DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Evaluation of DHS' Information Security Program for Fiscal Year 2005

Office of Information Technology

OIG-05-46 **September 2005**

Office of Inspector General

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

Homeland Security

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 DHS 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.

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Executive Summary 1

Background 3

Results of Independent Evaluation 6

Recommendations 14

Management Comments and OIG Analysis 14

Appendices

Appendix A:	Purpose, Scope, and Methodology	16
Appendix B:	Management Response to Draft Report	18
Appendix C:	Digital Dashboard	20
Appendix D:	System Inventory and IT Security Performance	21
Appendix E:	OIG Assessment of the Plan of Action and Milestones Process	24
Appendix F:	OIG Assessment of the Certification and Accreditation Process	25
Appendix G:	Agencywide Security Configuration Requirements	26
Appendix H:	Incident Detection and Handling Procedures	27
Appendix I:	Security Training Procedures	28
Appendix J:	Major Contributors to This Report	29
Appendix K:	Report Distribution	30

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
CSIRC	Computer Security Incident Response Center
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
E-authentication	Electronic Authentication
EP&R	Emergency Preparedness and Response
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center
FY	Fiscal Year
IAIP	Information Analysis and Infrastructure Protection

Table of Contents/Abbreviations

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
NSA	National Security Agency
ODP	Office of Domestic Preparedness
OIG	Office of Inspector General
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
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
USSS	United States Secret Service
US-VISIT	United States Visitor and Immigrant Status Indicator Technology

Executive Summary

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) of 2002*.[1] FISMA focuses on the program management, implementation, and evaluation of the security of unclassified and national security systems.[2]

To comply with OMB's FISMA reporting requirements, we conducted an independent evaluation of the Department of Homeland Security's (DHS) information security program and practices. As part of our review, we evaluated DHS' processes and the progress made in implementing its agencywide information security program. In doing so, we specifically assessed DHS' Plan of Action and Milestones (POA&M) as well as certification and accreditation (C&A) processes. We focused our evaluation on whether DHS' major organizational components are aligning their information security program and practices with DHS' agency-wide information security program.

We performed our work at both the program and the organizational component levels. The following organizational components were included in our review: United States Customs and Border Protection (CBP), United States Citizenship and Immigration Services (CIS), Emergency Preparedness and Response (EP&R), Federal Law Enforcement Training Center (FLETC), Information Analysis and Infrastructure Protection (IAIP), United States Immigration and Customs Enforcement (ICE), DHS Management (Management), Office of Inspector General (OIG), Science and Technology (S&T), Transportation Security Administration (TSA), United States Coast Guard (USCG); and United

[1] FISMA is included under Title III of the *E-Government Act* (Public Law 107-347).

[2] 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.

States Secret Service (USSS). See Appendix A for a detailed discussion of our purpose, scope, and methodology.

DHS achieved two significant milestones that will help the department move toward managing a successful information security program. First, DHS completed a comprehensive inventory of its major applications and general support systems, including contractor and national security systems, for all organizational components. Second, DHS implemented a department-wide certification and accreditation (C&A) tool that incorporates the guidance required to adequately complete a C&A for all systems. The completion of these two tasks eliminated two factors that significantly held the department back in achieving some success in establishing its security program in the last two years.

The Chief Information Security Officer (CISO) revised the baseline information technology (IT) security policies and procedures in the Sensitive Systems Policy Publication 4300A and its companion, the Sensitive Systems Handbook[3]; and National Security Systems Policy Publication 4300B and its companion, the National Security Systems Handbook[4] to include updated policy on Public Key Infrastructure (PKI), wireless communication and media reuse and disposition. Other changes included mandating that the components ensure that their systems meet the requirements specified in the DHS baseline configuration guides, as well as the acceptable methods for encrypting sensitive information. Additionally, DHS issued the *DHS Information Security Program Plan of Action and Milestones (POA&M) Process Guide*,[5] which provides the department and components with the necessary guidance and procedures to develop, maintain, report, and mature the POA&M process. 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.

As we reported in our Fiscal Year (FY) 2004 FISMA evaluation, and despite several major improvements in DHS' information security program, DHS organizational 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 certified and accredited.
- All organizational components' information security weaknesses are

[3] The latest versions are dated July 29, 2005.
[4] The latest versions are dated August 15, 2005
[5] Dated June 10, 2005.

not included in a POA&M.

- Data in the enterprise management tool, Trusted Agent FISMA, is not complete or current.
- System contingency plans have not been developed or tested for all systems.
- FISMA metrics data, captured within Trusted Agent FISMA and used by the Chief Information Officer (CIO) to monitor component's security programs, is not comprehensively verified.

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

In our FY 2004 report, we identified issues to be addressed to assist DHS and its components in the implementation of its information security program. While some of these issues have been addressed, such as completing a comprehensive inventory; the majority of DHS' operational systems have not been certified and accredited. Further, POA&Ms have not been developed for all weaknesses. We recommend that DHS continue to consider its information security program a significant deficiency for FY 2005.

In response to our draft report, DHS agreed and has already taken steps to implement each of our recommendations. DHS' response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

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.[6] 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.

[6] Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

FISMA requires each federal agency to develop, document, and implement an agency-wide security program. The agency's security program should protect the information and the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. As specified in FISMA, agency heads are charged with conducting an annual evaluation of information programs and systems under their purview, as well as assessments of related security policies and procedures. OIGs must independently evaluate the effectiveness of an agency's information security program and practices on an annual basis.

OMB issued memorandum M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, on June 13, 2005. 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.

