DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

INFORMATION TECHNOLOGY:

DHS Information Security Program
Evaluation, FY2003

Office of Information Technology

OIG-IT-03-02 September 2003

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 periodically as part of its oversight responsibility with respect to DHS to identify and prevent fraud, waste, abuse, and mismanagement.

This report is the result of an assessment of the strengths and weaknesses of the program, operation, or function 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, if any, have been developed on the basis of 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/or economical operations. I express my appreciation to all of those who contributed to the preparation of this report.

Clark Kent Ervin
Acting Inspector General

Contents

Appendices

Contents

Abbreviations

BCBP	Bureau of Customs and Border Protection
BICE	Bureau of Immigration and Customs Enforcement
BCIS	Bureau of Citizenship and Immigration Services
BTS	Border and Transportation Security
C&A	Certified and Accredited, Certification and Accreditation
CIAO	Critical Information Assurance Officer
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CSIRC	Computer Security Incident Response Center
DHS	Department of Homeland Security
EP&R	Emergency Preparedness and Response
FedCIRC	Federal Computer Incident Response Center
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center
GISRA	Government Information Security Reform Act
IAIP	Information Analysis and Infrastructure Protection
IG	Inspector General
IO	Information Officer
ISSB	Information Systems Security Board
ISSM	Information Systems Security Manager
IT	Information Technology
MD	Management Directive
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
S&T	Science and Technology
TSA	Transportation Security Administration
USCG	United States Coast Guard
USSS	United States Secret Service

Introduction

The Department of Homeland Security (DHS) was officially established in January 2003 by merging 22 federal agencies[1] into one department. Although the DHS Chief Information Officer (CIO) and Chief Information Security Officer (CISO) were in place in January 2003, the information security function did not begin acquiring needed staff and resources until March 2003. With limited resources, the CISO and program directors have worked to establish the framework for the DHS information technology (IT) security program over the last six months.

In response to the Federal Information Security Management Act (FISMA), the Office of Inspector General (OIG) performed an independent evaluation of DHS' information security program and practices. Our independent evaluation addressed the soundness of the department's information security program and includes the components' performance measures and progress in achieving those measures. Our evaluation included an assessment of DHS' progress in developing and managing its information security program; addressing security weaknesses identified for FY 2002; evaluating data submitted by DHS components; and verifying reported data. Further, OIG assessed components' compliance with the requirements of FISMA and related security policies, procedures, standards, and guidelines. The components included in this report are: Bureau of Citizenship and Immigration Services (BCIS); Border and Transportation Security (BTS); Emergency Preparedness and Response (EP&R); Information Analysis and Infrastructure Protection (IAIP); Science and Technology (S&T); United States Coast Guard (USCG); United States Secret Service (USSS); Management; and OIG. The purpose, scope, and methodology for this review are included in Appendix A.

To complete our independent evaluation for FY 2003, OIG requested information from all of the components listed above. Our information request included all items received through the end of August 2003. All of the components responded fully or in part to our data request. From the information received, we evaluated each component's progress in meeting the Office of Management and Budget (OMB) performance measures.

[1] See Appendix C for list of the agencies.

Results in Brief

In the short period of time since its establishment, DHS has made some progress in establishing a framework for its information systems security program. Still more needs to be done to ensure the security of DHS' information technology infrastructure and prevent disruptions to mission operations.

OIG found that the agency head designated the CIO as the person responsible for the security of information systems within DHS. The DHS CIO further designated a CISO to develop, implement, and manage the department-wide IT security program. Both the CIO and the CISO were in place since the inception of DHS in January 2003, however the information security function did not begin its staffing process until March 2003. The CISO selected program directors who are responsible for ensuring compliance with key FISMA requirements including: policy, compliance, training, incident handling, and critical infrastructure protection (CIP). The CISO developed and disseminated information system security policies and procedures to DHS employees. Finally, the CISO established an Information Systems Security Board (ISSB) consisting of Information Systems Security Managers (ISSM) from each component. The ISSB members help develop DHS security policies and procedures, and they are responsible for ensuring that all computer systems are operating in accordance with these security policies and procedures. The CIO and the CISO are continuing to build on the information security framework that they have established over the last six months to ensure an effective DHS security program.

The DHS CIO and CISO have made progress in a number of additional areas, which will aid DHS in implementing an agency-wide IT security program. OIG found that DHS has drafted an Information Security Strategic Plan, which will be used as a guide for the CISO and program directors to develop fully a comprehensive IT security program. Further, security policies and procedures were issued covering unclassified and classified systems, an incident response and reporting process was implemented, a security awareness training program was initiated, and a CIP working group was established to assist DHS in developing and maintaining a plan for protecting its critical infrastructure. In addition, DHS established an Investment Review Board to provide oversight of all investments. The DHS CIO, as a board member, ensures that decisions over IT investments support the future DHS architecture and business processes. In further support of managing the DHS IT investment portfolio, security costs reported in the Exhibit 300[2], Capital Asset Plan and Business Case, have been summarized for FY 2004 and will be consolidated for DHS' FY 2005 budget submission.

[2] Exhibit 300 is the OMB document used to request budget money for an IT investment.

OMB requires that Plans of Action and Milestones (POA&M) be developed for each program and system that has a weakness identified through FISMA reports, General Accounting Office or financial system audits, or vulnerability assessments. OIG found that DHS does not have a process to ensure that all POA&Ms are developed, implemented, and managed for every DHS system. Further, the process currently in place is not being followed by all DHS components. DHS has purchased an automated tool, which will require the use of the National Institute of Standards and Technology (NIST) self-assessment when performing program and system reviews. This database tool is being customized to provide additional information, which has been determined to be useful for the monitoring of identified security weaknesses. OIG found that all components' POA&Ms are not maintained in the centralized POA&M database because either the component is using its own database or the component has not been trained on use of the database tool. In addition, POA&Ms for security weaknesses relating to classified systems are not included within this database.

