of their systems. Our review of four systems at three components (Federal Emergency Management Agency (FEMA), United States Immigration and Customs Enforcement (ICE), and Directorate for Preparedness (Preparedness)) disclosed that some DHS baseline configuration requirements were not implemented for their Windows and Oracle systems.
- The CIO does not have a process to determine whether components have implemented DHS baseline configuration requirements.
- Vulnerability assessments performed at components reviewed during our laptop, Radio Frequency Identification (RFID), and Transportation Worker Identification Credential (TWIC) audits identified security concerns resulting from inadequate password controls, patch management, and configuration management. Components included United States Customs and Border Protection (CBP), OIG, Science and Technology (S&T), Transportation Security Administration



---

(TSA), and United States Visitor and Immigrant Status Indicator Technology (US-VISIT).<sup>9</sup>

See Appendix H for information regarding DHS' Agencywide Security Configuration Requirements.

### **Incident Detection, Handling, and Analysis Procedures**

DHS has not improved its incident detection, handling, and analysis procedures during the last year. DHS does not have a departmental vulnerability assessment program to ensure that all systems are tested at least yearly nor is there assurance that all security incidents are being reported.

#### **ISSUES TO BE ADDRESSED**

- DHS' vulnerability assessment program has not been fully established. Therefore, DHS does not have reliable measures or a baseline to assess the results of its vulnerability scans or its penetration testing.
- Some components are not reporting incidents to the DHS Computer Security Incident Response Center (CSIRC), as required. Components are required to submit weekly incident reports. Five components (FEMA, Federal Law Enforcement Training Center (FLETC), OIG, TSA, United States Secret Service (USSS)) did not submit reports every week during a 12-week period that we reviewed.
- DHS CSIRC does not follow-up with components that do not submit weekly incident reports.
- DHS does not have detailed procedures for reporting incidents externally to law enforcement authorities. We also reported this issue in our FY 2004 and FY 2005 FISMA reports.<sup>10</sup>
- The DHS CSIRC does not have detailed procedures for reporting incidents to the United States Computer Emergency Readiness Team (US-CERT).
- DHS has not defined detailed procedures for the DHS CSIRC to perform department-wide security incident analysis. We reported a similar issue in our FY 2005 FISMA report.

---

<sup>9</sup> *CBP's Trusted Traveler Systems Using RFID Technology Require Enhanced Security*, dated May 2006 (OIG-06-36); *Enhanced Security Controls Needed for US-VISIT's System Using RFID Technology*, dated June 2006 (OIG-06-39); *Improved Administration Can Enhance Science and Technology Laptop Computer Security*, dated June 2006 (OIG-06-42); *TSA's Development of Its Weapons Management System Using RFID*, dated July 2006 (OIG-06-44); *DHS Must Address Significant Security Vulnerabilities Prior to TWIC Implementation*, dated July 2006 (OIG-06-47); *Office of Inspector General Laptop Computers Are Susceptible To Compromise*, dated September 2006 (OIG-06-58).

<sup>10</sup> *Evaluation of DHS' Information Security Program for Fiscal Year 2004*, dated September 2004 (OIG-04-41); *Evaluation of DHS' Information Security Program for Fiscal Year 2005*, dated September 2005 (OIG-05-46).

---

See Appendix I for information regarding DHS' Incident Detection and Handling Procedures.

### **Security Training Procedures**

DHS has begun to validate employee 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 started quarterly reviews in May 2006 to validate security awareness training statistics entered into Trusted Agent FISMA by each component.
- The Training Office reviews training materials used by the components.

#### **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 2006. Currently, the plan is to launch the system by the end of August 2006 for DHS headquarters employees only. The system is expected to be fully functional (available to all components) by FY 2010.
- 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 ensures that ISSMs and ISSOs obtain specialized training, it relies on the components to ensure that other 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 2005 FISMA report.
- As of August 4, 2006, the Training Office had not begun to validate specialized security training for individuals with significant IT security responsibilities at each component.
- Some of the FY 2005 training plans (submitted by September 1, 2005) did not include all of the mandatory data elements required by the

---

DHS Handbook. For example, training plans did not include the number of employees and contractors with network accounts, dates for security awareness training, the number of information systems security employees, and dates for specialized training. Because the FY 2006 plans are not due until September 1, 2006, we were unable to determine whether these plans are adequate.

See Appendix J for information regarding DHS' Security Training Procedures.