DHS' CIO, who has oversight responsibilities for DHS' information security program, has delegated to the CISO, as required under FISMA, the authority to establish information security policies and procedures throughout the department. DHS' CISO has reorganized the staff into three main areas: program management, program services, and program performance. These areas are essential to deliver a successful security program to protect the confidentiality, integrity, and availability of information.

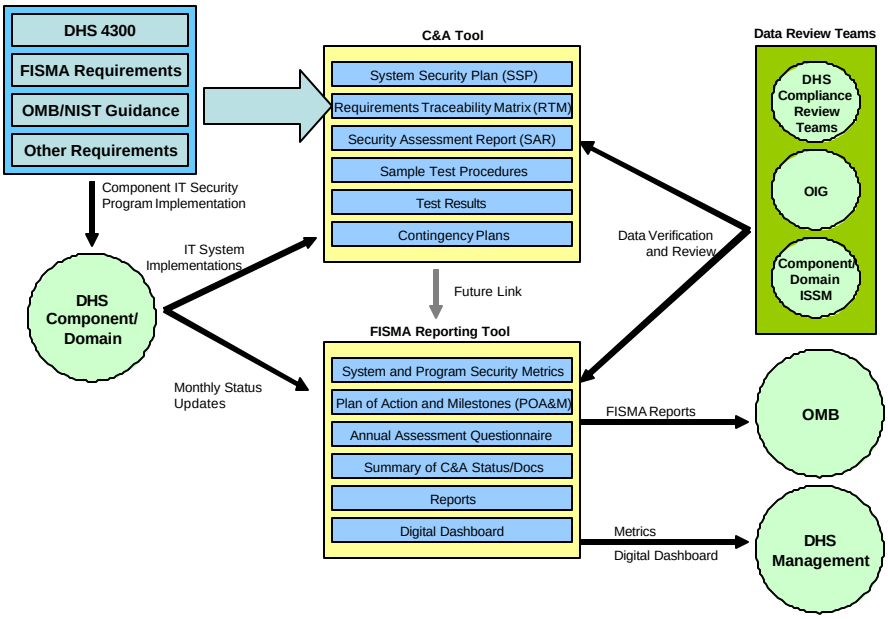
DHS has developed a process for reporting and capturing known security weaknesses in POA&Ms. DHS utilizes an enterprise management tool, Trusted Agent FISMA, to collect and track data related to all POA&M activities, including self-assessments, and certification and accreditation data. Trusted Agent 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. DHS also uses an enterprise C&A tool, Risk Management System, to automate and standardize portions of the C&A process to assist DHS to quickly and efficiently develop security accreditation packages. See Figure 1 for an illustration on how the tools are used within the department to collect, manage, and report information security metrics.

A Security Applications Working Group was established in June 2004. The group meets monthly to foster a dialogue between the CISO and the organizational components, to obtain the components' input on ways to improve the FISMA data collection effort, and address issues and

problems that relate to the use of Trusted Agent FISMA and the C&A tool.

To manage the organizational components' compliance with FISMA metrics and the effectiveness of their component-level information security programs, the CISO has developed a "digital dashboard," which uses red, yellow, and green indicators to reflect the status of each component's percentage of compliance.[7] The information used to develop the digital dashboard comes from data in Trusted Agent FISMA, and from DHS' program directors. See Appendix C for the digital dashboard as of August 26, 2005.

Figure 1: DHS' Enterprise Security Management Tools Usage



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

In addition to our independent evaluation, we conducted reviews of DHS' information systems and security program related areas throughout FY 2005. This report includes results of a limited number of systems evaluated during our on-going financial statement review, and from on-going audits of network security, database security, and United States Visitor and Immigrant Status Indicator Technology (US-VISIT) security.

[7] These metrics include the percentage of systems that have been accredited, systems and applications for which an annual self-assessment has been completed, systems with contingency plans developed and tested, personnel (employees and contractors) that completed security awareness, and IT security professionals trained.

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 2004 evaluation and issues that need to be addressed in order to be successful in the FISMA area.

System Inventory and IT Security Performance

DHS has made significant progress by compiling a department-wide system inventory and issuing additional guidance to the components. However, DHS must perform self-assessments and e-authentication risk assessments on all of its systems, including contractor systems.

PROGRESS

- DHS completed a comprehensive inventory of its major applications and general support systems, including contractor and national security systems. DHS identified 795 operational systems (as of August 25, 2005). In FY 2004, DHS reported 295 systems.
- DHS issued guidance for: (1) identifying security categories for information and information systems (Federal Information Processing Standard (FIPS) Publication 199)[8]; (2) determining if an electronic authentication (e-authentication) risk assessment is required (and the assurance level, as appropriate); and, (3) determining if a privacy impact assessment is required.
- DHS issued a draft PKI policy in April 2005 as well as a draft wireless policy and procedures in June 2005.
- DHS established a policy prohibiting peer-to-peer file sharing software on DHS computers or on any computer or information system that might be connected to its network.

ISSUES TO BE ADDRESSED

- Since completing its first comprehensive system inventory in August 2005, DHS has not yet developed a process that it will use to update its inventory at least annually beginning next year.
- Components have not completed e-authentication risk assessments for all systems.

[8] FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, dated February 2004, defines the standards all federal agencies are to use in categorizing information and information systems according to a range of risk levels impacting the confidentiality, integrity, and availability of the information or information systems.

- Components have only completed National Institute of Standards and Technology (NIST) 800-26 self-assessments on 46 percent of its contractor systems (as of August 26, 2005).[9]
- System contingency plans have not been developed or tested for all systems. For example, during our network audit, we determined that TSA and USSS had not developed a contingency plan; and, USCG had not tested its contingency plan. During our database audit, we determined that CIS, USCG, and USSS had not developed a contingency plan, while EP&R had not tested its contingency plan.