While the DHS CIO and CISO have achieved some success in developing the DHS IT security program, DHS must rely on its components to follow established policies and procedures in order to implement the program. OIG found that none of the DHS components has a fully functioning IT security program. Each of the components is lacking in one or more of the performance measurement areas established by FISMA. The Bureau of Customs and Border Protection (BCBP) and the Bureau of Immigration and Customs Enforcement (BICE), both of which are part of BTS, and USSS, have the most mature IT security programs. The majority of their systems have been reviewed, assessed for risk, and certified and accredited.

Overall, OIG's evaluation of DHS' compliance with FISMA identified key areas of security that require management attention. Specifically, OIG found that while 42 percent of DHS systems have security plans, only 37 percent of DHS systems were C&A, and 39 percent of systems had been assessed for risk. In addition, 21 percent of DHS systems' security controls had been tested and evaluated in the past year, and only 11 percent of DHS systems had contingency plans.

Finally, FISMA requires an agency to report any significant deficiency on the adequacy and effectiveness of its information security program as a material weakness.[3] As such, based on OIG's evaluation of DHS' IT security program, OIG recommends that the Chief Information Officer declare information security a material weakness at DHS.

[3] A material weakness is a significant deficiency in the adequacy and effectiveness of information security policy, procedure, and practice. Examples include the failure to perform adequate annual program and system reviews, lack of system security plans, absence of system certification and accreditation, and failure to maintain comprehensive POA&Ms.

Further, to assist the CIO in the development of the DHS security program, OIG makes several additional recommendations found at the end of OIG's independent evaluation.

Background

On December 17, 2002, the President signed into law the E-Government Act of 2002 (P.L. 107-347), which includes Title III, FISMA. FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act of 2000 (GISRA), which expired in November 2002. FISMA focuses on the security program management, implementation, and evaluation aspects of the security of unclassified and national information security systems. While FISMA continues the process for annual reviews and reporting requirements that were first introduced under GISRA, it also includes new guidance that is aimed at further strengthening the security of the federal government's information and information systems, including the development of minimum standards for agency information systems. NIST is to work with agencies in the development of those standards, per its statutory role in providing technical guidance to federal agencies. Title III, along with OMB policy, lays out a framework for annual IT security reviews, reporting, and remediation planning.

OMB issued memorandum M-03-18, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting* on August 1, 2003. One significant change directs Inspectors General (IGs) to assess specific criteria, where the agency has developed, implemented, and manages an agency-wide POA&M process. The agency report must consist of two separate components. One is to be prepared by the OIG, characterizing the results of its independent evaluation and agency progress in implementing its POA&Ms. The other component is to be prepared by the DHS CIO, working with program officials, reflecting the results of their annual system and program reviews and progress in implementing their POA&Ms.

Results of Independent Evaluation

A. Overview of FISMA IT Security Reviews

A.1. – Identify the agency's total IT security spending and each individual major operating division or bureau's IT security spending as found in the agency's FY03 budget enacted.

OIG is not required to report on this area.

A.2 – Programs and Systems

A.2a. Identify the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials and CIOs in FY03, the total number of contractor operations or facilities, and the number of contractor operations or facilities reviewed in FY03. Additionally, IGs shall also identify the total number of programs, systems, and contractor operations or facilities that they evaluated in FY03.

Bureau Name	FY03 Programs		FY03 Systems		FY03 Contractor Operations or Facilities	
	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed
BTS-BICE/BCIS	7	7	88	87	0	0
BTS-BCBP	6	0	25	23	17	17
BTS-TSA	13	0	79	2	9	9
BTS-FLETC	5	0	11	1	3	0
EP&R	11	0	58	8	2	2
IAIP	0	0	5	0	3	0
S&T[4]	0	0	0	0	0	0
USCG	5	0	55	14	3	0
USSS	3	0	20	17	1	1
OIG	4	0	2	0	0	0
Management	2	0	4	0	3	0
Agency Total	**56**	**7**	**347**	**152**	**41**	**29**

[4] S&T does not have any information systems.

A.2 – Programs and Systems, cont'd

A.2b. For operations and assets under their control, have agency program officials and the agency CIO used appropriate methods (e.g., audits or inspections, agreed upon IT security requirements for contractor provided services or services provided by other agencies) 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.** DHS has established "Information Systems Security Management Directive 4300 Publication" dated June 2003 that outlines agreed upon security requirements for contractor provided services. Outsourced services and operations must adhere to the DHS security policies. All contractors must adhere to the same rules and regulations as government employees.
c. If yes, what methods are used? If no, please explain why.	The requirements include non-disclosure agreements, minimum background investigations, appointment of a security point-of-contact or contracting officer for the duration of the contract, and onsite inspection of facilities.
d. Did the agency use the NIST self-assessment guide to conduct its reviews?	Only two components used the NIST self-assessment guide to conduct reviews. DHS has obtained an automated tool, Trusted Agent FISMA, which will be used department-wide to conduct all NIST self-assessments in FY 2004.
e. If the agency did not use the NIST self-assessment guide and instead used an agency-developed methodology, please confirm that all elements of the NIST guide were addressed in the agency methodology.	Components that did not use the NIST self-assessment guide developed their own in-house risk assessment checklists.
f. Provide a brief update on the agency's work to develop an inventory of major IT systems.	The DHS CIO continues to work with contractors to develop an accurate systems inventory. There are a number of activities planned or under way (financial statement audit, IT portfolio management review, and Project Matrix review) to update the current systems inventory. The DHS CIO believes that the existing inventory identified 90 to 95 percent of all information systems within DHS.

DHS is in the process of identifying its programs, systems, and contractor operations. DHS identified and reported to the OIG a total of 56 programs, 347 systems, and 41 contractor operations. OIG found that four components (BICE, EP&R, Federal Law Enforcement Training Center (FLETC), and USCG) have mapped each of their major systems to specific programs; the remaining components have not made such associations.