## **Recommendations**

We recommend that the DHS CIO:

1. Improve the CISO's review process to ensure that all POA&Ms are complete, accurate, and current. Deficiencies identified during the reviews should be corrected timely.
2. Ensure the quality of all C&A documents (complete, accurate, and properly validated) before a system is accredited by improving the artifact validation process.
3. Implement a department-wide incident analysis process and vulnerability assessment program (including baseline configuration requirements verification).
4. Ensure that all incidents are reported to the DHS CSIRC. The DHS CSIRC should follow-up with components that do not provide the required reports.
5. Develop and implement documented procedures to identify, report, and track incidents that should be forwarded to law enforcement authorities and US-CERT (for example, type of incidents to report, deadlines to report incidents, responsible agency and reporting contacts, methods to report incidents).
6. Establish appropriate training that is needed for all individuals with significant security responsibilities; ensure that these individuals complete the required training as part of the validation process performed by the Training Office.
7. Identify the Department's information data types and their minimum FIPS 199 categorizations to assist the components in determining the necessary security controls needed for their data.
8. Ensure that configuration requirements are developed and published for all major software systems used by DHS components.

---

## Management Comments and OIG Analysis

DHS agreed with recommendation 1. DHS continues to improve the POA&M process and will increase its focus on POA&M quality and timeliness in FY 2007.

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

DHS agreed with recommendation 2. DHS recently changed the personnel responsible for validating its C&A document to provide additional quality assurance safeguards. Continued quality improvements of its C&A documents will occur in FY 2007.

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

DHS agreed with recommendation 3. DHS plans to improve its vulnerability management as part of its enterprise Network Operations Center/Security Operations Center (NOC/SOC) in FY 2007. A Concept of Operations (CONOPS) for the NOC/SOC, which will provide detailed guidance, is under development and will be completed by March 30, 2007.

We agree that the steps DHS plans to take begin to satisfy this recommendation. However, DHS did not fully address our recommendation. We maintain that a department-wide incident analysis process and vulnerability program should be part of the NOC/SOC.

DHS agreed with recommendation 4. DHS plans to improve its security incident analysis and reporting with the implementation of its enterprise NOC/SOC CONOPS in FY 2007.

We agree that the steps DHS plans to take begin to satisfy this recommendation. However, DHS did not fully address our recommendation. We maintain that the DHS CSIRC should ensure that all incidents are reported.

DHS agreed with recommendation 5. DHS plans to improve its security incident analysis and reporting with the implementation of its enterprise NOC/SOC and development of a CONOPS in FY 2007.

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

DHS agreed with recommendation 6. The CISO provides specialized security training during its annual security conference and individuals receive role-based training on a case-by-case basis.

---

We agree that the steps DHS plans to take begin to satisfy this recommendation. However, DHS did not fully address our recommendation. We maintain that DHS should establish appropriate training for all individuals with significant security responsibilities and ensure that these individuals complete the required training.

DHS agreed with recommendation 7. DHS will expand its process for reviewing and possibly add additional information types in FY 2007.

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

DHS agreed with recommendation 8. The Department recently issued a configuration guide for Windows NT.

We agree that the steps DHS has taken satisfy this recommendation.

## Purpose, Scope, and Methodology

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-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, issued on July 17, 2006. We conducted our work at the program level and at DHS' major components (CBP, CIS, DHS Management, FEMA, FLETC, ICE, OIG, Preparedness, S&T, TSA, United States Coast Guard (USCG), and USSS).

In addition to our independent evaluation, we conducted reviews of DHS' information systems and security program related areas throughout FY 2006. This report includes results of a limited number of systems evaluated during our past and on-going financial statement review, laptop security, database security, RFID, TWIC program at TSA, and US-VISIT 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 at the program level and at the component level; (4) evaluated processes (i.e., system inventory, C&A, security training, and incident response) DHS has implemented as part of its agencywide information security program; and, (5) developed our independent evaluation of DHS' information security program.

OIG audit contractors were responsible for reviewing the quality of the C&A packages for a sample of 35 systems at 10 components (CBP, CIS, DHS Management, FEMA, ICE, Preparedness, S&T, TSA, USCG, and USSS) to ensure that all of the required documents were completed prior to being accredited.

We conducted our evaluation between May and September 2006 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 K.

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 18, 2006

**TO:** Frank Deffer  
Assistant Inspector General  
Information Technology

**FROM:** Charles R. Armstrong  
Deputy Chief Information Officer 

**SUBJECT:** CIO Comments on the *OIG-06-XX Evaluation of DHS' Information Security Program for Fiscal Year 2006* Dated September 14, 2006.

The Office of Information Security has reviewed the Office of Inspector General (OIG) *Evaluation of DHS' Information Security Program for Fiscal Year 2006*, dated September 14, 2006, and concurs with all recommendations with comments. Specific comments are included in the Attachment to this memo.

It is noted that unlike in 2005, the OIG is not recommending that the Information Security Program be considered a significant deficiency for 2006. Based on this, as well as the Department's significant progress over this past year as documented in the Department's 2006 FISMA submission, the Department now considers the 2005 FISMA Report (OIG-05-46) finding which identified the DHS Information Security Program as a significant deficiency to be closed.