See Attachment D for specific System Inventory and IT Security Performance data.

OIG Assessment of the Plan of Action and Milestones Process

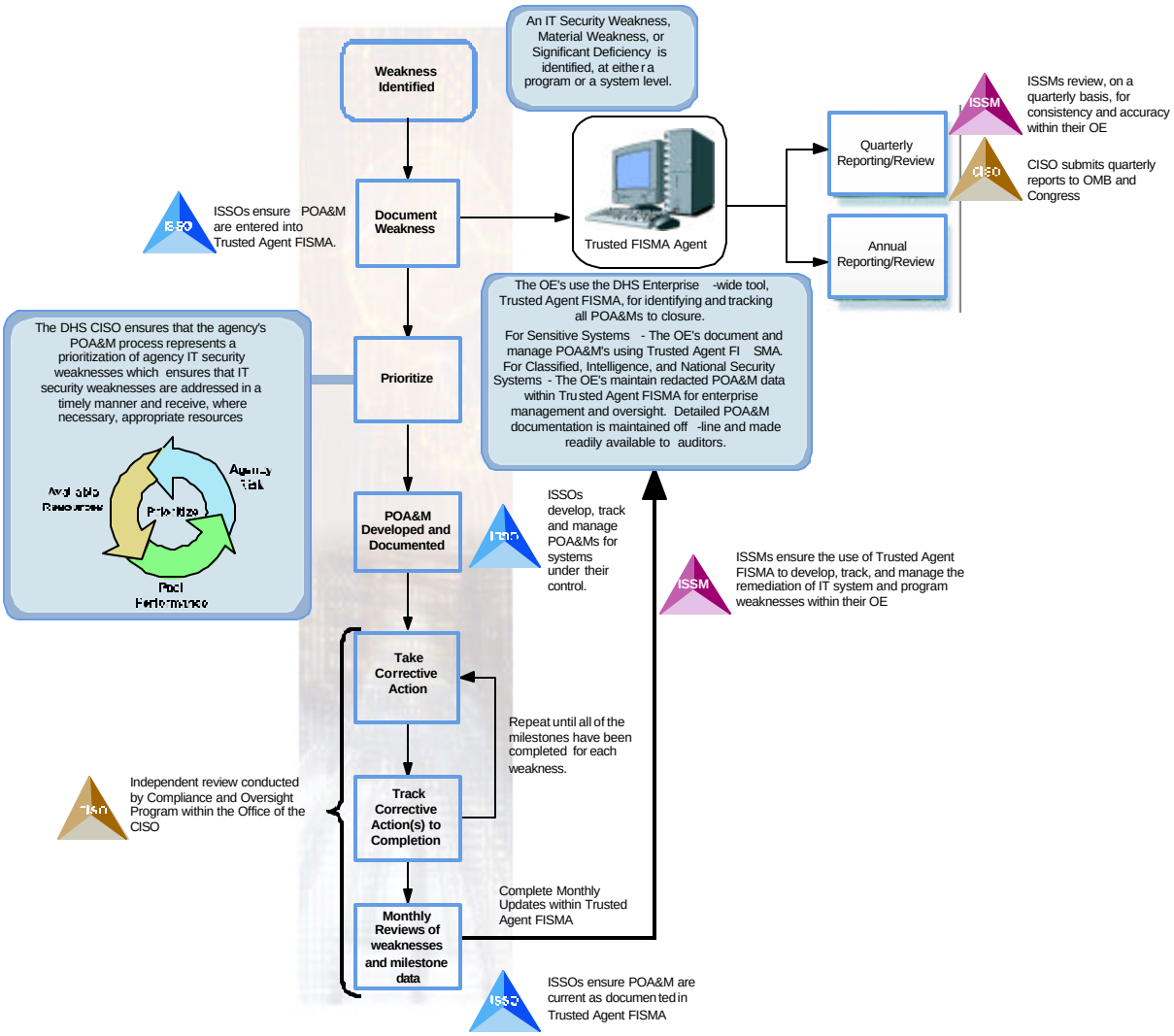
While DHS has issued guidance and implemented a tool to capture and track weaknesses, improvements are needed in the components' implementation of the POA&M process. The components are not including all IT security weaknesses in the tool nor is all of the data entered accurately.

PROGRESS

- DHS made numerous enhancements to Trusted Agent FISMA to make it a more useful tool to manage its security program. Enhancements included additional management reports at the component and department level, computed metrics, and updates to fields in the digital dashboard and other sections to support changes in FISMA reporting.
- DHS issued the *DHS Information Security Program Plan of Action and Milestones (POA&M) Process Guide* in June 2005. The document provides the department and components the guidance and procedures for developing, maintaining, reporting, and maturing the POA&M process. See Figure 2 for the DHS POA&M process.
- DHS established a process to conduct monthly, high-level reviews of some of the POA&M data entered into Trusted Agent FISMA to determine if the information is complete. The results of these reviews are communicated to DHS components through various means, including "Get Well" reports and in comments accessible through the Trusted Agent FISMA Digital Dashboard.

[9] Contractor systems include information systems used or operated by a contractor of an agency or other organization on behalf of an agency.

Figure 2: DHS' POA&M Process



Source: POA&M Guide

Note: Based on our review, the main reason for the process failure is due to the ISSMs and ISSOs not ensuring that POA&Ms are entered and current.

ISSUES TO BE ADDRESSED

- DHS' components have not created POA&Ms for all known weaknesses. As of August 22, 2005, only 35 percent of the 791 operational applications and general support systems listed in Trusted Agent FISMA had POA&Ms entered. Since 68 percent of the operational systems do not have a completed C&A (as of August 26, 2005 - see Appendix C), there should be at least one POA&M (lack of completed C&A) for each of these systems.