According to OMB memorandum M-03-18, components are required to use the NIST 800-26 self-assessment guide to review their programs, systems, and contractor operations. A total of 7 program, 152 system, and 29 contractor operation reviews were conducted by the components using various methodologies. Overall, the components conducted only 29 of 152 system reviews using NIST 800-26 self-assessments. The components conducted 7 program, 123 system, and 29 contractor operation reviews using methodologies, which comprised a variation of internal program audits, certification and accreditation (C&A) risk assessments, and component developed security checklists.

To ensure that contractor provided services are secure, DHS issued the "Information System Security Management Directive (MD) 4300 Publication for Sensitive and National Security Systems" that outlines specific IT security procedures and requirements. The security requirements include protection of sensitive information at the contractor site, background investigations and/or clearances on contractor personnel, and appointment of contracting officers for the duration of the contract. Internal and site reviews should be conducted to ensure that the security requirements outlined in the contract are implemented and enforced.

From February to April 2003, a DHS contractor conducted an inventory of its information systems, meaning its major applications and general support systems. The inventory identified 1,586 applications that were divided into four categories: mission, business, enterprise solutions, and infrastructure. The inventory was based on input from DHS components, allowing each component to divide its applications into further categories and at a greater level of detail. The DHS CIO believes that the inventory identified 90 to 95 percent of all information systems within DHS. As part of its independent evaluation, OIG determined that the programs and systems reported by the components under FISMA are included in the larger inventory of 1,586 applications mentioned above.

A.3 – Material Weaknesses

A.3 Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law in FY03. Identify the number of material weaknesses repeated from FY02, describe each material weakness, and indicate whether POA&Ms have been developed for all of the material weaknesses.

Bureau Name	FY 03 Material Weaknesses			
	Total Number	Total Number Repeated from FY02	Identify and Describe Each Material Weakness	POA&Ms developed? Y/N
BTS-BICE/BCIS	A	A	See below	N/A
BTS-BCBP	2	2	See below	Y
BTS-TSA	A	A	See below	--
BTS-FLETC	0	0	See below	--
EP&R	8	8	See below	Y
IAIP	A	A	See below	--
S&T	B	B	See below	--
USCG	A	A	See below	--
USSS	0	0	See below	--
OIG	0	N/A	See below	--
Management	0	N/A	See below	--
Agency Total	**10**	**10**		

A - Through reviews of FY 2002 GISRA reports and FY 2002 Performance and Accountability reports, OIG was unable to determine whether a material weakness existed for this component in FY 2003 or repeated from FY 2002 since the legacy agency identified only department-wide material weaknesses (not at the component level).
B - OIG was unable to determine whether material weaknesses existed for the component based on information provided either by DHS headquarters or legacy agency.

OIG was able to identify ten IT security material weaknesses in FY 2003 using the legacy agencies' FY 2002 GISRA reports and FY 2002 Performance and Accountability reports. These ten weaknesses were repeated from FY 2000.

Material weaknesses identified for the Federal Emergency Management Agency (FEMA) (now part of EP&R) and U.S. Customs Service (now part of BCBP) encompass serious shortcomings in such areas as system security program, security control implementation, contingency planning, computer security education and awareness, personnel security, risk assessments, security life cycle management, C&A, timely restoration of critical systems, and logical and technical systems security exposures. In addition, OIG noted that the eight POA&Ms for FEMA have not been resolved in a timely manner. Specifically, these material weaknesses were scheduled for remediation in early 2003; however, resolution was delayed because of a lack of funding. Details of each of the ten material weaknesses that were reported in FY 2002 follow:

FEMA

1. System Security Program- The System Security Program has not been implemented fully.

2. Security Control Implementation- Security controls have not been implemented consistently across all systems.

3. Contingency Planning- Only a few of the systems have formal contingency plans and some of these plans have not been tested on a regular basis.

4. Computer Security Education and Awareness- An agency-wide capability of providing basic computer security education and awareness training to all users needs to be established.

5. Personnel Security- Background investigations for all personnel have not been performed.

6. Risk Assessments- Risk assessments on at least one-third of its systems have not been performed.

7. Security Life Cycle Management- Security life cycle management is needed.

8. Certification and Accreditation- Full accreditation of at least one-third of the most critical systems has not been completed.

Customs

9. Inability to restore critical systems timely- Several significant deficiencies were identified in Customs' ability to provide for timely restoration of mission-critical systems that could impair its ability to respond effectively to a disruption in operations.[5]

10. Various logical and technical systems security exposures exist- Global update privileges were provided to numerous programs/data files, allowing potential changes that could compromise the integrity of data. Also, access was provided to programmers without appropriate tracking of their activities, or compensating controls, to ensure that all functions performed were appropriate to their assigned duties.

OIG was unable to identify the existence or non-existence of material weaknesses for BICE, IAIP, S&T, and USCG. FISMA and OMB guidance requires agencies to report all significant deficiencies as material weaknesses. The material weaknesses identified in the legacy agencies' FY 2002 GISRA and Performance and Accountability reports do not include an assessment of the significance within their respective agencies.

[5] The DHS OIG is in the process of issuing a report, which states that BCBP has taken the appropriate steps to eliminate the problems which resulted in the material weakness.

A.4 – Plan of Action and Milestones

A.4. This question is for IGs only. Please assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone process that meets the criteria below. Where appropriate, please include additional explanation in the column next to each criteria.	Yes	No
Agency program officials develop, implement, and manage POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.		X
Agency program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.		X
Agency CIO develops, implements, and manages POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.		X
The agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis.		X
The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.	X	
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) to tie the justification for IT security funds to the budget process.		X
Agency IGs are an integral part of the POA&M process and have access to agency POA&Ms.	X	
The agency's POA&M process represents a prioritization of agency IT security weaknesses that ensures that significant IT security weaknesses are addressed in a timely manner and receive, where necessary, appropriate resources.		X

OIG found that DHS does not have a process to ensure that all POA&Ms are developed, implemented, and managed for every DHS program and system. Although DHS has the framework for an agency-wide POA&M process, this process is not followed by all components. DHS has purchased a software tool that provides for a central database to track and monitor POA&Ms. This tool is being customized to provide assessment templates and questionnaires to meet DHS criteria. OIG found that all components' POA&Ms are not maintained in DHS' centralized database because either the component is using its own database or the component has not been trained on use of the database tool. Specifically, BCBP and USCG have not submitted all of their POA&Ms to the CISO. In addition, Transportation Security Administration (TSA) and USSS have classified POA&Ms that have not been submitted for inclusion in DHS' consolidated POA&M database.