Please let me know if you have any questions. The OIG office may also contact Robert West, Chief Information Security Officer (CISO) at (202) 447-0442.

cc: Robert West CISO  
Component CIOs  
Component ISSMs

Attachment/as stated



ATTACHMENT: CIO Feedback on OIG-06-xx

**Evaluation of DHS' Information Security Program for Fiscal Year 2006**

**COMMENTS ON THE SPECIFIC OIG RECOMMENDATIONS:**

1. Improve the CISO's review process to ensure that all Plan of Action and Milestones (POA&Ms) are complete, accurate, and current. Deficiencies identified during the reviews should be corrected timely.  
**Response: Concur.** The Office of Information Security continues to improve the POA&M process and will increase its focus on POA&M quality and timeliness in FY07.
2. Ensure the quality of all Certification and Accreditation (C&A) documents (complete, accurate, and properly validated) before a system is accredited by improving the artifact validation process.  
**Response: Concur.** The *Fiscal Year 2006 C&A Remediation Plan* successfully ensured a majority of DHS systems provided C&A documents consistent with DHS and NIST guidance. The Department recently changed the contracted C&A document reviews to provide additional quality assurance safeguards. The Five-Year Information Security Strategic Plan calls for continued quality improvements in conjunction with the 2007 Program theme of "Raising the Bar."
3. Implement a department-wide incident analysis process and vulnerability assessment program (including baseline configuration requirements verification).  
**Response: Concur.** With the implementation of an enterprise Network Operations Center/Security Operations Center (NOC/SOC) as part of OneNet Project in Fiscal Year 2007, security and privacy incident analysis and reporting will be improved, as well as improved vulnerability management. A Concept of Operations (CONOPS) for the enterprise NOC/SOC is under development which will provide detailed guidance for incident reporting. The CONOP will be completed by the end of 2<sup>nd</sup> quarter, Fiscal Year 2007.
4. Ensure that all incidents are reported to the Department's Computer Security Incident Response Center (DHS CSIRC). The DHS CSIRC should follow-up with components that do not provide the required reports.  
**Response: Concur.** Procedures for incident reporting, including privacy incidents, will be fully addressed in the NOC/SOC CONOPS. See comments to recommendation 3 above.
5. Develop and implement documented procedures to identify, report, and track incidents that should be forwarded to law enforcement authorities and United States Computer Emergency Response Team (US-CERT). For example, type of incidents to report, deadlines to report incidents, responsible agency and reporting contacts, methods to report incidents).  
**Response: Concur.** See response to recommendation 3. It should be noted that the Department has documented incident reports to law enforcement. Furthermore, many of the Components are law enforcement organizations.
6. Establish appropriate training that is needed for all individuals with significant security responsibilities and ensure that these individuals complete the required training as part of the validation process performed by the Training Office.  
**Response: Concur.** Individuals with significant security responsibilities receive role-based training on a case by case basis, in direct relation to their position, experience level and duties. Specialized security training is provided to individuals at the annual Security Conference.
7. Identify the Department's information data types and their minimum FIPS 199 categorizations to assist the components in determining the necessary security controls needed for their data.

ATTACHMENT: CIO Feedback on OIG-06-xx

**Evaluation of DHS' Information Security Program for Fiscal Year 2006**

**Response: Concur.** The Department published a *FIPS 199 Workbook* and an *Information Security Categorization Guide* in 2005. These documents provide detailed guidance on implementing National Institute of Standards and Technology (NIST) Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories* in conjunction with the Enterprise Architecture. Nearly 100% of the Department's systems have completed an initial categorization using this standard and guide. The process for reviewing and potentially adding additional information types (e.g. privacy data, transportation data, and other specialized data) will be expanded in 2007.

8. Ensure that configuration requirements are developed and published for all major software systems used by DHS components.

**Response: Concur.** Originally Windows NT was identified as a prohibited operating system, and no configuration guide was published for this operating system. Based on a small footprint of Windows NT systems still in use in the Department, a configuration guide has been published for Windows NT and is available online. Currently less than 3% of the Department's system inventory is identified as supporting Windows NT. With the exception of Windows NT, the Department had previously published configuration guidance for all other operating systems in use in the Department and those remain in effect today.

**COMMENTS ON THE OIG NARRATIVE REPORT:**

The CIO appreciates the OIG recognizing the significant accomplishments of the Information Security Program during Fiscal Year 2006, and we look forward to working with the OIG in the future as we continue to improve. The following comments are provided in response to the narrative report provided as part of the OIG submission.

**1. Standard Reports (Page 7)**

The CISO requires all metrics reported be validated for correctness. Standard Application reports have not been tailored or optimized for the Department. The Information Security Office provides custom database queries to support the extensive audit and FISMA reporting requirements for both internal and external reporting requirements. In order to maximize quality assurance of inventory and component reporting all tool updates and reporting processes are regularly reviewed to consistently addresses and resolved any identified reporting discrepancy. The Department's system reporting methods will continue to be updated in 2007 to expand reporting requirements for FISMA, Capital Planning and Investment Control, Privacy, Configuration Management, Financial Systems, etc. All reported data reported has been thoroughly evaluated to ensure correctness.