- DHS relies on the component ISSMs and Information Systems Security Officers (ISSO) to ensure that POA&M information is entered, accurate, and that weaknesses listed in the POA&Ms are resolved. However, based upon our analysis of data in Trusted Agent FISMA as of August 22, 2005, the ISSMs and ISSOs are not maintaining current information as to the progress of security weakness remediation.
    - We determined that 650 of the 2,425 open POA&Ms (27 percent) had estimated completion dates prior to July 22, 2005. Therefore, POA&Ms have not been updated in over a month, including 40 (2 percent) that had not been updated in over a year.
    - Ninety-five POA&Ms (4 percent) did not have an estimated completion date entered in the system.
    - Only 370 of the 2,425 open POA&Ms (15 percent) included the resources required for remediation, and almost half of those (152) listed the cost of remediation as one dollar. The total estimated cost of remediation for the 370 POA&Ms is approximately $24.3 million. Since this amount represents only a small percent of all POA&Ms, the actual cost to remediate all weaknesses cannot be accurately budgeted by the components or the department.
- The components have not created POA&Ms for all OIG audit report findings in Trusted Agent FISMA. Of the seven components notified of security weaknesses during fiscal year 2005 network, database and US-VISIT audits (CBP, CIS, EP&R, TSA, USCG, USSS, and US-VISIT), only EP&R had established POA&Ms for all identified weaknesses.
- The CISO has not established detailed procedures to review the component's POA&M information for accuracy, completeness, and quality at least quarterly, as required by OMB. DHS plans to hire a contractor to conduct component site visits, which would include detailed reviews of the POA&M process, including reviewing the quality and completeness of the component's POA&M data. The methodology of the reviews has not been established.
- Based on our review of data in Trusted Agent FISMA as of August 22, 2005, we determined that ten components did not appropriately assign security responsibilities for their respective systems. Specifically, CBP, CIS, IAIP, ICE, Infrastructure, Office of Domestic Preparedness (ODP), S&T, TSA, USCG, and USSS each had three or more major applications or general support systems with no security personnel identified in Trusted Agent FISMA - including TSA and USCG which

each had 15 systems with no designated personnel. Further, four components had designated one person as the ISSO for numerous major applications or general support systems (e.g., CIS-24 systems, IAIP-16 systems, USCG-144 systems, USSS-39 systems).

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

OIG Assessment of the Certification and Accreditation Process

DHS has implemented a departmental C&A tool. However, we determined that many C&A packages did not contain all of the required documents. In addition, the majority of DHS' systems have not been certified and accredited.

PROGRESS

- DHS deployed a C&A tool to establish a standard process to certify and accredit IT systems. For all C&A's beginning in April 2005, components were required to use the tool to accredit all unclassified and collateral classified systems.
- DHS issued guidance to assist components in determining system impact levels in accordance with FIPS 199.

ISSUES TO BE ADDRESSED

- Our review of 16 certification and accreditation packages at nine components found 15 instances in which accreditation packages were incomplete. Specifically, systems were accredited, although some key security documents were either not prepared, in draft, or did not meet all applicable OMB and National Institute of Standards and Technology (NIST) guidelines. Documents include system security plans, risk assessments, FIPS 199 security categorizations, privacy impact assessments, e-authentication assessments, memorandum of understandings, contingency plans, and contingency plan testing.
- Components have not defined impact levels according to FIPS 199 for all systems in Trusted Agent FISMA.
- Components have not performed privacy impact assessments for all systems.
- The CISO requires Authority to Operate (ATO) memorandums to be uploaded into Trusted Agent FISMA in order for a system to be counted as accredited. Our review of 215 ATO letters in Trusted Agent FISMA on May 31, 2005 disclosed some were not valid. Specifically, nine were Interim ATO letters, nine were

recommendations for ATO, eight were ATO letters for a different system, two were not ATO letters, and two were blank documents.

- As of August 26, 2005, only 32 percent of DHS' 795 operational systems have been certified and accredited.

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

Agencywide Security Configuration Requirements

DHS has issued baseline software security configuration guides for many of its systems. However, the components have not implemented security configuration requirements for all systems.

PROGRESS

- DHS developed agencywide security baseline configuration guides for Windows 2000, Windows 2003/ XP Professional, Solaris, HP-UX, Linux, Cisco Routers, and Oracle database servers in November 2004.
- DHS requires that components ensure that the installation of hardware and software products meet the requirements specified in applicable DHS baseline configuration guides.
- Several of the components included in our review have developed their own baseline security configuration requirements, or incorporated some of the configuration guidelines published by DHS and other agencies (such as NIST, the National Security Agency [NSA], and the Defense Information Systems Agency [DISA]), for at least some of their applications and operating system environments. For example: CBP is using many sources as a baseline to develop its policies including DHS, NIST, NSA and DISA guidelines; and, USCG uses DISA guidelines as a baseline for its policies.

ISSUES TO BE ADDRESSED

- At the time of our review, baseline configuration guides had not been developed for all hardware and software systems in use at DHS (for example, Windows NT, Microsoft SQL Server database management system).
- Our review of four baseline configuration guides (Windows 2000, Linux, Solaris, and Oracle) disclosed that improvements are needed for three of the guides (Linux, Solaris, and Oracle) in order to properly secure DHS' systems. While DHS issued updated guides on September 1, 2005, we were unable to determine if the guides are adequate.

- DHS policy does not require that the components use NIST's security configuration checklists - NIST Special Publication (SP) 800-70 - for systems where DHS has not developed its own baseline configuration guides.
- DHS components have not implemented security configuration requirements for all of their systems.
- The CIO does not have a process to determine that components have implemented DHS baseline configurations.

