DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Evaluation of DHS' Information Security Program for Fiscal Year 2004

Office of Information Technology

OIG-04-41

September 2004

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, investigative, and special reports prepared by the OIG as part of its DHS oversight responsibility to identify and prevent fraud, waste, abuse, and mismanagement.

This report assesses the strengths and weaknesses of the program or operation under review. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to the OIG, and have been discussed in draft with those responsible for implementation. It is my hope that this report will result in more effective, efficient, and economical operations. I express my appreciation to all of those who contributed to the preparation of this report.

Clark Kent Ervin
Inspector General

Contents

Appendices

Abbreviations

ATO	Authority to Operate
C&A	Certification and Accreditation
CBP	United States Customs and Border Protection
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIS	United States Citizenship and Immigration Services
CISO	Chief Information Security Officer
COMSEC	Communications Security
COOP	Continuity of Operations Plan
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 Directorate
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act

Contents

FY	Fiscal Year
IAIP	Information Analysis and Infrastructure Protection Directorate
IATO	Interim Authority to Operate
ICE	United States Immigration and Customs Enforcement
IRP	Information Requirements Plan
IS	Information System
ISSB	Information Systems Security Board
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
MD	Management Directive
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security Systems
OCIO	Office of the Chief Information Officer
OE	Organizational Element
OIG	Office of Inspector General
OMB	Office of Management and Budget
PAR	Performance & Accountability Report
POA&M	Plan of Action and Milestones
Pub	Publication
S&T	Science and Technology Directorate
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

Introduction

Due to the increasing threat to information systems and the highly networked nature of the federal computing environment, the Congress, in conjunction with the Office of Management and Budget (OMB), requires an annual review and reporting of agencies' compliance with the requirements under the Federal Information Security Management Act (FISMA) of 2002.[1] FISMA focuses on the program management, implementation, and evaluation of the security of unclassified, classified, and national security systems (NSS).[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' established processes and the progress DHS has made in implementing its agencywide information security program. In doing so, we specifically assessed DHS' Plan of Action and Milestones (POA&M) and certification and accreditation (C&A) processes. We also focused on whether DHS' major organizational components are aligning their information security program and practices with DHS' agencywide information security program. Additionally, we tested the effectiveness of information technology (IT) security controls for a subset of DHS' information systems. We did not gather statistical data for incident reporting and analysis or training as part of our evaluation.

We performed our work at both the program and the organizational component levels. The following major organizational components were included in our

[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.

review: United States Customs and Border Protection (CBP), Emergency Preparedness and Response Directorate (EP&R); Information Analysis and Infrastructure Protection Directorate (IAIP); United States Immigration and Customs Enforcement (ICE), Science and Technology Directorate (S&T); Transportation Security Administration (TSA), United States Citizenship and Immigration Services (CIS), United States Coast Guard (USCG); and United States Secret Service (USSS). We also included the Office of Inspector General (OIG) in our evaluation. See Appendix A for a detailed discussion of our purpose, scope, and methodology.

Background

The E-Government Act of 2002 (Public Law 107-347), signed into law by the President on December 17, 2002, recognized the importance of information security[3] to the economic and national security interests of the United States. Title III of the E-Government Act, entitled FISMA, provides a comprehensive framework for ensuring 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 provide security for 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 are to independently evaluate the effectiveness of an agency's information security program and practices on an annual basis.

OMB issued memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, on August 23, 2004. The memorandum provides updated instructions for agency and OIG reporting under FISMA. This annual evaluation summarizes the results of our review of DHS' IT security program and practices according to OMB's instructions.

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

In addition to our independent evaluation, we conducted reviews of DHS' information systems and security program related areas throughout Fiscal Year (FY) 2004. This report summarizes the results of a limited number of systems evaluated during our on-going financial statement and classified systems reviews. It also includes results from an on-going audit of remote access, and reports issued on wireless security,[4] DHS' efforts to implement *The National Strategy to Secure Cyberspace*,[5] and DHS' IT management structure.[6]

Results in Brief

DHS has made significant progress over the last year in developing, managing, and implementing its information security program at the departmental level. DHS' Information Security Program Strategic Plan[7] provides the foundation for an agencywide, consolidated information security program. In this plan, DHS' Chief Information Officer (CIO) and Chief Information Security Officer (CISO) identify eight distinct security program areas, as shown in Figure 1. These areas are essential to provide security services that protect the confidentiality, integrity, and availability of information, and to assign accountability for the administration of DHS' networks and computing platforms. The strategic plan also describes the goals and objectives for establishing a dynamic information security organization over the next five years.

DHS' CIO, who has oversight responsibilities for DHS' information security program, has delegated the CISO, as required under FISMA, the authority to establish information security policies and procedures throughout the department. Under this authority, the CISO developed the Information Security Program Management Plan,[8] which is the CISO's blueprint for managing DHS' information security program. The CISO also developed and issued an Information Security Risk Management Plan,[9] which documents DHS' plan for developing, implementing, and institutionalizing a risk management process in support of its information security program.

The CISO updated the baseline IT security policies and procedures in Management Directive (MD) 4300; Sensitive Systems Policy Publication 4300A and its companion, the Sensitive Systems Handbook; and National Security

[4] *Inadequate Security Controls Increase Risks to DHS' Wireless Networks*, OIG-04-27, June 2004.

[5] *Progress and Challenges in Securing the Nation's Cyberspace*, OIG-04-29, July 2004.

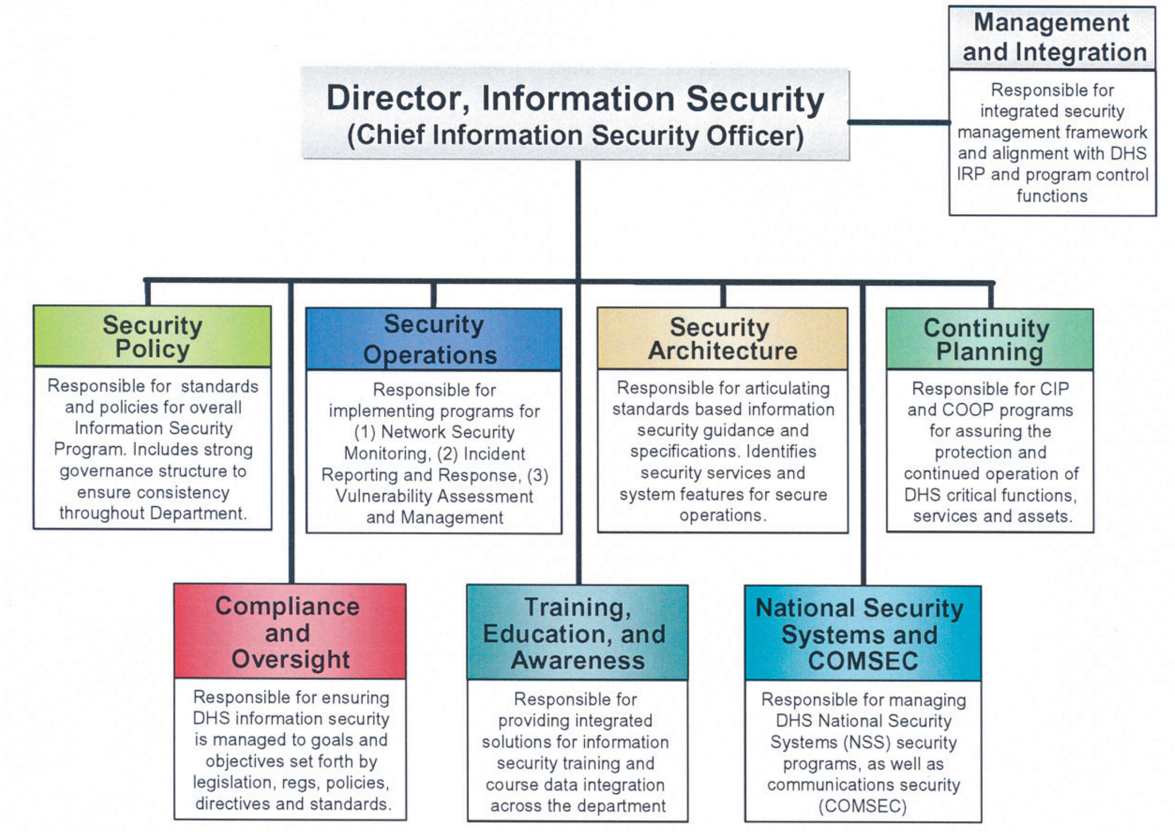
[6] *Improvements Needed to DHS' Information Technology Management Structure*, OIG-04-30, July 2004.