**2. C&A Duration. (Page 11)**

The CISO allows components to accredit systems for less than the three-year maximum allowed and based on mission needs. Neither Department Information Security Policies nor NIST guidance specify a minimum time for C&A's, and C&As of a shorter duration than the maximum allowed time frame are consistent with Department policy and NIST guidance for risk-based decisions. This allows the Designated Approving Authority (DAA) to have an appropriate level of authority based on unique mission requirements and documented acceptance of risk. Furthermore, all ATO's were manually validated by the Office of Information Security as part of the development of the Department's FISMA Report for 2006.

ATTACHMENT: CIO Feedback on OIG-06-xx  
**Evaluation of DHS' Information Security Program for Fiscal Year 2006**

**COMMENTS ON THE OIG FY 2006 FISMA SUBMISSION TO OMB**

The Office of Information Security requests the OIG update their FY 2006 FISMA submission in the following areas:

<b>Reference</b>	<b>Change Request</b>
Appendix F, footnote (f). Comment	The priority levels were added to the FISMA Reporting Tool in August 2006.
Appendix H, Question 6a Comment	Windows NT guidance has been posted to the DHS OnLine. Currently only 2.9 percent of the DHS system inventory reports using this product.
Appendix J, Question 8 comment	Many of the Components use the significant specialized IT security training included in the DHS Security Conference to provide specialized training for the individuals with significant security responsibility.
Appendix J, Question 9 comment	Remove FLETC from this comment. FLETC has completed its update to reflect peer-to-peer file sharing. Proof was provided to the OIG by the Training Manager.

**FOR ILLUSTRATION PURPOSES ONLY**

Department of Homeland Security  
FISMA Manager

LOGOFF DASHBOARD ? HELP

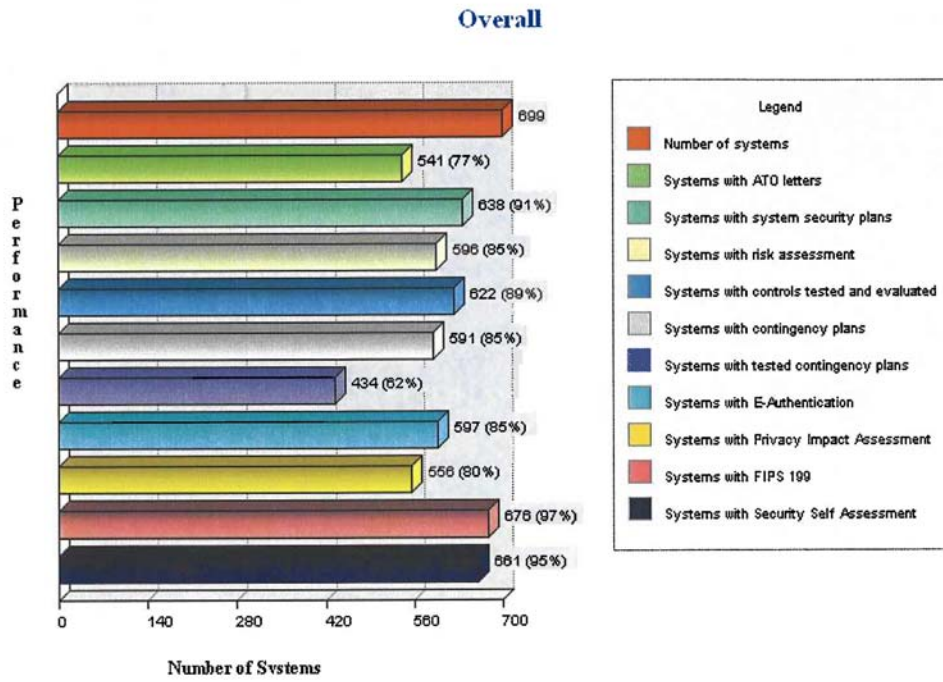
Component	Digital Dashboard		
	Inventory	C & A	Security Training
CBP	43		
CIS	95		
DNDO	1		
FEMA	32		
FLETC	11		
IA	3		
ICE	98		
Infrastructure	20		
OIG	3		
Operations Directorate	1		
Preparedness	41		
Science and Technology	15		
TSA	70		
US-VISIT	8		
USCG	224		
USSS	34		
Overall	699		

Legend  
**Red** - Marginal  
**Yellow** - Basic  
**Green** - Mature  
 Clear - Undefined

Notes  
 1. Click on Component name to display security performance for the organization.  
 2. Click on gauge to display details for security metric.  
 3. Click [here](#) to display the criteria for the security metrics.