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

Incident Detection, Handling, Reporting, and Analysis Procedures

DHS has not improved its incident detection, handling, reporting, 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.

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 tests.
- Vulnerability assessments performed at components reviewed during our network, database, and US-VISIT audits (CBP, CIS, EP&R, TSA, USCG, USSS, US-VISIT) identified security concerns resulting from inadequate password controls, patch management, and configuration management.
- 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. Four components (CBP, CIS, EP&R, FLETC) did not submit reports every week during a ten-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 FISMA report.[10]

[10] *Evaluation of DHS' Information Security Program for Fiscal Year 2004*, dated September 2004 (OIG-04-41).

- The department has not defined detailed procedures for the DHS CSIRC to perform department-wide security incident analysis. We reported a similar issue in our FY 2004 FISMA report.

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

Security Training Procedures

DHS needs to improve its security awareness and security professional training programs. The components have not identified all employees and contractors with significant security responsibilities or the specific training that is needed for these employees.

PROGRESS

- DHS has established an IT Security Training Working group, which meets monthly and includes representatives from all components. The goal of the group is to improve IT security training efforts throughout the department by developing an enterprise solution for security awareness and role-based training.
- DHS' Director for Information Security Training, Education, and Awareness conducted an assessment of each components' IT security training program in June 2005.
- DHS' Director for Information Security Training, Education, and Awareness is requiring each component to develop its security awareness, training, and education plan by September 1, 2005.

ISSUES TO BE ADDRESSED

- DHS has not implemented a department-wide web-based IT security training program to standardize security awareness training and to track the completion of the training. The training program was originally planned to be implemented in FY 2004 but is now projected to be implemented in FY 2006.
- Most of the components' IT security awareness training do not explain DHS' policy regarding peer-to-peer file sharing.
- DHS components have not identified all employees, including contractors, with significant IT security responsibilities or been able to ensure that employees in those positions have received the necessary specialized security training.
- The Department's Information Security Training, Education, and Awareness office (Training office) does not verify or validate the

training data reported by the components. The Training office relies on the component's ISSMs to review, summarize, and enter the training data into Trusted Agent FISMA for reporting.

- The Training office does not enforce the requirement that all employees and contractors complete refresher security awareness training by May 31st of each year, as stated in the DHS policy.
- As of August 2, 2005, none of the components had submitted an IT Security Awareness and IT Professional Training plan for this year. In addition, no training plans were submitted last fiscal year (DHS policy requires plans to be submitted by September 1st of each year).

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

Recommendations

We recommend that the DHS CIO:

1. Report the DHS information security program as a significant deficiency for FY 2005 in its POA&M.
2. Ensure that all operational systems are certified and accredited in accordance with applicable OMB and NIST guidance.
3. Establish a process to ensure that all data in Trusted Agent FISMA, including POA&Ms, is complete, accurate, and current.
4. Develop a process to maintain a current department-wide system inventory.

Management Comments and OIG Analysis

DHS agreed with recommendation 1. DHS has developed a detailed remediation plan for FY 2006 to improve its security program.

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

DHS agreed with recommendation 2. DHS deployed a C&A tool department-wide in April 2005 to be used to accredit all systems. Completion of accreditations of all systems is the goal of the DHS Information Security Program for FY 2006.

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

DHS agreed with recommendation 3. DHS has made over 100 upgrades in FY 2005 to Trusted Agent FISMA to improve the accuracy and completeness of the data. In FY 2006, DHS will identify other ways to improve the review process and increase accountability at the component level.

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

DHS agreed with recommendation 4. DHS completed a comprehensive inventory in FY 2005. The department recently implemented an inventory change control process, and plans on conducting periodic inventory updates with each component in FY 2006.

We agree that the steps DHS has taken, and plans to take 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. We evaluated DHS' progress in developing, managing, and implementing its information security program, too.

Our independent evaluation focused on DHS' information security program and practices, based on the requirements outlined in FISMA, and utilizing OMB Memorandum M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, issued on June 13, 2005. We conducted our work at the program level and at DHS' major organizational components (CBP, CIS, FLETC, ICE, IAIP, Management, OIG, S&T, TSA, USCG, and USSS).

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 organizational 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 16 systems at nine organizational components (CBP, CIS, FLETC, IAIP, ICE, Management, OIG, S&T, and USCG) to ensure that all of the required documents were completed prior to being accredited; and, evaluating DHS' major organizational components progress in developing, aligning, and managing their information security program and practices in compliance with DHS' agencywide information security program.

We conducted our review between April and September 2005 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 review are identified in Appendix J.