B. Responsibilities of Agency Head

B.1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth FISMA's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced?

The Under Secretary for Management delegated to the DHS CIO oversight responsibilities for DHS' information security program. In turn, the DHS CIO designated a CISO, as required under FISMA, with the authorities and responsibilities to establish and enforce information security policies and procedures throughout the department.

The DHS CIO is currently developing an agency-wide information security program. An IT Security Program Handbook, which provides specific policies and procedures for implementing security requirements for Sensitive But Unclassified and National Security Systems and networks, was disseminated in June 2003. Policies addressed in the handbook include (but are not limited to) capital planning and investment control, critical infrastructure protection, physical security, and contingency planning. In order to manage the IT activities of the components, the DHS CIO established a Senior IT Leadership Council, which includes each of the component's Information Officers. The CISO established an ISSB consisting of security managers from each component. These two groups are the mainstay in the establishment and enforcement of department-wide information system security policies and procedures. Also, the DHS CIO is establishing a Security Operations Center to provide comprehensive IT security support, including centralized support for security event monitoring.

B.2. Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?

A major operating component of DHS cannot make an IT investment decision without review by and the concurrence of the DHS CIO. In May 2003, DHS issued MD 1400 - *Investment Review Process,* which applies to all components, departmental offices, agencies, and sub-elements within DHS for the acquisition of all capital assets and services. MD 1400 requires that business cases[6] and investment portfolios[7] go through a review before they can be approved. All investments are categorized into one of

[6] Business cases are also referred to as Exhibit 300s.
[7] Investment portfolios are also referred to as Exhibit 53s.

four levels based on specific criteria and each level requires a specific review and approval level. The DHS CIO is a member of the three boards that review and approve investments for Levels 1-4 (based on dollar thresholds). Our review included testing and reviewing a sample of 20 of DHS' 120 business cases to ensure that they were reviewed by and included in the budget of the DHS CIO and program officials. Our review disclosed that four IT investments did not have security costs detailed in the business case. See section C.4 for a more detailed discussion of IT capital planning and investment.

B.3. How does the head of the agency ensure that the agency's information security plan is practiced throughout the life cycle of each agency system?

The DHS Secretary has delegated oversight for the information security program to the Under Secretary of Management. The Under Secretary has assigned the responsibilities and authorities to the DHS CIO for the oversight of the agency information security program. Specifically, OIG noted that:

- Program officials are accountable for the security programs under their control. Every system has a senior management official with the authority to assume responsibility formally for operating a system at an acceptable level of risk.

- The DHS CIO develops, implements, and manages the DHS information security program that consolidates the DHS components' information security programs into one.

- The CISO serves as the department-wide security administrator and advisor on technical computer security matters.

- The DHS CIO has a system development methodology policy that, once implemented, will help ensure that security plans are practiced throughout the life cycle of each agency system.

The agency head has certified and approved MD 4300, Information Technology Systems Security. This directive establishes the IT Systems Security Program that provides for a comprehensive IT security policy for each component. Specifically, the security change management policy requires that new systems and newly modified systems proceed through the system development life cycle with changes documented in the security plan, tested, and approved prior to placing these systems into the operational environment. OIG determined that, although appropriate delegations have been made and management directives issued, a review by the CIO's office has not been performed to ensure that

DHS's information security plan is practiced throughout the life cycle of each agency system.

B.4. During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system? Please describe.

In FY 2003, the DHS agency head took the following specific and direct actions to oversee the performance of the DHS CIO and program officials:

- The DHS Secretary has bi-weekly security briefings with senior officials. These meetings include discussions on the performance of the agency security strategy and related plans.

- The DHS Secretary authorized DHS system approval as part of a formal C&A process where the approving authority is the Designated Approving Authority. The process includes determining that security controls for IT systems are implemented and functioning correctly, which includes a review of current security plans. However, OIG found that some of the testing of system security controls was not performed.

- The DHS CIO has periodic senior IT Leadership Council briefings, which consist of the components' Information Officers (IOs)[8] (see section B.1). Each IO is responsible for certifying that each system, before implementation, has a security plan, been assessed for risk, and has had its security controls tested.

B.5. Has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., continuity of operations, and physical and operational security)? Please describe.

DHS has not integrated its information and information technology security program with its CIP responsibilities, and other security programs. However, DHS has taken a number of steps toward this goal. Specifically, DHS' Critical Information Assurance Officer (CIAO) has established and chartered a CIP working group to develop collectively policy, strategy, implementation guidance, and an oversight capability. Each component has designated a CIP officer who is responsible for integrating and coordinating

[8] Chief Information Officers from each major division and critical agency.

CIP requirements within and among the components' various security programs and infrastructure asset owners. Each component has a CIAO who is responsible for ensuring components' CIP requirements are met and are compliant.

In addition, DHS established the DHS Critical Infrastructure Protection Strategic Plan (DHS Strat Plan) that serves as a foundation for components to use in integrating their information technology security programs with their CIP responsibilities. The DHS Strat Plan represents a strategy designed to help the components address effectively the long-term challenges posed by the need to protect DHS' critical cyber, physical, and personnel assets. Each DHS component shares responsibility for identifying the critical assets under its cognizance, assessing the vulnerabilities of those assets, and assuming their availability, integrity, confidentiality, survivability, and adequacy. The DHS CIAO oversees the CIP program and is aware of the progress within each component on implementing CIP responsibilities within their security programs through the CIP Working Group.