[7] Final, version 1, dated April 4, 2004.

[8] Version 1.0, dated June 15, 2004.

[9] Version 1, dated June 9, 2004.

Systems Policy Publication 4300B and its companion, the National Security Systems Handbook.[10] Additionally, DHS issued the *ISSM Guide to the DHS Information Security Program* (ISSM Guide),[11] which outlines the specific responsibilities for the components' Information Systems Security Managers (ISSM) and Information Systems Security Officers (ISSO). The guidelines provide the ISSMs with the guidance and procedures needed to align their security programs with DHS' Information Security Program. 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.


Director, Information Security
(Chief Information Security Officer)
Management and Integration
Responsible for integrated security management framework and alignment with DHS IRP and program control functions
Security Policy
Responsible for standards and policies for overall Information Security Program. Includes strong governance structure to ensure consistency throughout Department.
Security Operations
Responsible for implementing programs for (1) Network Security Monitoring, (2) Incident Reporting and Response, (3) Vulnerability Assessment and Management
Security Architecture
Responsible for articulating standards based information security guidance and specifications. Identifies security services and system features for secure operations.
Continuity Planning
Responsible for CIP and COOP programs for assuring the protection and continued operation of DHS critical functions, services and assets.
Compliance and Oversight
Responsible for ensuring DHS information security is managed to goals and objectives set forth by legislation, regs, policies, directives and standards.
Training, Education, and Awareness
Responsible for providing integrated solutions for information security training and course data integration across the department
National Security Systems and COMSEC
Responsible for managing DHS National Security Systems (NSS) security programs, as well as communications security (COMSEC)

Source: ISSM Guide

[10] The latest versions of 4300A, 4300B, and their corresponding handbooks, are dated July 26, 2004.

[11] Version 2.0, dated July 19, 2004.

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.[12] The information used to develop the digital dashboard comes from DHS' enterprise management tool, Trusted Agent FISMA. See Appendix C for the digital dashboard as of September 18, 2004.

Even though DHS has made several improvements in its information security program, the organizational components have not yet fully aligned their respective security programs with DHS' overall policies, procedures, and practices. For example:

- DHS cannot effectively manage its information security program while lacking an accurate and complete system inventory. DHS has begun an effort with an outside contractor to identify and establish an agencywide system inventory. With the exception of IAIP, most components have made attempts to identify their inventory of programs and systems, including those that are contractor owned or operated.
- Although defined a number of times, ISSMs for five of the nine components (CBP, EP&R, IAIP, S&T, and USSS) contacted us for additional clarification on the definition of programs and systems. This continued lack of understanding by those responsible for identifying required program and system information, has hindered DHS' ability to compile a comprehensive system inventory.
- As reported in our FY 2003 security program evaluation, DHS' organizational components are not ensuring that all IT security weaknesses are included in POA&Ms. Therefore, DHS cannot effectively oversee and measure component-level FISMA metrics.
- FISMA metrics data, captured within Trusted Agent FISMA, is not comprehensively verified. Until this verification is accomplished, DHS cannot rely totally on the information reported by the organizational components in Trusted Agent FISMA, which impacts overall security program management.
- Most component-level policies and procedures are in draft, such as those for C&A, and have not been formally approved or communicated to program officials and members of the IT security organizations. For example, only

[12] These metrics include the percentage of systems and projects with adequate life cycle security requirements funding, systems accredited, systems and applications for which an annual self-assessment has been completed, personnel (employees and contractors) with network accounts that completed security awareness, and IT security professionals trained.

three components (EP&R, ICE, and USCG) have updated their C&A policies to ensure their compliance with MD 4300 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37.[13]

While DHS has issued considerable guidance, we identified areas where agencywide information security procedures require strengthening: (1) wireless technologies according to NIST SP 800-48; (2) protecting critical infrastructures from cyber vulnerabilities and threats; (3) remote access to DHS' systems; (4) vulnerability scanning; (5) penetration testing; (6) incident detection, analysis, and reporting; (7) security configuration polices and procedures; (8) specialized security training; and (9) IT security training costs.

Additionally, although the DHS' CIO is charged with implementing DHS' agencywide information security program, the CIO is not a member of the department's senior management team. Therefore, the CIO does not have the authority to strategically manage agencywide IT programs, systems, or investments. There is no formal reporting relationship between the DHS CIO and the component CIOs or between the CISO and the ISSMs. The lack of a formal reporting structure between the DHS CIO and CISO with the organizational components hinders agencywide support in implementing its information security program.[14]

We made specific recommendations to assist DHS in the development and implementation of its information systems security program in our FY 2003 report. While a few of these recommendations were implemented, such as the certification of Trusted Agent FISMA and the reporting of DHS' information systems security program as a material weakness, recommendations related to the tracking and remediation of material weaknesses and completion of a system inventory remain open. We recommend that DHS continue to consider its information systems security program a significant deficiency for FY 2004.

We obtained written comments on a draft of this report from DHS' CIO. DHS generally concurred with the report's recommendations and has already initiated several projects in the later part of FY 2004 that address some of the

[13] NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, dated May 2004, provides guidelines for the C&A of information systems to help achieve more secure systems supporting executive agencies of the federal government. Security certification and accreditation are important activities that support a risk management process and are an integral part of an agency's information security program.

[14] *Improvements Needed to DHS' Information Technology Management Structure*, OIG-04-30, July 2004.

recommendations. These include a system inventory project that is working towards a comprehensive inventory of DHS' general support systems and major applications. Similarly, a project to review and verify FISMA metrics data captured within an automated system was recently initiated. These and other activities will continue to be implemented in FY 2005 to improve the communication between the CISO and DHS' components, and to increase the accountability of the components. See Appendix B for DHS' comments in their entirety.

Results of Independent Evaluation

System Inventory and IT Security Performance

Progress

- DHS hired a contractor, who has developed a system inventory methodology. Under the methodology, a consistent approach will be used to identify an inventory of DHS' systems across the organizational components, including contractor run systems. It will also help the department maintain an agencywide inventory of systems, major applications, networks, and interfaces that is consistent with its information systems security program. The OIG has reviewed the methodology and provided a listing of the components' systems. The contractor began interviews with the first of DHS' organizational components, TSA, on September 9, 2004.
- The ISSM Guide documents DHS' policy for conducting annual self-assessments for all programs and systems according to NIST SP 800-26.[15] It also adequately defines the requirements for POA&M reporting, including the ISSMs' duties and responsibilities for developing and managing the POA&M process at the organizational component level.
- DHS has adopted an enterprise management tool, Trusted Agent FISMA, to collect and track data related to all FISMA metrics, including self-assessment data. Trusted Agent FISMA also collects data on other FISMA metrics, such as the number of systems with contingency plans, system contingency plans tested, systems certified and accredited, and employees that have received

[15] NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, dated November 2001, provides guidance for performing systems self-assessments for 17 different control areas, such as those pertaining to identification and authentication and contingency planning. In addition, the guide provides control objectives and techniques that can be measured for the control areas. Self-assessments provide a method for agency officials to determine the current status of their information security programs, and where necessary, establish a target for improvement.