**FOR ILLUSTRATION PURPOSES ONLY**

Department Name: Department of Homeland Security Fiscal Year: 2006  
Component: Overall

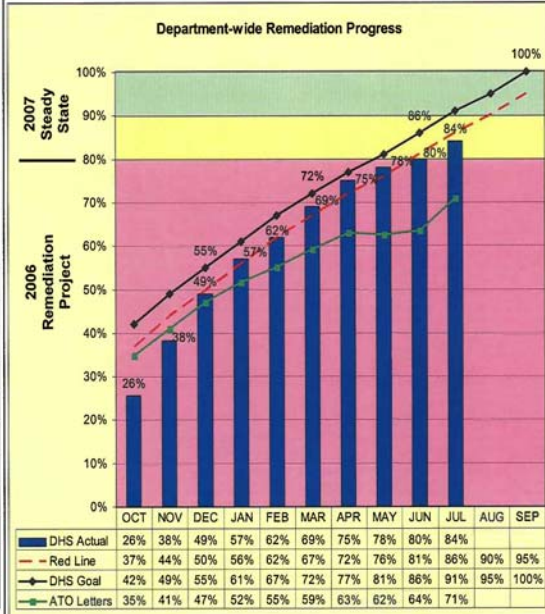




**Department-wide IT Security Scorecard  
C&A Remediation Progress Report**

**- July 2006**

Inventory Status			DHS C&A Remediation			ATO Letters
Component	Systems	Change	Actual	Gap	Trend	% ATO
CBP	43	0	95%	4%	7%	95%
CIS	94	0	83%	-8%	2%	67%
DNDO	1	0	100%	9%	0%	100%
FEMA	32	0	72%	-19%	-3%	53%
FLETC	11	0	83%	-8%	4%	82%
Ops Directorate	1	0	72%	-19%	40%	100%
IA	3	0	75%	-16%	25%	67%
ICE	98	4	81%	-10%	-2%	56%
Infrastructure	20	0	86%	-5%	3%	60%
OIG	3	0	93%	2%	0%	67%
Preparedness	41	-3	38%	-53%	6%	32%
S&T	15	0	99%	8%	5%	100%
TSA	71	0	93%	2%	7%	77%
USCG	225	0	88%	-3%	4%	86%
USSS	34	0	90%	-1%	1%	32%
US-VISIT	8	0	93%	2%	4%	100%
<b>DHS Overall</b>	<b>700</b>	<b>1</b>	<b>84%</b>	<b>-7%</b>	<b>4%</b>	<b>71%</b>



2006 Remediation Project Key	
Definition	Code
Actual % at or above Performance Goal	Green
Actual % within -5% of Performance Goal	Yellow
Actual % less than or equal to -5% of Performance Goal	Red
2007 Steady State Key	
Definition	Code
Both Actual % and ATO Letter % are at or above 90%	Green
Both Actual % and ATO Letter % are at or above 80%	Yellow
Either Actual % or ATO Letter % is below 80%	Red

Data compiled on 8/3/06

Notes  
There was a slight decrease in some components scores due to failed PIA's. Whenever a component has two different scores (Red; Yellow; Green) as a result of the two separate scoring systems, the components receives the better of the two colors.  
e.g. FLETC would have received a Red according to 2006 Remediation Project Scoring but a Yellow according to Steady State scoring. Therefore, FLETC receives the better of the two scores: Yellow.

Appendix E  
System Inventory and IT Security Performance

**Question 1 and 2 – System Inventory and IT Security Performance**

1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).

- To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
- 1) Continue to use NIST Special Publication 800-26, or,
  - 2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

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.

2. For each part of this question, identify actual performance over the past fiscal year by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems, which have completed the following: have a current certification and accreditation, a contingency plan tested within the past year, and security controls tested within the past year.