B.6. Does the agency have separate staffs devoted to other security programs, are such programs under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complementary across the various programs and disciplines?

DHS has separate staffs devoted to other information security programs. Currently, the DHS IT security program resides with the DHS CIO and CISO. As noted in section B.1, the Under Secretary for Management has designated the DHS CIO as having the oversight responsibilities for the information security program at DHS. The DHS CIO has assigned the CISO with the information security officer responsibilities and authorities as outlined in FISMA. OIG found that each DHS component has its own security program. Specifically, each component has an ISSM, who meets with the CISO on a bi-weekly basis to discuss overall DHS security issues; however, ISSMs report to their component IO and not the CISO. This structure provides for a separate security function that is not under the direct control of the DHS CIO and the CISO.

In addition, OIG noted that physical security resides with the DHS Security Office. This office is responsible for providing and overseeing the physical security of DHS facilities, including the various DHS data centers. DHS has not taken specific steps to determine whether there is unnecessary duplication of overhead costs related to its security programs.

B.7 – Critical Operations and Assets

B.7 Identification of agency's critical operations and assets (both national critical operations and assets and mission critical) and the interdependencies and interrelationships of those operations and assets.				
a. Has the agency fully identified its national critical operations and assets?	Yes		No	X
b. Has the agency fully identified the interdependencies and interrelationships?	Yes		No	X
c. Has the agency fully identified its mission critical operations and assets?	Yes		No	X
d. Has the agency fully identified the interdependencies and interrelationships of those mission critical operations and assets?	Yes		No	X
e. If yes, describe the steps the agency has taken as a result of the review.	No, See Explanation Below.			
f. If no, please explain why.				

DHS has not identified all of its critical assets or operations. A two-step Project Matrix[9] methodology will be used to identify these assets or operations. Until an official Project Matrix review can be conducted, an unofficial list of CIP assets has been compiled based on Project Matrix or other critical asset identification reviews that were performed by legacy agencies. BCBP, FLETC, USSS, and Management have used Project Matrix to identify their critical assets. BCIS, BICE, EP&R, and USCG used a hybrid approach to identify their critical assets. IAIP, S&T, and TSA have not yet identified their critical assets. A contractor will assist the DHS CIP Program Director in conducting an official review during the first quarter of FY 2004 to identify all DHS' critical assets and operations.

DHS has not completed an interdependency analysis. This analysis will be performed upon completion of critical assets and operations identification. DHS will develop a methodology using one set of criteria for consistency in data capture and a standardized approach will be used to ensure that processes are uniformly applied across all platforms. DHS will conduct this review in FY 2004.

[9] Project Matrix involves a two-step process in which each agency identifies its nationally critical functions and services and the infrastructure of assets and links required to perform or provide them.

B.8 – Reporting of Security Incidents

B.8. How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities?				
a. Identify and describe the procedures for external reporting to law enforcement authorities and to the Federal Computer Incident Response Center (FedCIRC).	The DHS CSIRC is responsible for notifying FedCIRC and law enforcement authorities of all DHS security incidents. This process formally began in June 2003. DHS notifies FedCIRC via an emailed version of the DHS Daily Operations and Monthly reports (which includes security incidents).			
b. Total number of agency components or bureaus.	**11** (See section B.9 for components)			
c. Number of agency components with incident handling and response capability.	**9** (IAIP and S&T will establish the capability once they own their own systems.)			
d. Number of agency components that report to FedCIRC.	**0** (DHS CSIRC reports all incidents)			
e. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?	**Yes** In June 2003, the DHS CSIRC began reporting all reported significant incidents daily to FedCIRC; a summary of all significant and minor incidents is reported monthly to FedCIRC.			
f. What is the required average time to report to the agency and FedCIRC following an incident?	**Agency: 4** **FedCIRC: daily** Significant incidents must be initially reported to the DHS CSIRC within 4 hours. DHS reports significant incidents to FedCIRC daily.			
g. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?	There is no formal process by the agency CSIRC or at the components to confirm that patches have been tested and installed in a timely manner.			
h. Is the agency a member of the Patch Authentication and Distribution Capability operated by FedCIRC?	Yes		No X	DHS is in the process of developing an enterprise solution for patch identification and deployment to include FedCIRC's PADC. Two components are now members.
i. If yes, how many active users does the agency have for this service?	4 (FLETC: 3, USCG: 1)			
j. Has the agency developed and complied with specific configuration requirements that meet their own needs?	Yes		No X	The overall security architecture at DHS is still under development. Once established, the architecture should address configuration requirements for all systems. Some components have their own standards and procedures for configuring systems.
k. Do these configuration requirements address patching of security vulnerabilities?	Yes		No X	DHS will include patching of security vulnerabilities in its configuration requirements.

DHS established and implemented an agency-wide Computer Security Incident Response Center (CSIRC) in January 2003. The DHS CSIRC serves as a mechanism to receive and/or disseminate incident information and provide a consistent capability to respond to and report on security incidents. Incident response policies and procedures were finalized in June 2003 and were included in the DHS IT Security Program Handbook and disseminated to the components.

The components are required to report significant incidents upon discovery and validation of the incident and provide a full report to the DHS CSIRC within four hours. The number of minor incidents by category is reported to the DHS CSIRC on a monthly basis. The DHS CSIRC reviews and monitors all significant security incidents that are reported by the components and notifies IT management of all significant incidents. The CSIRC does not have a process to ensure that the components are reporting all incidents that have occurred. The CSIRC ensures that all components understand the DHS security incident response and reporting requirements.