IT security awareness training. DHS has mandated that the organizational components enter metrics data in Trusted Agent, and requires that the information be updated every 30 days.

- DHS issued guidance, which references OMB M-04-04 and NIST SP 800-63, for conducting electronic authentication (E-authentication) risk assessments.[16] Three organizational components (CBP, USCG, and USSS) have begun E-authentication risk assessments.

Issues to be Addressed

- DHS has not yet compiled a comprehensive inventory of its programs and systems, nor identified its major applications or nationally critical systems. Without a complete and accurate inventory of its information systems, DHS cannot manage effectively its information systems security program or test and evaluate adequately the effectiveness of the information security controls over its mission critical resources.
- In FY 2003, DHS hired a contractor to develop an inventory of DHS' major applications and general information support systems from February to April 2003. At that time, the CIO believed that the contractor had identified 90 to 95 percent of all information systems within DHS. In FY 2004, DHS hired another contractor to identify its system inventory for FISMA purposes.
- DHS' policy and procedures do not provide organizational components with guidance on conducting reviews of their contractor or other agency-provided services. Further, there was little evidence that components are ensuring that contractor or other agency provided services are secure and comply with DHS' security program requirements.
- In an attempt to validate DHS' self-assessment process, we selected a sample of NIST SP 800-26 evaluations completed by seven organizational components (CBP, CIS, EP&R, ICE, S&T, USCG, and USSS). We then independently scored each question and compared our results to the components' completed questionnaires. In several instances, we noted that we scored components either higher or lower for specific questions. We

[16] E-authentication is the process of establishing confidence in user identities electronically presented to an information system. OMB-04-04, *E-Authentication Guidance for Federal Agencies*, provides agencies with the criteria for determining the level of E-authentication assurance required for specific applications and transactions, based on the risks and their likelihood of occurrence for each application and transaction. NIST SP 800-63, *Electronic Authentication Guideline*, dated June 2004, provides technical guidance that supplements the OMB guidance, which defines four levels of authentication, Levels 1 to 4, in terms of the consequences of authentication errors and the misuse of credentials.

also identified that components did not properly define security weaknesses. Additionally, five components included in our review (CIS, EP&R, ICE, S&T, and USCG) did not develop POA&Ms for all system weaknesses identified through their NIST SP 800-26 self-assessments.

- With the exception of USSS, the results of self-assessments are not verified by the organizational components' CIOs.

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

Significant Deficiencies[17]

Progress

- DHS has developed a process to capture and report significant deficiencies in POA&Ms at the department level and for each organizational component.
- DHS' ISSM Guide requires the CISO to prioritize IT security weaknesses.

Issues to be Addressed

- DHS has not implemented fully a process for identifying, managing, or verifying the accuracy of significant deficiencies reported. In addition, known, significant deficiencies are not being prioritized for remediation.
- Two weaknesses are flagged as agencywide IT material weaknesses within Trusted Agent FISMA. However, within Trusted Agent, we identified inconsistencies in reporting of material weaknesses. For example, the Office of the CIO's (OCIO) POA&M reports two material weaknesses, but the "FY 2004 Material Weaknesses by Organizational Elements" report shows only the one significant deficiency reported in the Performance Accountability Report (PAR) for FY 2003.
- DHS does not have a process to ensure that all material weaknesses reported in the PAR and other sources (i.e., OIG audits, GAO audits, and NIST SP 800-26 assessments) are identified and documented in a POA&M for remediation.

[17] A significant deficiency is a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of information, information systems, personnel, or other resources, operations, or assets.

- Agencywide, material, IT security weaknesses have not been identified as significant deficiencies at the respective components.
- DHS' CIO does not have sufficient staff to manage, verify and/or assess the accuracy and consistency of significant deficiencies, evaluate and prioritize significant deficiencies for remediation, or verify that the significant deficiencies are linked to the budget and remediation process.[18]

See Appendix E for specific significant deficiencies identified.

OIG Assessment of the Plan of Action and Milestones Process

Progress

- DHS has developed an adequate process for reporting and capturing known security weaknesses in POA&Ms, as shown in Figure 2. DHS has also issued high-level guidance on the POA&M process.
- DHS has adopted an enterprise management tool, Trusted Agent FISMA, to collect and track data related to all POA&M activities, including self-assessment data. Trusted Agent FISMA also collects data on other FISMA metrics, such as the number of system contingency plans, system contingency plans tested, systems certified and accredited, and employees that have received IT security awareness training.
- A FISMA Management and Reporting Working Group, established in June 2004, meets monthly to foster a dialogue between the OCIO and the organizational components, obtain the components input on ways to improve the FISMA data collection effort, and address problems/issues that relate to the use of Trusted Agent FISMA.
- ISSOs are responsible for entering all known security weaknesses identified, as well as updating the progress for mitigating each of the security weaknesses, in Trusted Agent FISMA. ISSMs are responsible for reviewing the organizational components' POA&M data for consistency and accuracy.

Issues To Be Addressed

- DHS cannot rely on the accuracy and completeness of the data contained in Trusted Agent FISMA. Specifically, the information entered by the

[18] Improvements Needed to DHS Information Technology Management Structure, OIG-04-30, July 2004.

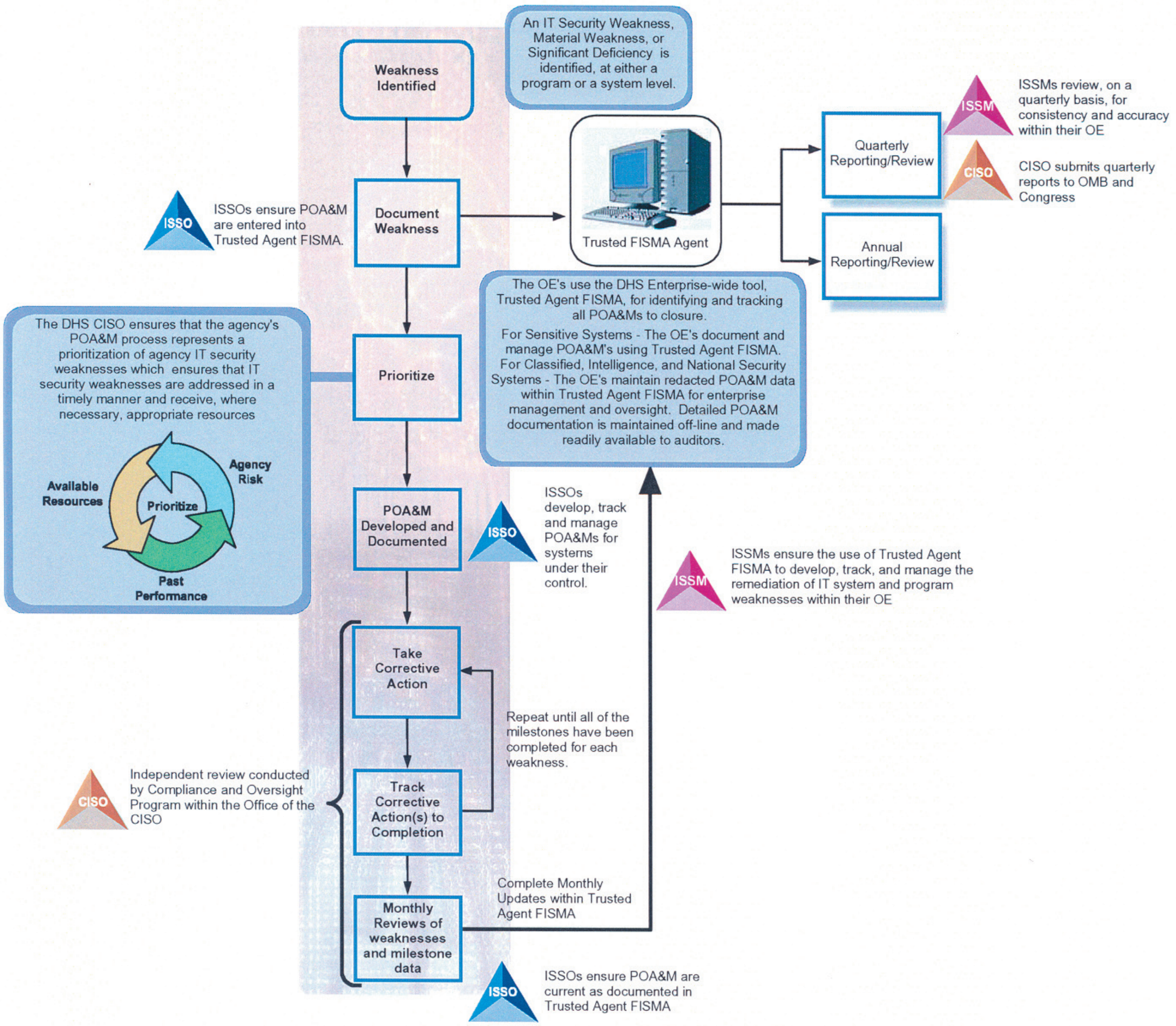
organizational components is not comprehensively verified; there is no audit trail capability; and some of the fields, such as the "Scheduled Completion Date" for POA&M milestones, can be arbitrarily revised by the organizational components. In August 2004, a contractor was brought on-board to do a complete review and analysis of DHS' POA&Ms.