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 21, 2005

Memorandum For: Richard L. Skinner
Inspector General

From: Scott Charbo
Chief Information Officer

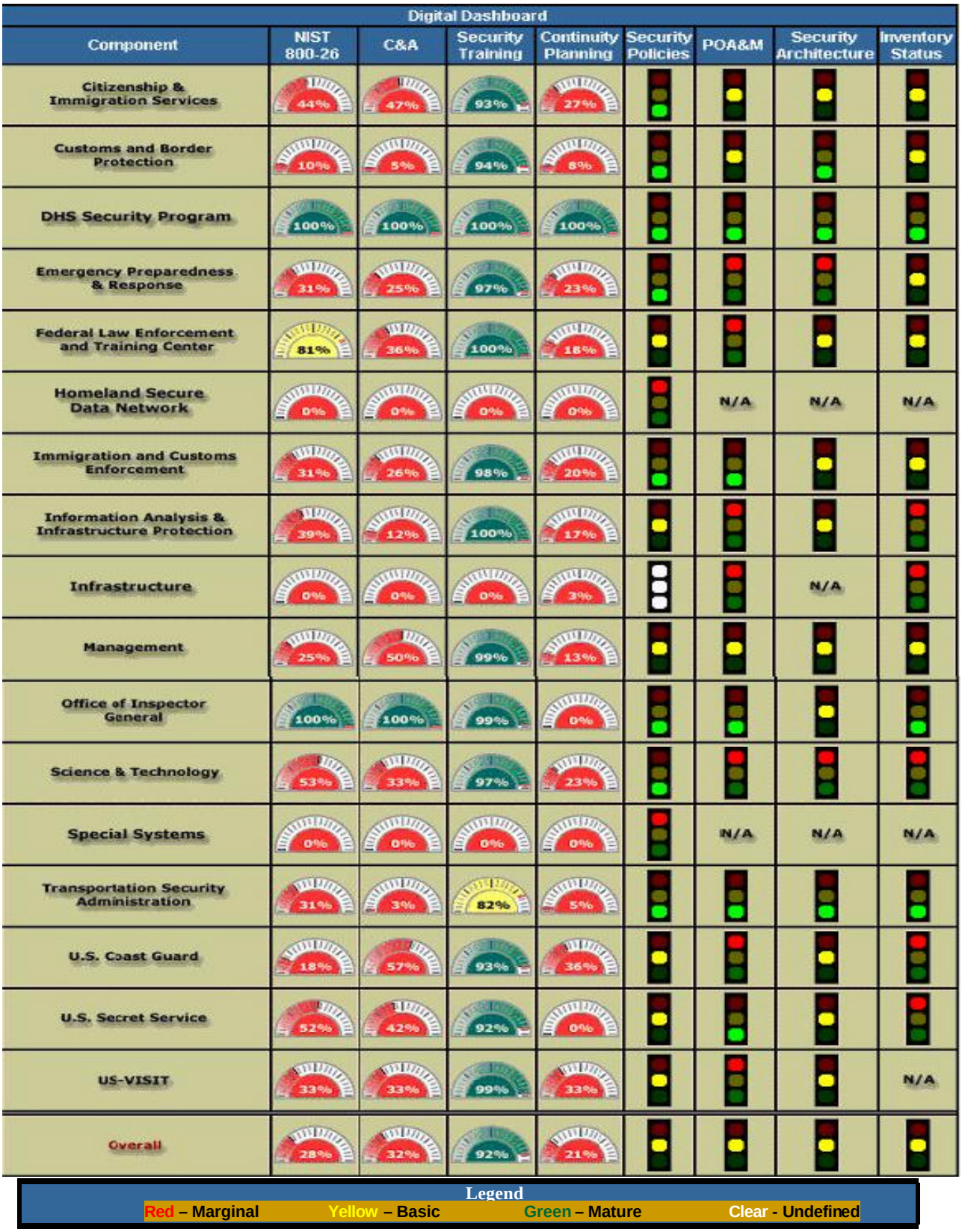
Subject: Office of Inspector General Report, *Evaluation of DHS' Information Security Program for Fiscal Year 2005*

Thank you for the opportunity to comment on the referenced report. I appreciate that the narrative report acknowledges the progress that my office has made in moving the Department's Information Security Program forward. The completion of a comprehensive IT system inventory and implementation of an enterprise Certification and Accreditation (C&A) Tool are highlighted as significant successes throughout the report, and those two milestones now provide a comprehensive baseline for executing a full remediation plan in Fiscal Year 2006.

I concur with your report and will implement remediation for your four major recommendations as described below:

1. **Report the DHS IT security program as a significant deficiency for FY 2005 in its Plan of Attack and Milestones (POA&M).** A detailed remediation plan has been developed for fiscal year 2006, and our goal is 100% accreditation by the end of the year.
2. **Ensure that all operational systems are certified and accredited in accordance with applicable OMB and NIST guidance.** 100% completion of systems' accreditation is the top goal of the DHS Information Security Program for Fiscal Year 2006. Our newly deployed C&A tool incorporates all current federal requirements, including both NIST and OMB guidance, and it is for this reason that the use of the tool is now mandatory throughout the Department.
3. **Establish a process to ensure that all data in Trusted Agent FISMA, including POA&Ms, is complete, accurate, and current.** In response to earlier OIG findings, we have already made over 100 upgrades to Trusted Agent FISMA to improve the accuracy and completeness of the data. In Fiscal Year 2006, we will work to identify other ways to improve the Headquarters' review process and increase accountability at the Component level.

4. **Develop a process to maintain a current department-wide system inventory.** In Fiscal Year 2005, the Department completed a comprehensive inventory for all information technology systems in use by the Department. The Department has recently implemented an inventory change control process, and is planning to conduct periodic inventory updates with each component to ensure continued accuracy of data in the future.



Digital Dashboard								
Component	NIST 800-26	C&A	Security Training	Continuity Planning	Security Policies	POA&M	Security Architecture	Inventory Status
Citizenship & Immigration Services	44%	47%	93%	27%				
Customs and Border Protection	10%	5%	94%	8%				
DHS Security Program	100%	100%	100%	100%				
Emergency Preparedness & Response	31%	25%	97%	23%				
Federal Law Enforcement and Training Center	81%	36%	100%	18%				
Homeland Secure Data Network	0%	0%	0%	0%		N/A	N/A	N/A
Immigration and Customs Enforcement	31%	26%	98%	20%				
Information Analysis & Infrastructure Protection	39%	12%	100%	17%				
Infrastructure	0%	0%	0%	3%			N/A	
Management	25%	50%	99%	13%				
Office of Inspector General	100%	100%	99%	0%				
Science & Technology	53%	33%	97%	23%				
Special Systems	0%	0%	0%	0%		N/A	N/A	N/A
Transportation Security Administration	31%	3%	82%	5%				
U.S. Coast Guard	18%	57%	93%	36%				
U.S. Secret Service	52%	42%	92%	0%				
US-VISIT	33%	33%	99%	33%				N/A
Overall	28%	32%	92%	21%				