Beginning in June 2003, the DHS CSIRC began requiring each component to submit a monthly summary incident report for the previous month's incidents. Of the 11 components required to submit monthly summaries, 5 components (BCBP, BICE, EP&R, TSA, and USSS) submitted reports in June and 6 components (BCBP, BICE, EP&R, TSA, USCG, and USSS) submitted reports in July. The CSIRC began formally reporting all incidents (as reported by the components) to the Federal Computer Incident Response Center (FedCIRC) in June 2003. Significant incidents are reported daily via the DHS Daily CSIRC Report, as well as a summary of all reported significant and minor incidents via the DHS Monthly CSIRC Report.

Nine of the eleven components reviewed have an incident handling and response capability. The two components that do not have this capability (IAIP, S&T) are newly formed and are using the DHS CSIRC until they establish their own capability.

The DHS CSIRC evaluates new vulnerabilities and identifies patches.[10] Once a vulnerability and patch are identified, an email is sent to all DHS components. Since this is an informational service only, the DHS CSIRC does not ensure that patches are actually installed. Because DHS does not have a consistent approach to patch management, each of the components continues to use their own processes. In addition, there are no formal processes at DHS to ensure that patches have been tested and installed in a timely manner.

[10] A patch is a fix to mitigate or remove a vulnerability from a computer or system.

B.9 – Number of Security Incidents (October 2002 to June 2003)

B.9. Identify by bureau, the number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported and those reported to FedCIRC or law enforcement.			
Bureau Name	**Number of incidents reported**	**Number of incidents reported externally to FedCIRC**	**Number of incidents reported externally to law enforcement (D)**
BTS-BICE	131	2 (C), (D)	0
BTS-CBP	7	0 (D)	0
BTS-TSA	19	0 (D)	0
BTS-FLETC	2	0 (D)	0
EP&R	15	1	0
IAIP	0	0	0
S&T	0	0	0
USCG	15	1 (C), (D)	0
USSS	4	0 (D)	0
OIG	0	0	0
Management	0	0	0
Total	**193**	**4**	**0**

C - Reported by the DHS CSIRC
D - Does not include the number of incidents reported by legacy agency organization to FedCIRC or law enforcement on the component's behalf prior to it moving to DHS

According to component information provided to OIG, the total number of computer incidents during FY 2003 was 193. Because some of the components did not have a formal means to record and maintain documentation on security incidents, OIG could not validate the resolution of all incidents.

OIG found that computer incidents and reporting requirements are handled differently among the components. Since DHS did not issue draft incident response and reporting procedures to the components until May 2003, the DHS CSIRC has begun only recently to ensure that the components are complying with these procedures. The procedures provide components with a consistent methodology to identify, document, and report computer security incidents.

OIG also found that the definition of incidents for reporting purposes differs between DHS and FedCIRC. Some incidents that FedCIRC considers a reportable incident are not deemed so by DHS. The number of security incidents may change significantly once DHS ensures that the definitions are in agreement with FedCIRC and that all components are following the same methodology to report incidents.

C. Responsibilities of Agency Program Officials and Agency Chief Information Officer

C.1 – IT Security Program Performance Measures

C.1. Have agency program officials and the agency CIO: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques? By each major agency component and aggregated into an agency total, identify actual performance in FY03 according to the measures and in the format provided below for the number and percentage of total systems.

Bureau name	Total number of systems	Number of systems assessed for risk and assigned a level or risk		Number of systems that have an up-to-date IT security plan		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	
		No.	%	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
BTS - BICE	88	66	75%	76	86%	88	100%	30	34%	23	26%	66	75%	9	10%
BTS- BCBP	25	23	92%	24	96%	20	80%	6	24%	24	88%	23	92%	22	88%
BTS - TSA	79	2	3%	1	1%	0	0%	11	14%	0	0%	0	0%	0	0%
BTS-FLETC	11	1	9%	1	9%	0	0%	2	18%	0	0%	1	9%	0	0%
EP&R	58	11	19%	9	16%	4	7%	9	16%	18	31%	9	16%	4	7%
IAIP	5	0	0%	0	0%	0	0%	1	20%	0	0%	0	0%	0	0%
S&T	0	0	0%	0	0%	0	0%	0	0%	0	0%	0	0%	0	0%
USCG	55	14	25%	17	31%	5	9%	15	27%	2	4%	8	15%	2	4%
USSS	20	17	85%	17	85%	12	60%	1	5%	5	25%	9	45%	1	5%
OIG	2	0	0%	0	0%	0	0%	0	0%	0	0%	0	0%	0	0%
Management	4	0	0%	0	0%	0	0%	0	0%	0	0%	0	0%	0	0%
Total	**347**	**134**	**39%**	**145**	**42%**	**129**	**37%**	**75**	**22%**	**72**	**21%**	**116**	**33%**	**38**	**11%**

The CISO is in the process of identifying all programs and systems. As these programs and systems are identified, the components are working to determine which are risk assessed, have up-to-date security plans, are C&A, and have contingency plans. DHS will use the TrustedAgent FISMA tool to perform NIST 800-26 self assessments in the future and is looking at potential contractors who can perform C&As for all programs and systems. Also, DHS is planning to develop performance measures for risk assessments, security plans, C&As, and contingency plans.

The Under Secretary of Management has identified four areas of interest (incident handling, CIP, compliance and training) that the CISO has indicated will be the focus of

performance measures. The DHS CIO and the CISO are currently meeting with potential vendors about the development of the DHS scorecard that will provide performance measures for each of these areas. Our review disclosed that overall, 39 percent of the 347 systems identified had risk assessments performed on a regular basis or whenever the system, facilities, or other conditions changed. Some components have low numbers for risk assessments. For example, USCG has assessed 25 percent of its 55 systems, and EP&R has assessed 19 percent of its 58 systems. Components with high percentages of risk assessments include BCBP (92%), BICE (75%), and USSS (85%).

As reported in our table, the number of system security plans that have been developed, authorized, and kept up-to-date varied depending on the component. For example, among the components with the highest number of security plans are BCBP (96%), BICE (86%), and USSS (85%). However, components with few up-to-date security plans are EP&R (16%), FLETC (9%), and TSA (1%).