- Seven of nine components (EP&R, IAIP, ICE, OIG, S&T, TSA, and USCG) have not documented and implemented their POA&M process to ensure that they contain all known security weaknesses, have been reviewed for accuracy and completeness, have been prioritized, and are in compliance with all applicable DHS policies.
- POA&M data in Trusted Agent FISMA is not current and is not updated periodically.
- DHS' CISO does not have the authority to oversee and ensure that the organizational components' implementation and management of the POA&M process complies with DHS' agencywide security program policies and procedures. Strong oversight is needed to ensure that DHS has an enterprise-wide, repeatable, and robust POA&M process for meeting FISMA's security requirements and to ensure accurate assessments of the aggregated security postures of each organizational component.
- System-level POA&Ms are not linked to individual components' budget submissions. The CISO does not enforce the requirement that components are to prioritize security weaknesses and estimate the funding necessary to mitigate the weaknesses identified in their POA&M submissions via Trusted Agent FISMA. Only one component (EP&R) had documentation that linked its system-level POA&Ms to its budget submission.
- OIG findings have not been incorporated into the POA&M process.
- Only four components (CBP, ICE, USCG, and USSS) stated that their program officials are involved in the POA&M process.
- Only three components (CBP, EP&R, and USCG) capture security weaknesses from all sources, as required by OMB,[19] in their POA&Ms.

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

[19] OMB's guidance requires agencies to capture all security weaknesses found during any review done by, for, or on behalf of the agency in its POA&Ms, including program reviews, OIG audits, GAO audits, financial system audits, and critical infrastructure vulnerability assessments.

Figure 2: DHS' POA&M Process



An IT Security Weakness, Material Weakness, or Significant Deficiency is identified, at either a program or a system level.

ISSOs ensure POA&M are entered into Trusted Agent FISMA.

ISSMs review, on a quarterly basis, for consistency and accuracy within their OE

CISO submits quarterly reports to OMB and Congress

The DHS CISO ensures that the agency's POA&M process represents a prioritization of agency IT security weaknesses which ensures that IT security weaknesses are addressed in a timely manner and receive, where necessary, appropriate resources

The OE's use the DHS Enterprise-wide tool, Trusted Agent FISMA, for identifying and tracking all POA&Ms to closure.

For Sensitive Systems - The OE's document and manage POA&M's using Trusted Agent FISMA. For Classified, Intelligence, and National Security Systems - The OE's maintain redacted POA&M data within Trusted Agent FISMA for enterprise management and oversight. Detailed POA&M documentation is maintained off-line and made readily available to auditors.

ISSOs develop, track and manage POA&Ms for systems under their control.

ISSMs ensure the use of Trusted Agent FISMA to develop, track, and manage the remediation of IT system and program weaknesses within their OE

Repeat until all of the milestones have been completed for each weakness.

Independent review conducted by Compliance and Oversight Program within the Office of the CISO

Complete Monthly Updates within Trusted Agent FISMA

ISSOs ensure POA&M are current as documented in Trusted Agent FISMA

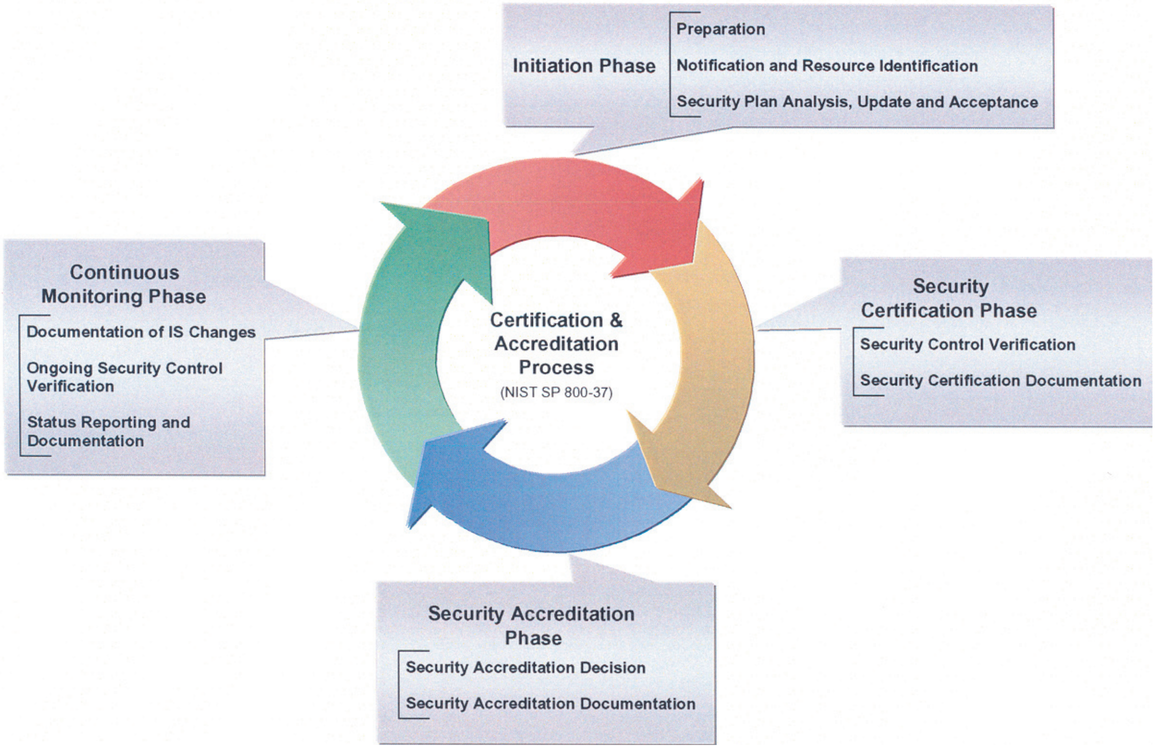
Source: ISSM Guide

OIG Assessment of the Certification and Accreditation Process

Progress

- Sensitive Systems Policy Publication 4300A specifies that the organizational components are to follow NIST SP 800-37 for all sensitive systems certified and accredited after May 2004. This process is documented in the ISSM Guide, as shown in Figure 3.
- In August 2004, DHS purchased a C&A tool. A decision on whether components will be required to use the tool will be made after a piloting phase. ICE is the primary component involved in the pilot effort.
- Four components (CBP, EP&R, ICE, and USSS) have a documented process for incorporating security costs into the system life cycle process.