		Question 1						Question 2					
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	FIPS 199 Risk Impact Level	(a) Total Number	Number Reviewed	(a) Total Number	Number Reviewed	(a) Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
CBP	High		4		0		4	4	100.0%	3	75.0%	3	75.0%
	Moderate		9		0		9	6	66.7%	5	55.6%	1	11.1%
	<b>Sub-total</b>		<b>13</b>		<b>0</b>		<b>13</b>	<b>10</b>	<b>76.9%</b>	<b>8</b>	<b>61.5%</b>	<b>4</b>	<b>30.8%</b>
CIS	Moderate		2		2		4	3	75.0%	2	50.0%	1	25.0%
	<b>Sub-total</b>		<b>2</b>		<b>2</b>		<b>4</b>	<b>3</b>	<b>75.0%</b>	<b>2</b>	<b>50.0%</b>	<b>1</b>	<b>25.0%</b>
FEMA	High		4		0		4	2	50.0%	3	75.0%	2	50.0%
	Moderate		0		1		1	1	100.0%	0	0.0%	1	100.0%
	<b>Sub-total</b>		<b>4</b>		<b>1</b>		<b>5</b>	<b>3</b>	<b>60.0%</b>	<b>3</b>	<b>60.0%</b>	<b>3</b>	<b>60.0%</b>
FLETC	Moderate		2		0		2	2	100.0%	2	100.0%	0	0.0%
	<b>Sub-total</b>		<b>2</b>		<b>0</b>		<b>2</b>	<b>2</b>	<b>100.0%</b>	<b>2</b>	<b>100.0%</b>	<b>0</b>	<b>0.0%</b>
ICE	High		1		2		3	2	66.7%	2	66.7%	3	100.0%
	Moderate		1		1		2	2	100.0%	0	0.0%	1	50.0%
	<b>Sub-total</b>		<b>2</b>		<b>3</b>		<b>5</b>	<b>4</b>	<b>80.0%</b>	<b>2</b>	<b>40.0%</b>	<b>4</b>	<b>80.0%</b>



Appendix E  
System Inventory and IT Security Performance

Bureau Name	FIPS 199 Risk Impact Level	(a) Total Number	Number Reviewed	(a) Total Number	Number Reviewed	(a) Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
Infrastructure	High		0		2		2	1	50.0%	1	50.0%	1	50.0%
	Moderate		1		0		1	1	100.0%	1	100.0%	1	100.0%
	<b>Sub-total</b>		<b>1</b>		<b>2</b>		<b>3</b>	<b>2</b>	<b>66.7%</b>	<b>2</b>	<b>66.7%</b>	<b>2</b>	<b>66.7%</b>
OIG	High		2		0		2	1	50.0%	1	50.0%	0	0.0%
	<b>Sub-total</b>		<b>2</b>		<b>0</b>		<b>2</b>	<b>1</b>	<b>50.0%</b>	<b>1</b>	<b>50.0%</b>	<b>0</b>	<b>0.0%</b>
Preparedness	High		2		2		4	3	75.0%	3	75.0%	3	75.0%
	Moderate		1		0		1	0	0.0%	0	0.0%	0	0.0%
	<b>Sub-total</b>		<b>3</b>		<b>2</b>		<b>5</b>	<b>3</b>	<b>60.0%</b>	<b>3</b>	<b>60.0%</b>	<b>3</b>	<b>60.0%</b>
S&T	High		2		1		3	3	100.0%	2	66.7%	3	100.0%
	Moderate		1		0		1	1	100.0%	1	100.0%	1	100.0%
	<b>Sub-total</b>		<b>3</b>		<b>1</b>		<b>4</b>	<b>4</b>	<b>100.0%</b>	<b>3</b>	<b>75.0%</b>	<b>4</b>	<b>100.0%</b>
TSA	High		1		1		2	1	50.0%	2	100.0%	1	50.0%
	Moderate		3		1		4	4	100.0%	3	75.0%	2	50.0%
	Low		1		0		1	1	100.0%	1	100.0%	1	100.0%
	<b>Sub-total</b>		<b>5</b>		<b>2</b>		<b>7</b>	<b>6</b>	<b>85.7%</b>	<b>6</b>	<b>85.7%</b>	<b>4</b>	<b>57.1%</b>
US-VISIT	Moderate		1		0		1	1	100.0%	1	100.0%	1	100.0%
	<b>Sub-total</b>		<b>1</b>		<b>0</b>		<b>1</b>	<b>1</b>	<b>100.0%</b>	<b>1</b>	<b>100.0%</b>	<b>1</b>	<b>100.0%</b>
USCG	High		2		1		3	2	66.7%	2	66.7%	3	100.0%
	Moderate		5		0		5	5	100.0%	4	80.0%	1	20.0%
	<b>Sub-total</b>		<b>7</b>		<b>1</b>		<b>8</b>	<b>7</b>	<b>87.5%</b>	<b>6</b>	<b>75.0%</b>	<b>4</b>	<b>50.0%</b>
USSS	High		3		0		3	3	100.0%	3	100.0%	1	33.3%
	<b>Sub-total</b>		<b>3</b>		<b>0</b>		<b>3</b>	<b>3</b>	<b>100.0%</b>	<b>3</b>	<b>100.0%</b>	<b>1</b>	<b>33.3%</b>
Agency Totals	High		21		9		30	22	73.3%	22	73.3%	20	66.7%
	Moderate		26		5		31	23	74.2%	17	54.8%	9	29.0%
	Low		1		0		1	1	100.0%	1	100.0%	1	100.0%
	<b>Total</b>		<b>48</b>		<b>14</b>		<b>62</b>	<b>46</b>	<b>74.2%</b>	<b>40</b>	<b>64.5%</b>	<b>30</b>	<b>48.4%</b>

Comments:

- (a) We are reporting the number of systems that we reviewed, therefore the total number and number reviewed are the same. See the CIO's report for the total number of systems for each component.
- (b) The number of systems certified and accredited is based on an ATO letter, not on the adequacy of the documents required.