Legend

Red – Marginal Yellow – Basic Green – Mature Clear - Undefined

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 in FY 05 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. FY 05 Agency Systems		b. FY 05 Contractor Systems		c. FY 05 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		3		1		4	4	100.0%	3	75.0%	4	100.0%
	Moderate		2		0		2	2	100.0%	2	100.0%	2	100.0%
	Sub-total		**5**		**1**		**6**	**6**	**100.0%**	**5**	**83.3%**	**6**	**100.0%**
CIS	High		0		2		2	2	100.0%	0	0.0%	0	0.0%
	Moderate		1		2		3	3	100.0%	0	0.0%	0	0.0%
	Sub-total		**1**		**4**		**5**	**5**	**100.0%**	**0**	**0.0%**	**0**	**0.0%**
EP&R	High		9		1		10	3	30.0%	2	20.0%	0	0.0%
	Moderate		1		1		2	0	0.0%	0	0.0%	0	0.0%
	Sub-total		**10**		**2**		**12**	**3**	**25.0%**	**2**	**16.7%**	**0**	**0.0%**
FLETC	High		2		0		2	2	100.0%	0	0.0%	0	0.0%
	Sub-total		**2**		**0**		**2**	**2**	**100.0%**	**0**	**0.0%**	**0**	**0.0%**
IAIP	High		1		1		2	0	0.0%	0	0.0%	0	0.0%
	Sub-total		**1**		**1**		**2**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
ICE	High		1		1		2	2	100.0%	0	0.0%	1	50.0%
	Sub-total		**1**		**1**		**2**	**2**	**100.0%**	**0**	**0.0%**	**1**	**50.0%**
MGMT	High		1		0		1	0	0.0%	0	0.0%	1	0.0%
	Moderate		0		1		1	1	100.0%	1	100.0%	1	100.0%

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
	Sub-total		**1**		**1**		**2**	**1**	**50.0%**	**1**	**50.0%**	**1**	**50.0%**
OIG	High		2		0		2	2	100.0%	0	0.0%	0	0.0%
	Sub-total		**2**		**0**		**2**	**2**	**100.0%**	**0**	**0.0%**	**0**	**0.0%**
ODP	High		1		0		1	1	100.0%	0	0.0%	0	0.0%
	Sub-total		**1**		**0**		**1**	**1**	**100.0%**	**0**	**0.0%**	**0**	**0.0%**
S&T	High		0		1		1	1	100.0%	0	0.0%	0	0.0%
	Moderate		1		0		1	1	100.0%	0	0.0%	0	0.0%
	Sub-total		**1**		**1**		**2**	**2**	**100.0%**	**0**	**0.0%**	**0**	**0.0%**
TSA	High		0		1		1	0	0.0%	0	0.0%	0	0.0%
	Moderate		0		2		2	0	0.0%	0	0.0%	0	0.0%
	Not Categorized		2		2		4	0	0.0%	0	0.0%	0	0.0%
	Sub-total		**2**		**5**		**7**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
US-Visit	High		0		1		1	1	100.0%	1	100.0%	0	0.0%
	Moderate		0		1		1	1	100.0%	1	100.0%	0	0.0%
	Sub-total		**0**		**2**		**2**	**2**	**100.0%**	**2**	**100.0%**	**0**	**0.0%**
USCG	High		2		1		3	3	100.0%	1	33.3%	0	0.0%
	Moderate		5		2		7	1	14.3%	3	42.9%	0	0.0%
	Not Categorized		4		0		4	2	50.0%	0	0.0%	0	0.0%
	Sub-total		**11**		**3**		**14**	**6**	**42.9%**	**4**	**28.6%**	**0**	**0.0%**
USSS	High		3		0		3	3	100.0%	0	0.0%	0	0.0%
	Moderate		1		0		1	0	0.0%	1	100.0%	0	0.0%
	Sub-total		**4**		**0**		**4**	**3**	**75.0%**	**1**	**25.0%**	**0**	**0.0%**
Agency Totals	**High**		**25**		**10**		**35**	**24**	68.6%	**7**	20.0%	**5**	14.3%
	Moderate		**11**		**9**		**20**	**9**	45.0%	**8**	40.0%	**3**	15.0%
	Low		**0**		**0**		**0**	**0**		**0**		**0**	
	Not Categorized		**6**		**2**		**8**	**2**	25.0%	**0**	0.0%	**0**	0.0%
	Total		**42**		**21**		**63**	**35** (b)	55.6%	**15**	23.8%	**8**	12.7%

Comments:

(a) Since we are only reporting the number of systems that we reviewed, the total number and number reviewed is the same. See the CIO's report for the total number of systems for each component.

(b) The number of systems with a current C&A is based on an ATO letter, not on the adequacy of the documents required. As noted in Appendix F, 15 of the 16 accreditation packages that the OIG reviewed were incomplete.