Figure 3: DHS' C&A Process


Initiation Phase
Preparation
Notification and Resource Identification
Security Plan Analysis, Update and Acceptance
Security Certification Phase
Security Control Verification
Security Certification Documentation
Security Accreditation Phase
Security Accreditation Decision
Security Accreditation Documentation
Continuous Monitoring Phase
Documentation of IS Changes
Ongoing Security Control Verification
Status Reporting and Documentation
Certification & Accreditation Process
(NIST SP 800-37)

Source: ISSM Guide

Issues to be Addressed

- DHS may overstate the number of systems certified and accredited to OMB because Trusted Agent FISMA does not distinguish between systems with Interim Authority to Operate (IATO) and systems fully accredited with Authority to Operate (ATO). For example, three ICE systems listed as having ATOs in Trusted Agent FISMA, had only been granted IATOs. Systems with IATOs should not be included in an agency's count of its systems certified and accredited.
- DHS cannot identify systems that are due for recertification and accreditation based on the information reported in Trusted Agent FISMA.
- Five components (EP&R, IAIP, ICE, S&T, and USCG) reported that they did not have the ability to track the C&A status of the systems they identified in their inventory.
- Components have not defined impact levels for all systems in Trusted Agent FISMA according to draft Federal Information Processing Standard (FIPS) Publication (Pub) 199.[20]
- System accreditation packages for 12 systems included in our review did not meet all applicable OMB and NIST guidelines. Specifically, our quality reviews of the accreditation packages found instances in which systems were accredited even though: (1) key security documents (such as system security plans, risk assessments, and contingency plans) prepared did not meet all the requirements outlined in applicable NIST guidance; (2) documentation did not clearly indicate what residual risks the accrediting official was accepting in making the accreditation decision; and (3) contingency plans had not been developed or tested.
- Only three components (EP&R, ICE, and USCG) have updated their C&A policies to ensure that they are in compliance with Sensitive Systems Policy Publication 4300A and NIST SP 800-37. One component (CBP) indicated that it planned to use its existing policies to reaccredit its legacy systems instead of following NIST SP 800-37.
- Five components (IAIP, OIG, S&T, TSA, and USCG) lacked a solid, documented, and implemented process to ensure IT security costs are integrated into the system life cycle process.

[20] FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems*, dated December 2003, 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.

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

Agencywide Security Configuration Requirements

Progress

- DHS has developed agencywide security configuration polices and procedures for Windows 2000 and Solaris.
- 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 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 NSA and DISA guidelines as a baseline to develop its policies; IAIP uses NSA guidelines as a baseline for its policies; and USCG has produced its configuration policies.

Issues To Be Addressed

- Because DHS agencywide security configuration polices and procedures for Windows 2000 and Solaris were not issued until September 16, 2004, we were not able to evaluate the degree to which the guidelines address the patching of vulnerabilities or the extent to which they had been implemented. Policies and procedures for other applications and operating system environments have not yet been developed.
- None of the DHS components we reviewed have implemented security configuration requirements for all of their systems.

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

Incident Detection and Handling Procedures

Progress

- DHS has established and implemented agencywide policy and procedures for reporting incidents to United States Computer Emergency Readiness Team (US-CERT).[21]
- DHS has established a vulnerability assessment program.
- DHS employs various devices and technologies (such as network and host based intrusion detection devices, packet filtering, and proxy firewalls) to help protect against malicious activity and to mitigate its IT security risks.

Issues To Be Addressed

- DHS does not have reliable measures or a baseline to assess the results of its vulnerability scans or its penetration tests.
- DHS' vulnerability assessment program is not being enforced and does not have organizational component support. Therefore, DHS does not have a mechanism to collect and analyze the results of all its scans and tests.
- DHS does not have documented procedures for reporting incidents externally to law enforcement authorities.

See Appendix I for the Incident Detection and Handling Procedures.

Incident Reporting and Analysis

Progress

- DHS has established and implemented agencywide policy and procedures for reporting incidents internally.

[21] US-CERT, established in September 2003, is a public-private partnership charged with improving computer security preparedness and response to cyber attacks in the United States. Specifically, US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

Issues To Be Addressed

- DHS has not defined a process or procedures for incident analysis.
- DHS is not uniformly collecting OMB required information when incidents are reported, nor can it identify whether systems affected by an incident have been certified and accredited or whether required system patches have been installed.

Training

Progress

- DHS has established policies for security awareness training and the use of peer-to-peer sharing software on DHS computers.
- Additionally, ISSMs have been given the authority to develop their own information security training program, under the guidance of the Department's Program Manager for Information Security Training, Education, and Awareness.
- During FY 2004, three methods were available for ensuring employees and their contractors received annual security awareness training: CD, on-line tutorial, and classroom-based.

Issues To Be Addressed

- DHS' security awareness training does not explain policy on peer-to-peer file sharing.[22]
- Identification and management of all employees, contractors and other government personnel with access to component's information continues to be a challenge. Many organizational components identify who needs training based on whether they have an account on DHS' network.
- DHS has not identified employees with significant IT security responsibilities or been able to ensure that employees in those positions have received the necessary specialized security training. Only one of the components (CBP) has identified employees in those positions that need specialized training and ensured that required training was received.
- Costs associated with IT security training are not being captured.

[22] This answers question G.2.a from the OMB reporting requirements for Section G, Training.

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 also 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, as outlined in OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*. We conducted our work at the program level and at DHS' major organizational components (CBP, EP&R, IAIP, ICE, S&T, TSA, USCG, and USSS), including the OIG.

As part of our evaluation of DHS' compliance with FISMA, we tested the effectiveness of IT security controls for a subset of DHS' information systems. We also assessed DHS' compliance with the security requirements mandated by FISMA and other federal information systems security policies, procedures, standards, and guidelines; including NIST SP 800-26, NIST SP 800-37, and FIPS Pub 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) identified the policies, procedures, and practices that DHS has at the program level and at the organizational component level; (4) evaluated processes (i.e., 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.