Appendix E  
System Inventory and IT Security Performance

Question 3 – System Inventory and IT Security Performance	
In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.	
<p><b>3.a.</b> 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. Self-reporting of NIST Special Publication 800-26 and/or NIST 800-53 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient.</p> <p>Response Categories:</p> <ul style="list-style-type: none"> <li>- Rarely, for example, approximately 0-50% of the time</li> <li>- Sometimes, for example, approximately 51-70% of the time</li> <li>- Frequently, for example, approximately 71-80% of the time</li> <li>- Mostly, for example, approximately 81-95% of the time</li> <li>- Almost Always, for example, approximately 96-100% of the time</li> </ul>	<p>- Almost Always, for example, approximately 96-100% of the time <sup>(a)</sup></p>
<p><b>3.b.1</b> The agency has developed an 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"> <li>- Approximately 0-50% complete</li> <li>- Approximately 51-70% complete</li> <li>- Approximately 71-80% complete</li> <li>- Approximately 81-95% complete</li> <li>- Approximately 96-100% complete</li> </ul>	<p>- Approximately 96-100% complete</p>
<p><b>3.b.2</b> If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please list the systems that are missing from the inventory.</p>	<p>N/A</p>
<p><b>3.c.</b> The OIG <b>generally</b> agrees with the CIO on the number of agency owned systems.</p>	<p>Yes</p>
<p><b>3.d.</b> The OIG <b>generally</b> 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.</p>	<p>Yes</p>
<p><b>3.e.</b> The agency inventory is maintained and updated at least annually.</p>	<p>Yes</p>
<p><b>3.f.</b> The agency has completed system e-authentication risk assessments.</p>	<p>Yes</p>

Comments:

- (a) DHS requires contractor systems to be evaluated in the same manner as agency owned systems. As of September 15, 2006, 96 percent of contractor systems have been reviewed, based on the completion of the components' NIST 800-26 self-assessment. This response is a result of DHS' reported performance metrics. The OIG has not evaluated the quality of the assessments performed.

**Question 4 – OIG Assessment of the POA&M Process**

Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below.

For items 4a.-4.f, the response categories are as follows:

- 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><b>4.a.</b> The POA&amp;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>- Almost Always, for example, approximately 96-100% of the time <sup>(a)</sup></p>
<p><b>4.b.</b> When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&amp;Ms for their system(s).</p>	<p>- Sometimes, for example, approximately 51-70% of the time <sup>(b)</sup></p>
<p><b>4.c.</b> Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.</p>	<p>- Frequently, for example, approximately 71-80% of the time <sup>(c)</sup></p>
<p><b>4.d.</b> CIO centrally tracks, maintains, and reviews POA&amp;M activities on at least a quarterly basis.</p>	<p>- Mostly, for example, approximately 81-95% of the time <sup>(d)</sup></p>
<p><b>4.e.</b> OIG findings are incorporated into the POA&amp;M process.</p>	<p>- Mostly, for example, approximately 81-95% of the time <sup>(e)</sup></p>
<p><b>4.f.</b> POA&amp;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>- Sometimes, for example, approximately 51-70% of the time <sup>(f)</sup></p>

Comments:

- (a) DHS requires all known IT security weaknesses be included in Trusted Agent FISMA.
- (b) DHS requires components to create POA&Ms for all IT security weaknesses. As of June 8, 2006, 55 percent of the operational systems had a POA&M in Trusted Agent FISMA. We reviewed 27 operational systems that had not been accredited and found 18 systems (67 percent) that did not have at least one POA&M (lack of a completed C&A). In addition, many of the POA&Ms did not contain all required information, such as resources required for remediation.
- (c) DHS components are required to update all information in their POA&Ms at least monthly. However, as of June 8, 2006, 13 percent of open POA&Ms had estimated completion dates that were at least 3 months past due (prior to March 8, 2006), including 37 that had estimated completion dates more than 1 year old. In addition, not all IT security weaknesses are being reported.
- (d) The CIO conducts quarterly reviews of the POA&Ms for status and completion and issues reports to the components. However, the CIO relies on the components to correct and update the POA&Ms based on the findings in the reports.
- (e) The CIO requires all OIG findings be included in each component’s POA&M. We noted that most of the FY 2006 OIG findings were incorporated into a POA&M.
- (f) DHS established new POA&M weakness priority levels in August 2006 for program officials to use to prioritize IT security weaknesses. The CISO has not begun to use the priority levels to ensure the timely resolution of critical weaknesses.