Overall, 129 of 347 (37%) systems were reported to have undergone C&A. BICE reported 100 percent and BCBP reported 80 percent of their systems have been C&A.

Three components (FLETC, IAIP, and TSA) did not report any systems that had security controls tested and evaluated. In addition, the number of systems for which security controls have been tested and evaluated in the last year totaled 72 (21%). OIG also noted that contingency plans were in place for 116 (33%) out of 347 systems reviewed.

OIG also reviewed a subset of systems at BICE, EP&R, IAIP, TSA, and USCG. The review included risk assessments, C&As, and contingency plans for the following systems: BICE's Criminal Alien Investigation System, IAIP's Project Matrix, EP&R's National Flood Insurance Program, TSA's Law Enforcement Message Switch, USCG's Defense Messaging System, and Automated Mutual Assistance Vessel Rescue. OIG noted that while risk assessments were performed for all six systems reviewed, C&As were completed for 4 of the 6 systems, and contingency plans were in place for 4 of the 6 systems.

C.2 – Agency-wide Security Program

C.2. Identify whether the agency CIO has adequately maintained an agency-wide IT security program and ensured the effective implementation of the program and evaluated the performance of major agency components.				
Has the agency CIO maintained an agency-wide IT security program? Y/N	**Did the CIO evaluate the performance of all agency bureaus/components? Y/N**	**How does the agency CIO ensure that bureaus comply with the agency-wide IT security program?**	**Has the agency CIO appointed a senior agency information security officer per the requirements in FISMA?**	**Do agency POA&Ms account for all known agency security weaknesses including all components?**
N	N	System Development Methodology	Y	N

The DHS CIO has developed security policies, standards, and procedures and has disseminated these to DHS components. These policies, and procedures provide the framework for an effective information security program; however, DHS IT systems are at increased risk because these policies have not been implemented fully across the department.

For example:

- The POA&M process does not account for all known agency security weaknesses.
- Only eight percent of DHS employees and contractors have received security awareness training.
- An accurate inventory that identifies all major DHS programs and associated systems does not exist.
- All systems have not been C&A.

DHS is aware of these weaknesses in its IT security program and is working to resolve these issues.

C.3. Security Training and Awareness

C.3. Has the agency CIO ensured security training and awareness of all agency employees, including contractors and those employees with significant IT security responsibilities?							
Total number of agency employees in FY03	Agency employees that received IT security training in FY03		Total number of agency employees with significant IT security responsibilities	Agency employees with significant security responsibilities that received specialized training		Briefly describe training provided	Total costs for providing training in FY03
	Number	Percentage		Number	Percentage		
208785	16994 (E)	**8% (E)**	1188	561	**47%**	LAN/Network Security, Win 2000, CISSP workshop, AIS security, SANS conferences, Unix, new employee orientation, security administration	$650,642 (F)

(See Appendix C for specific component information)

E - Does not include IAIP or S&T employees trained by their legacy agencies
F - Does not include IAIP and Management

An IT security training program director is responsible for developing an IT security training strategic plan and for consolidating the management and content of such training across DHS. A web-based security awareness training course is in development for use by all DHS employees and contractors. The program director is also in the process of identifying specialized training courses that employees with security responsibilities need to take on a yearly basis. These initiatives should be implemented in FY 2004. It will remain the responsibility of each component to ensure that all of its employees and contractors receive security awareness and specialized training each year.

Our review of the IT security training at DHS for FY 2003 found that only eight percent of DHS employees and contractors had security awareness training and 47 percent of employees known to have significant security responsibilities had specialized training. For example, BICE provided only ten percent of its employees with security awareness training in FY 2003. BICE previously relied on its legacy agency to supply web-based training but was not able to use it during FY 2003. BICE is in the process of acquiring training, which will be available in the first quarter of FY 2004. BICE also reported that none of its security personnel received specialized security training during FY 2003. BCBP and USSS reported that they would roll out their awareness training to all employees in September 2003. FLETC and TSA are in the process of providing awareness training (via a CD or the internet) to all employees. None of the TSA security personnel has received any specialized training in FY 2003 due to a lack of funding.

USCG reported that only 13 percent of its employees have received security awareness training in FY 2003.

The training coordinators for each of seven components (BCBP, BICE, EP&R, IAIP, S&T, TSA, and USCG) did not know the total number of employees with security responsibilities. Without this information, it will be difficult to ensure that all security personnel receive adequate training. In addition, OIG noted that seven of the components (BICE, FLETC, IAIP, OIG, S&T, TSA, and USCG) did not have a means to track, by name and position, employees who have received security (awareness and specialized) training and the associated costs of the training.

C.4 – Capital Planning and Investment

C.4. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were IT security requirements and costs reported on every FY05 business case (as well as in the exhibits 53) submitted by the agency to OMB?				
Bureau Name	**Number of business cases submitted to OMB in FY05**	**Did the agency program official plan and budget for IT security and integrate security into all of their business cases? Y/N**	**Did the agency CIO plan and budget for IT security and integrate security into all of their business cases? Y/N**	**Are IT security costs reported in the agency's exhibit 53 for each IT investment? Y/N**
BTS-BICE	10	Yes	Yes	H
BTS-BCIS	4	Yes	Yes	H
BTS-BCBP	23	Yes	Yes	H
BTS-TSA	33	Yes	Yes	H
BTS-FLETC	2	No	No	H
EPR	22	No	No	H
IAIP	1	Yes	Yes	H
S&T	0	G	G	G
USCG	11	Yes	Yes	H
USSS	2	Yes	Yes	H
OIG	0	None submitted	None submitted	N/A
Management	12	Yes	Yes	H
Total	**120**			

G- S&T does not have any systems.
H- Exhibit 53s have not yet been prepared.