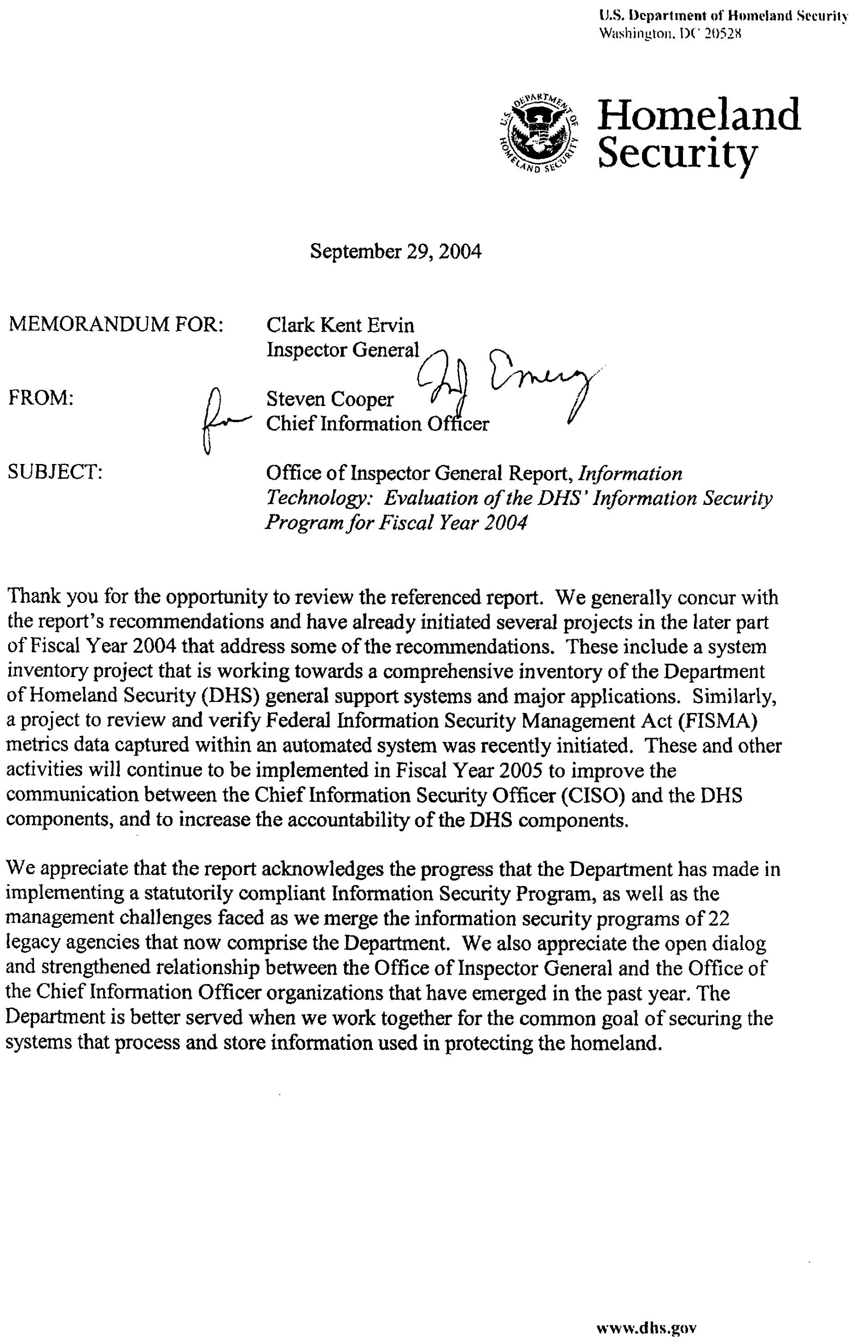
Though we evaluated DHS' processes for incident reporting and analysis and security training, we did not gather statistical information to complete the applicable OMB tables for these areas. We determined that we would rely on the data DHS collected to complete these tables.

OIG audit contractors were responsible for: (1) testing DHS' compliance with an abbreviated version of NIST SP 800-26 for a sample of eight systems at seven organizational components (CBP, CIS, EP&R, ICE, S&T, USCG, and USSS) to ensure that weaknesses, if any, are identified, captured, and tracked in the POA&Ms; and (2) 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. CIS was only included in our scope for our validation of NIST SP 800-26 assessments.

All audit work was conducted between April and September 2004.

******

Throughout the review, we worked closely with the OCIO and personnel at the major organizational components. The cooperation and courtesies extended to the audit team and our contractors are appreciated. The principal OIG points of contact for the audit are Frank Deffer, Assistant Inspector General, Office of Information Technology, (202) 254-4041, and Edward G. Coleman, Director, Information Security Audit Division, (202) 254-5444. Major OIG contributors to the audit are identified in Appendix J.



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

Homeland
Security

September 29, 2004

MEMORANDUM FOR: Clark Kent Ervin
Inspector General

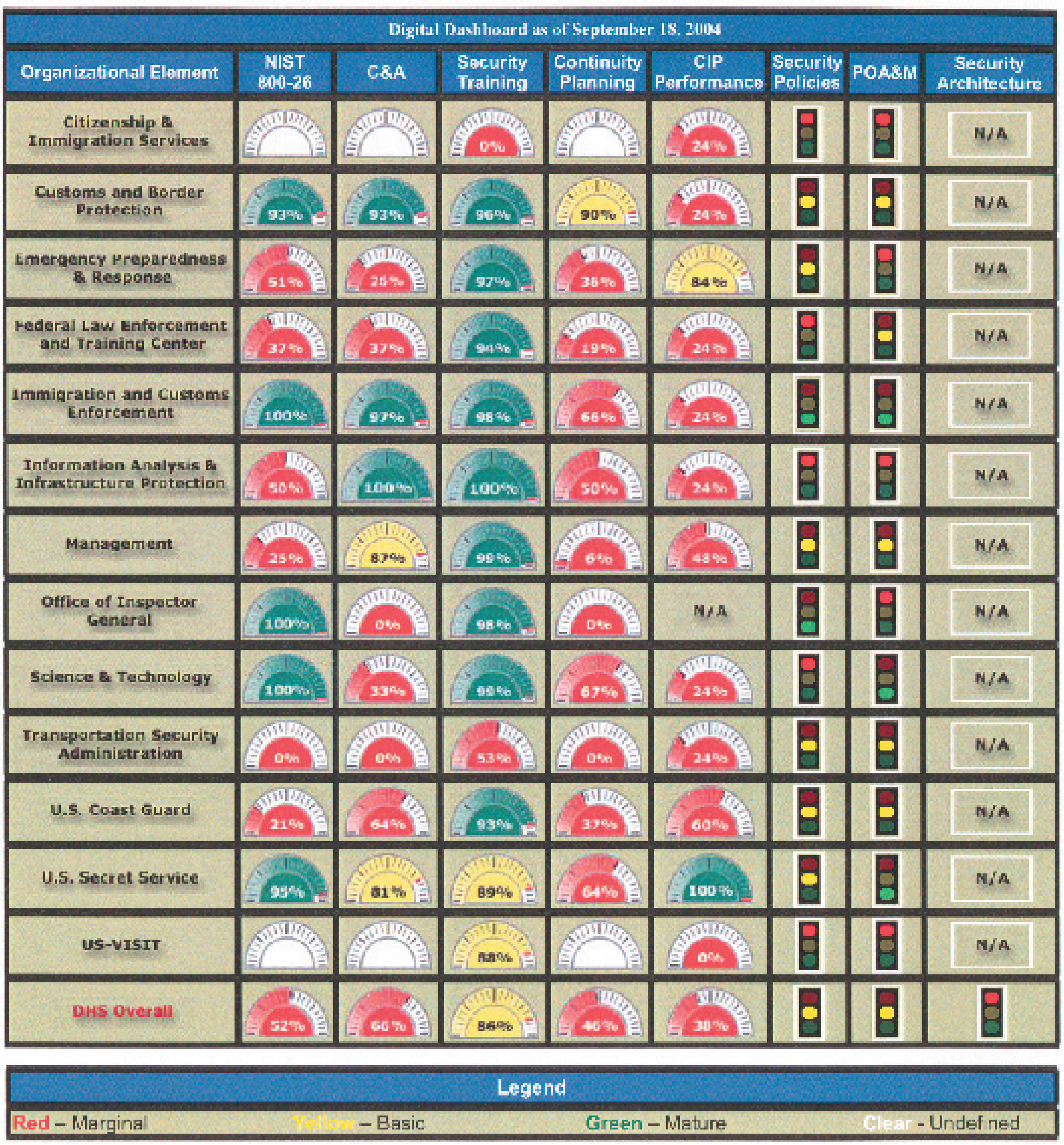
FROM: for Steven Cooper Emery
Chief Information Officer

SUBJECT: Office of Inspector General Report, *Information Technology: Evaluation of the DHS' Information Security Program for Fiscal Year 2004*

Thank you for the opportunity to review the referenced report. We generally concur with the report's recommendations and have already initiated several projects in the later part of Fiscal Year 2004 that address some of the recommendations. These include a system inventory project that is working towards a comprehensive inventory of the Department of Homeland Security (DHS) general support systems and major applications. Similarly, a project to review and verify Federal Information Security Management Act (FISMA) metrics data captured within an automated system was recently initiated. These and other activities will continue to be implemented in Fiscal Year 2005 to improve the communication between the Chief Information Security Officer (CISO) and the DHS components, and to increase the accountability of the DHS components.