Question 5 – OIG Assessment of the C&A Process	
<p>OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assessment of the agency’s certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, <i>Guide for the Security Certification and Accreditation of Federal Information Systems</i> (May 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199 (February 2004), <i>Standards for Security Categorization of Federal Information and Information Systems</i>, to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans.</p>	
<p>Assess the overall quality of the Department's certification and accreditation process.</p> <p>Response Categories:</p> <ul style="list-style-type: none"> <li>- Excellent</li> <li>- Good</li> <li>- Satisfactory</li> <li>- Poor</li> <li>- Failing</li> </ul>	<p>- Satisfactory<sup>(a)</sup></p>

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 800-53 security controls for all system certifications begun after June 1, 2006. However, for many systems, the artifacts that are required to C&A a system were either missing or incomplete. Our review of 35 C&A packages at 10 components found 27 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.

Appendix H  
Agencywide Security Configuration Requirements

Question 6 – Agencywide Security Configuration Requirements			
<b>6.a.</b>	Is there an agency wide security configuration policy? Yes or No.		Yes
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. However, DHS has not developed configuration guides for all hardware and software systems being used by its components.			
<b>6.b.</b>	Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.		
Product	Addressed in agencywide policy?  Yes, No, or N/A.	Do any agency systems run this software?  Yes or No.	Approximate the extent of implementation of the security configuration policy on the systems running the software.  Response choices include: - Rarely, or, on approximately 0-50% of the systems running this software - Sometimes, or on approximately 51-70% of the systems running this software - Frequently, or on approximately 71-80% of the systems running this software - Mostly, or on approximately 81-95% of the systems running this software - Almost Always, or on approximately 96-100% of the systems running this software
Windows XP Professional	Yes	Yes	(a)
Windows NT	No	Yes	
Windows 2000 Professional	Yes	Yes	
Windows 2000 Server	Yes	Yes	
Windows 2003 Server	Yes	Yes	
Solaris	Yes	Yes	
HP-UX	Yes	Yes	
Linux	Yes	Yes	
Cisco Router IOS	Yes	Yes	
Oracle	Yes	Yes	
Other: SQL Server	Yes	Yes	

Comments:

- (a) Many of the components use standard configurations for their systems, but have not fully implemented DHS' baseline configuration guides. In addition, the CIO has not verified or determined whether components are in compliance with DHS baseline configurations (or other system configuration guides).

Appendix I  
Incident Detection and Handling Procedures

Question 7 – Incident Detection and Handling Procedures	
Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.	
<b>7.a.</b> The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes <sup>(a)</sup>
<b>7.b.</b> The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	No <sup>(b)</sup>
<b>7.c.</b> The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). Yes or No.	Yes

Comments:

- (a) While DHS requires components to submit weekly incident reports, during a 12-week period in FY 2006, five major components (FEMA, FLETC, OIG, TSA, USSS) did not submit reports every week. In addition, the DHS CSIRC does not follow-up with the components to ensure that all incidents are being reported.
- (b) We again determined that DHS does not have detailed documented procedures for reporting incidents to law enforcement authorities.

Question 8 – Security Training Procedures	
<p>Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities?</p> <p>Response Choices include:</p> <ul style="list-style-type: none"> <li>- Rarely, or, approximately 0-50% of employees have sufficient training</li> <li>- Sometimes, or approximately 51-70% of employees have sufficient training</li> <li>- Frequently, or approximately 71-80% of employees have sufficient training</li> <li>- Mostly, or approximately 81-95% of employees have sufficient training</li> <li>- Almost Always, or approximately 96-100% of employees have sufficient training</li> </ul>	<ul style="list-style-type: none"> <li>- Frequently, or, approximately 71-80% of employees have sufficient training</li> </ul>

Comments: The Training Office has begun a validation process to ensure that the components provide IT security awareness training to its employees. As of August 4, 2006, the Training Office has not begun validating training for employees with significant IT security responsibilities. In addition, the Training Office has not established the appropriate security training that is needed for all individuals with significant IT security responsibilities (including network, database and system administrators).

Question 9 – Security Training Procedures	
<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 (FLETC, USCG) did not explain DHS' policy regarding peer-to-peer file sharing risks during its IT security awareness training.

**Information Security Audit Division**

Edward G. Coleman, Director  
Jeff Arman, Audit Manager  
Chiu-Tong Tsang, Senior IT Auditor  
Tarsha Ross, Senior IT Auditor  
Charles Twitty, IT Auditor  
Swati Mahajan, IT Specialist  
Michael Horton, Referencer

**Advanced Technology Division**

Eric Baechle, Senior Security Engineer  
Michael Goodman, Security Engineer

**Department of Homeland Security**

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

**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) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at [www.dhs.gov/oig](http://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 the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or email [DHSOIGHOTLINE@dhs.gov](mailto:DHSOIGHOTLINE@dhs.gov). The OIG seeks to protect the identity of each writer and caller.