Question 3 – System Inventory and IT Security Performance		
In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.		
3.a.	The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. Self-reporting of NIST Special Publication 800-26 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient. Response Categories: - Rarely, for example, approximately 0-50% of the time - Sometimes, for example, approximately 51-70% of the time - Frequently, for example, approximately 71-80% of the time - Mostly, for example, approximately 81-95% of the time - Almost Always, for example, approximately 96-100% of the time	- Rarely, for example, approximately 0-50% of the time (a)
3.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. Response Categories: - Approximately 0-50% complete - Approximately 51-70% complete - Approximately 71-80% complete - Approximately 81-95% complete - Approximately 96-100% complete	- Approximately 96-100% complete
3.c.	The OIG **generally** agrees with the CIO on the number of agency owned systems.	Yes
3.d.	The OIG **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
3.e.	The agency inventory is maintained and updated at least annually.	No (b)
3.f.	The agency has completed system e-authentication risk assessments.	No

Comments:

(a) DHS requires contractor systems to be evaluated in the same manner as agency owned systems. However, as of August 26, 2005, only 46% of contractor systems have been reviewed this fiscal year.

(b) DHS recently completed its first comprehensive system inventory. DHS has not developed a process that it will use to update its system inventory beginning next year.

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 do wn 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		
4.a.	The POA&M is an agency wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	- Rarely, for example, approximately 0-50% of the time (a)
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	- Rarely, for example, approximately 0-50% of the time (b)
4.c.	Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	- Frequently, for example, approximately 71-80% of the time (c)
4.d.	CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	- Sometimes, for example, approximately 51-70% of the time (d)
4.e.	OIG findings are incorporated into the POA&M process.	- Sometimes, for example, approximately 51-70% of the time (e)
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources	- Rarely, for example, approximately 0-50% of the time (f)

Comments:

(a) DHS requires all known IT security weaknesses be included in Trusted Agent FISMA. As of August 22, 2005, only 35 percent of the 791 operational applications and general support systems in Trusted Agent FISMA had POA&Ms. Since only 32% of the operational systems have a completed C&A (see Appendix C), there should be at a minimum, at least one POA&M (lack of completed C&A) for 68% of the systems.

(b) DHS requires components to create POA&Ms for all IT security weaknesses. However, most of the POA&Ms do not contain all required information, such as resources required.

(c) The CIO does not ensure that components update the status of their remediation progress. As of August 22, 2005, 27% of open POA&Ms had an estimated completion date before July 22, 2005 (which includes 2% that had not been updated in over one year).

(d) While the CIO reports to OMB quarterly on the status of its POA&Ms, the CIO does not ensure that the information in the POA&M is complete and accurate. The CIO relies on the component ISSMs to review and update their POA&Ms on a monthly basis.

(e) While the CIO requires all OIG findings be included in each component's POA&M, we noted OIG findings at six components that were not incorporated into a POA&M.

(f) Most of the components do not have a formal process to prioritize its POA&Ms.

Question 5 – OIG Assessment of the C&A Process	
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, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May, 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans.	
Assess the overall quality of the Department's certification and accreditation process. Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Poor [(a)]

Comments:

(a) Our review of 16 certification and accreditation packages at nine components found 15 instances in which the accreditation packages were incomplete. Specifically, systems were accredited, although some key security documents were either not prepared, in draft, or did not meet all applicable OMB and NIST guidelines. Documents include system security plans, risk assessments, FIPS 199 security categorizations, privacy impact assessments, e-authentication assessments, memorandum of understandings, contingency plans, and contingency plan testing.

Note: The implementation of the department-wide C&A tool (required use as of April 2005) may improve the quality of the C&A packages in the future.

Question 6 – Agencywide Security Configuration Requirements		
6.a.	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 baseline configuration guides. However, DHS has not developed configuration guides for all hardware and software systems being used by its components.		
6.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. Specify:	N/A		

Comments:

(a) While many of the components use standard configurations for some of their systems, most have not implemented DHS' configuration guides that were issued in November 2004. In addition, the CIO has not verified or determined whether components are using DHS standard configurations (or any other standard configurations).

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.		
7.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes [(a)]
7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	No [(b)]
7.c.	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, we determined that during a ten-week period in 2005, four major components (CBP, CIS, EP&R, FLETC) did not submit reports every week.

(b) We again determined that DHS has not documented detailed procedures for reporting incidents to law enforcement authorities.

Question 8 – Security Training Procedures	
Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Response Choices include: - Rarely, or, approximately 0-50% of employees have sufficient training - Sometimes, or approximately 51-70% of employees have sufficient training - Frequently, or approximately 71-80% of employees have sufficient training - Mostly, or approximately 81-95% of employees have sufficient training - Almost Always, or approximately 96-100% of employees have sufficient training	- Mostly, or, approximately 81-95% of employees have sufficient training

Comments: Eight of the components reviewed have established a process to determine that all employees, including contractors, receive IT security awareness training. Components have not identified all of the employees with significant IT responsibility, or have established the type of specialized training to be provided to such employees. The CIO does not perform any verification of the number of employees that the components report as being trained.

Question 9 – Security Training Procedures	
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.	No

Comments: Most of the component's IT security awareness training materials do not explain DHS' policy regarding Peer-to-Peer file sharing risks.

Information Security Audit Division

Edward G. Coleman, Director
Jeff Arman, Audit Manager
Patrick Nadon, Audit Manager
Chiu-Tong Tsang, Senior IT Auditor
Jason Bakelar, Senior IT Auditor
Pedro Calderon, IT Auditor
Chris Udoji, IT Auditor
Swati Mahajan, IT Auditor
Scott Binder, IT Auditor
Kelby Funn, IT Auditor
Charles Twitty, Referencer

Advanced Technology Division

Jim Lantzy, Director
Michael Goodman, Security Engineer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
General Counsel
Executive Secretariat
Chief Information Officer
Chief Financial Officer
Chief Information Security Officer
Public Affairs
Legislative Affairs
Office of Security
Director, Departmental GAO/OIG Liaison Office
Director, Compliance and Oversight Program
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.

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