We appreciate that the report acknowledges the progress that the Department has made in implementing a statutorily compliant Information Security Program, as well as the management challenges faced as we merge the information security programs of 22 legacy agencies that now comprise the Department. We also appreciate the open dialog and strengthened relationship between the Office of Inspector General and the Office of the Chief Information Officer organizations that have emerged in the past year. The Department is better served when we work together for the common goal of securing the systems that process and store information used in protecting the homeland.

www.dhs.gov



Digital Dashboard as of September 18, 2004

Organizational Element	NIST 800-26	C&A	Security Training	Continuity Planning	CIP Performance	Security Policies	POA&M	Security Architecture
Citizenship & Immigration Services			0%		24%	🟥	🟥	N/A
Customs and Border Protection	93%	93%	96%	90%	24%	🟨	🟨	N/A
Emergency Preparedness & Response	51%	26%	97%	36%	84%	🟨	🟥	N/A
Federal Law Enforcement and Training Center	37%	37%	94%	19%	24%	🟥	🟨	N/A
Immigration and Customs Enforcement	100%	97%	98%	66%	24%	🟩	🟩	N/A
Information Analysis & Infrastructure Protection	50%	100%	100%	50%	24%	🟥	🟥	N/A
Management	25%	87%	99%	6%	48%	🟨	🟨	N/A
Office of Inspector General	100%	0%	98%	0%	N/A	🟩	🟥	N/A
Science & Technology	100%	33%	99%	67%	24%	🟥	🟩	N/A
Transportation Security Administration	0%	0%	53%	0%	24%	🟨	🟨	N/A
U.S. Coast Guard	21%	64%	93%	37%	60%	🟨	🟨	N/A
U.S. Secret Service	95%	81%	89%	64%	100%	🟨	🟩	N/A
US-VISIT			88%		0%	🟥	🟥	N/A
DHS Overall	52%	60%	86%	46%	30%	🟨	🟨	🟥

Legend

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

System Inventory and IT Security Performance

By bureau (or major agency operating component), identify the total number of programs and systems in the agency and the total number of contractor operations or facilities. The agency CIOs and OIGs shall each identify the total number that they reviewed as part of this evaluation in FY 2004. NIST 800-26 is to be used as guidance for these reviews.

For each part of this question, identify actual performance in FY04 for the total number of systems by bureau (or major agency operating component) in the format provided below.

Bureau Name	FY04 Programs		FY04 Systems		FY04 Contractor Operations or Facilities		Number of systems certified and accredited		Number of systems with security control costs integrated into the life cycle of the system		Number of systems for which security controls have been tested and evaluated in the last year		Number of systems with a contingency plan		Number of systems for which contingency plans have been tested	
	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
Total	45[a]	1[b]	387[a]	63[c]	13[a]	0	27[c]	43%[g]	[d]	[d]	24[e]	38%[g]	30[f]	48%[g]	13[f]	21%[g]

Comments:

Note: Only agencywide totals are provided.

[a] Based on our June 2004 data call to ISSMs of nine major components; CIS was only included in our scope for our validation of NIST SP 800-26 assessments. The DHS CIO and OIG agree on the total number of systems for FY 2004.

[b] Based on our ongoing financial statement audit.

[c] Based on our C&A quality review, ongoing financial statement audit, validation of a sample of DHS' NIST SP 800-26 evaluations, ongoing review of classified systems, and audit of wireless networks (*Inadequate Security Controls Increase Risks to DHS Wireless Networks*, OIG-04-27, June 2004).

[d] We did not collect this information during our FY 2004 audit work.

[e] Based on our ongoing CFO audit, validation of a sample of DHS' NIST SP 800-26 evaluations, and ongoing review of classified systems.

[f] Based on our C&A quality review, ongoing financial statement audit, validation of a sample of DHS' NIST SP 800-26 evaluations, and ongoing review of classified systems.

[g] Percentages are based on the 63 systems the OIG reviewed, not the 387 systems reported for DHS.

System Inventory and IT Security Performance

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 Comment area provided below.

Statement	Evaluation
a. Agency program officials and the agency CIO have used appropriate methods to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.	Yes
b. The reviews of programs, systems, and contractor operations or facilities, identified above, were conducted using the NIST self-assessment guide, 800-26.	Yes
c. In instances where the NIST self-assessment guide was not used to conduct reviews, the alternative methodology used addressed all elements of the NIST guide.	N/A (Must use SP 800-26)
d. The agency maintains an inventory of major IT systems and this inventory is updated at least annually.	No
e. The OIG was included in the development and verification of the agency's IT system inventory.	Yes
f. The OIG and the CIO agree on the total number of programs, systems, and contractor operations or facilities.	Yes
g. The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) within the agency.	Yes[a]
Statement	**Yes or No**
h. The agency has begun to assess systems for E-authentication risk.	**Yes**
i. The agency has appointed a senior agency information security officer that reports directly to the CIO.	**Yes**

<u>Comments</u>:

[a] The Investment Review Board (IRB) is in charge of reviewing IT investments. Though the CIO is a voting member of the IRB and is called upon as needed to provide guidance on IT investments, the CIO does not have full authority to approve major IT programs, systems, or investments (*Improvements Needed to DHS' Information Technology Management Structure*, OIG-04-30, July 2004).

Identification of Significant Deficiencies				
By bureau, identify all FY 2004 significant deficiencies in policies, procedures, or practices required to be reported under existing law. Describe each on a separate row, and identify which are repeated from FY 2003. In addition, for each significant deficiency, indicate whether a POA&M has been developed. Insert rows as needed.				
Bureau Name	FY04 Significant Deficiencies			
	Total Number	Number Repeated from FY03	Identify and Describe Each Significant Deficiency	POA&M developed? Yes or No
OCIO	2	[a]	• Security Program, Program Management Office. • Security Program – Compliance and Oversight: POA&M tracking is not FISMA compliant. The POA&M management system needs to be completed.	Yes
Agency Total				

Comments:

[a] We were unable to determine the number of significant deficiencies repeated from FY 2003 because component material weaknesses from FY 2003 were consolidated with FY 2004 OCIO significant deficiencies.

OIG Assessment of the POA&M Process	
Assess whether the agency has developed, implemented, and is managing an agencywide plan of action and milestone (POA&M) process. This question is for OIGs only. 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 Comment area provided below.	
Statement	**Evaluation**
a. Known IT security weaknesses, from all components, are incorporated into the POA&M.	**Rarely, or 0-50% of the time** DHS' ISSOs are to use Trusted Agent FISMA to develop, track, and manage POA&Ms for all systems under their control. DHS' ISSMs are to conduct quarterly reviews of the consistency and accuracy of their POA&M data. Seven of the nine components reviewed lack a documented and implemented POA&M process to ensure POA&Ms contain all weaknesses. We did not verify whether all known IT security weaknesses were incorporated into the POA&M.
b. Program officials develop, implement, and manage POA&Ms for systems they own and operate (systems that support their programs) that have an IT security weakness.	**Rarely, or 0-50% of the time** According to DHS' POA&M policy, program officials are to develop, implement, and manage corrective action plans for all programs and systems that support their operations and assets. However, seven of the nine components reviewed have either not developed, or are in the process of developing a well-documented POA&M process for systems they own and operate.
c. Program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.	**Rarely, or 0-50% of the time** According to DHS' POA&M policy, program officials are to develop, implement, and manage corrective action plans for all programs and systems that support their operations and assets. ISSMs are to ensure that Trusted Agent FISMA is used to manage the remediation of IT program and system weaknesses within their organizational components. The CIO does not receive reports of remediation progress. The CIO does not ensure that components update the status of their remediation progress.
d. CIO develops, implements, and manages POA&Ms for every system they own and operate (a system that supports their program or programs) that has an IT security weakness.	**Rarely, or 0-50% of the time** DHS' CIO has not developed or implemented POA&Ms for every system owned and operated. The CIO has not compiled a comprehensive inventory of all systems.
e. CIO centrally tracks, maintains, and reviews all POA&M activities on at least a quarterly basis.	**Rarely, or 0-50% of the time** While the CIO maintains the quarterly POA&Ms, DHS does not verify the accuracy or completeness of the report.
f. The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.	**Rarely, or 0-50% of the time** The POA&M is DHS' authoritative tool to identify and monitor the status of IT security weaknesses. We do not use POA&Ms as our authoritative management tool. We also conduct vulnerability analyses to identify weaknesses and perform follow-up audits to monitor the status of corrective actions.
g. System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11).	**Rarely, or 0-50% of the time** At the component level, linkage of security costs to the budget was minimal. There are different opinions and approaches by the components on how to report resources and costs in POA&Ms. Approaches ranged from no reporting, to only reporting what could not be covered in existing program funds.
h. OIG has access to POA&Ms as requested.	**Almost always, or 96-100% of the time**
i. OIG findings are incorporated into the POA&M process.	**Rarely, or 0-50% of the time** OIG findings are not incorporated into the POA&M process.
j. POA&M process prioritizes IT security weaknesses to help ensure that significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	**Rarely, or 0-50% of the time** Most of the components do not have a formal process to prioritize their IT security weaknesses.

OIG Assessment of the Certification and Accreditation Process

Assess the agency's certification and accreditation process in order to provide a qualitative assessment of this critical activity. This assessment should consider the quality of the Agency's certification and accreditation process. Any new certification and accreditation work initiated after completion of NIST SP 800-37 should be consistent with NIST SP 800-37. This includes use of the FIPS 199, "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. Earlier NIST guidance is applicable to any certification and accreditation work completed or initiated before finalization of NIST SP 800-37. Agencies were not expected to use NIST SP 800-37 as guidance before it became final.

Statement	Evaluation
Assess the overall quality of the Agency's certification and accreditation process. Comments: Although OMB encouraged the early implementation of draft NIST SP 800-37 by issuing interim certification and accreditation guidance to federal agencies in July 2003, DHS did not require its organizational components to follow the NIST SP 800-37 process until the publication was finalized in May 2004. Because of DHS' late adoption of NIST SP 800-37, we could not evaluate new certification and accreditation work initiated after May 2004. However, we selected 12 certified and accredited systems at four components, and evaluated three key security documents that are part of the accreditation packages for compliance with applicable OMB and NIST guidance.	**Poor** We determined that 11 of the 12 systems evaluated were certified and accredited using a number of different processes: National Information Assurance Certification and Accreditation Process, Department of Defense Information Technology Security Certification and Accreditation Process, Presidential Decision Directive 63, Treasury Directive P 71-10. Specifically, we noted instances in which key security documents prepared did not meet all OMB and NIST requirements, such as: • Up-to-date and approved system security plan. • Current risk assessment. • Contingency plan. Until DHS has a complete inventory of its systems, they will be unable to determine whether all of its systems have been certified and accredited. A complete inventory of major information systems is a key element of FISMA and is needed to effectively manage DHS' IT resources and its information security program.

Policies and Security Configurations

First, answer D.1. If the answer is yes, then proceed. If no, then skip to Section E. For D.1.a-f, identify whether agencywide security configuration requirements address each listed application or operating system (Yes, No, or Not Applicable), and then evaluate the degree to which these configurations are implemented on applicable systems. For example: If your agency has a total of 200 systems, and 100 of those systems are running Windows 2000, the universe for evaluation of degree would be 100 systems. If 61 of those 100 systems follow configuration requirement policies, and the configuration controls are implemented, the answer would reflect "yes" and "51-70%". If appropriate or necessary, include comments in the Comment area provided below.

Answer Yes or No, and then evaluate the degree to which the configuration requirements address the patching of security vulnerabilities. If appropriate or necessary, include comments in the Comment area provided below.

Has the CIO implemented agencywide policies that require detailed specific security configurations and what is the degree by which the configurations are implemented?	Yes, No, or N/A	Evaluation
a. Windows XP Professional	No	Due to the use of legacy systems at DHS' components and the disparity between the components' operating environments, it would not be feasible to implement the guidelines throughout the department. Nonetheless, DHS is working with its components to develop minimum agencywide security configuration polices and procedures. Once completed, DHS will rely on its components to develop more specific guidelines applicable to their operating respective environments. DHS issued security configuration guides for Windows 2000 and Solaris (dated September 16, 2004); however, due to our FISMA deadline, we did not have time to review the guidelines.
b. Windows NT	No	
c. Windows 2000 Professional	No	
d. Windows 2000	**Yes**	
e. Windows 2000 Server	No	
f. Windows 2003 Server	No	
g. Solaris	**Yes**	
h. HP-UX	No	
i. Linux	No	
j. Cisco Router IOS	No	
k. Oracle	No	
l. Other (specify):	No	
	Yes or No	**Evaluation**
Do the configuration requirements implemented above, address patching of security vulnerabilities?	N/A	Patch management is the responsibility of the components. However, the DHS Computer Security Incident Response Center (CSIRC) has implemented the Information Security Vulnerability Message, which is a technical advisory bulletin, sent to each component's CSIRC, that provides them with the latest information related to updates and patches.

Incident Detection and Handling Procedures

Evaluate the degree to which the following statements reflect the status at your agency. If appropriate or necessary, include comments in the Comment area provided below.

Statement	Evaluation
a. The agency follows documented policies and procedures for reporting incidents internally.	Yes
b. The agency follows documented policies and procedures for external reporting to law enforcement authorities.	No
c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov	Yes

Incident Detection Capabilities.

	Number of Systems	Percentage of Total Systems
a. How many systems underwent vulnerability scans and penetration tests in FY 2004?	5202[a]	[b]

b. Specifically, what tools, techniques, technologies, etc., does the agency use to mitigate IT security risk?

Answer: DHS employs various devices and technologies (such as network and host based intrusion detection devices, packet filtering, and proxy firewalls) to help protect against malicious activity and to mitigate its IT security risks.

Comments:

[a] We obtained this number from DHS. For this question only, DHS defines systems as unique internet protocol addresses. Therefore, the number reported in the table is not the total number of systems that underwent vulnerability scans and penetration tests in FY 2004. The number represents only a fraction of systems' vulnerability scans and penetration tests performed. DHS could not determine the total number of systems, or determine the percentage that underwent vulnerability scans or penetration tests conducted in FY 2004, because some of the organizational components are not reporting the results of their scans and tests to DHS' Computer Security Incident Response Center or to Security Operations.

[b] We did not obtain this information. Refer to DHS' FY 2004 FISMA report for this number.

Office of Information Technology
Information Security Audit Division

Edward G. Coleman, Director
Barbara Bartuska, Audit Manager
Jeff Arman, Audit Manager
Patrick Nadon, Audit Manager
Chelsea Pickens, Senior IT Auditor
Tom Tsang, Senior IT Auditor
Benita Holliman, IT Auditor
Pedro Calderon, IT Auditor
William Matthews, IT Auditor
Chris Udoji, IT Auditor
Jason Bakelar, IT Auditor
Michelle Bellamy, IT Auditor
Scott Binder, IT Auditor
Werner Roberts, IT Auditor
Evan Portelos, Associate
Meghan Sanborn, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
General Counsel
DHS OIG Liaison
DHS Chief Financial Officer
DHS CISO
DHS Public Affairs
CIO Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Appropriate Congressional Oversight and Appropriations Committees

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 Department of Homeland Security, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.