In May 2003, DHS issued two directives, the IT Capital Planning and Investment Control and Portfolio Management and the Investment Review Process, MDs 4200.1 and 1400 respectively. These directives provide guidance to the components on preparing Exhibit 300s and the process used to review and approve investment requests. OIG determined that these MDs are being used by all components in the capital planning process. In addition, we were able to confirm, through the review of budget documentation, that

agency program officials and the DHS CIO have planned and budgeted for IT security and integrated these costs into the business cases for DHS systems.

Because DHS had not started using the Information Technology Investment Portfolio System at the time of our evaluation, OIG requested a sample of hardcopy Exhibit 300s for review. We reviewed 20 (17%) of the 120 Exhibit 300s and the associated capital planning information submitted by the components for FY 2005. We found that four of the business cases reviewed did not contain IT security costs. The business cases were: EP&R's Multi Hazard Map project, EP&R's e-Nemis, FLETC's Momentum project, and FLETC's Student Administration and Scheduling System project.

The Office of the DHS Chief Financial Officer plans to review and validate all security information contained in budget documents prior to submission to OMB. Because Exhibit 300s were still in draft and Exhibit 53s had not yet been prepared for FY 2005, OIG was unable to verify the numbers DHS prepared.

Recommendations

FISMA requires agencies to report any significant deficiency in the adequacy and effectiveness of information security programs as a material weakness. As such, based on OIG's evaluation of DHS' IT security program, OIG recommends that the Chief Information Officer declare information security a material weakness.

In addition, to assist DHS in the development and implementation of its information security program, the OIG recommends that the Chief Information Officer:

- Conduct an assessment of the Department's various information security programs to determine if there is unnecessary duplication of overhead costs. If such unnecessary duplication is identified, the Chief Information Officer should take steps to redirect resources related to those programs so they can be used in implementing the DHS security program.

- Develop and implement a process to identify information security-related material weaknesses in mission-critical programs and systems. This process should identify all deficiencies that pose a significant risk or threat to operations or assets. In addition, the Chief Information Officer should implement an oversight and reporting function to track the progress of remediation of material weaknesses.

- Conduct certification and accreditation of the Trusted Agent application to provide assurance that all information in the database is secure.

- Complete an inventory of all DHS programs and associated systems and require updates on a periodic basis from Information Systems Security Managers.

- Require DHS Information Officers to assign Information Systems Security Officers to oversee the security controls of each major application and general support system. Further, the Chief Information Officer should require Information Systems Security Managers to oversee the certification and accreditation of all systems within their component.

******

We would like to extend our appreciation to the Department of Homeland Security for the cooperation and courtesies extended to our staff during the review. If you have any questions, please feel free to contact me at (202) 254-4100, or Frank Deffer, Assistant Inspector General, Office of Information Technology Audits, at (202) 254-4041. A list of major contributors to this report is listed in Appendix D.

Our independent evaluation included assessing DHS' progress developing and managing the security program; evaluating data submitted by DHS components for FY 2003; and verifying the reported data. Further, we assessed DHS components' compliance with the requirements of FISMA and related security policies, procedures, standards, and guidelines. In addition, we reviewed a sub set of DHS systems at BICE, EP&R, IAIP, TSA and USCG using NIST 800-26.

OMB requires OIGs to respond to the three performance measurement areas identified in the reporting instructions for FY 2003. These areas include: (1) Overview of FISMA IT Security Reviews; (2) Responsibilities of Agency Head; and (3) Responsibilities of Agency Program Officials and Agency Chief Information Officer.

OIG reviewed component responses, performance measures, and actual practices for five DHS major divisions and several other critical agencies (components).

Our fieldwork was conducted from April through August 2003.

	FY		DHS Management	BTS-ICE (INS)	BTS-CBP (Customs)	BTS-TSA	BTS-FLETC	EPR (FEMA)	Coast Guard	USSS	IAIP	S&T	OIG	Total
Agency employees including contractors	FY03	Total employees	1,000 (F)	35,000 (F)	45,000 (F)	60,091 (A)	1,144	6,972	52,586	6,500	NA	60 (D)	432	208,785
Number and percentage receiving security training		Received training	0	3,540	175	1,200	0	4,055	6,889	1,135	(B)	0 (B)	0	16,994
		Percentage trained	0%	10%	0%	2%	0%	58%	13%	17%	(B)	0%	0%	8%
Employees with significant responsibility	FY03	Total employees	13	162 (E)	800 (E), (F)	5 (E)	20	126 (E)	41 (E)	8	9 (E)	1 (E)	3	1,188
Number and percentage receiving specialized training		Received training	NA	0	396	0	4	125	18	7	9	0	2	561
		Percentage trained	NA	0%	50%	0%	20%	99%	44%	88%	100%	0%	67%	47%
Costs for providing training.	FY03		NA	$240,100(C)	$300,000	$0	$8,147	$4,885	$80,520	$15,000	NA	$0	$1990	$650,642

(A) Employees only (number of contractors not known)
(B) Employees of the components had training under their prior legacy agency
(C) Cost of DHS Security Conference
(D) Includes only headquarters employees
(E) Includes only those in headquarters and known personnel in other offices. Additional security professionals exist but number is unknown.
(F) Estimated
NA Information not provided

The Department of Homeland Security Components

Border & Transportation Security

Immigration and Naturalization Service
Office of Domestic Preparedness
Federal Protection Services
United States Customs Service
Animal and Plant Health Inspection Service
Transportation Security Administration
Federal Law Enforcement Training Center

Emergency Preparedness & Response

Federal Emergency Management Agency
Nuclear Incident Response Team
National Domestic Preparedness Office
Domestic Emergency Support Team
Strategic National Stockpile and National Disaster Medical Systems

Information Analysis & Infrastructure Protection

National Communications System
National Infrastructure Protection Center
Federal Computer Incident Response Center
Critical Infrastructure Assurance Office
National Infrastructure Simulation and Analysis Center

Science & Technology

Plum Island Animal Disease Center
National BW Defense Analysis Center
CBRN Countermeasures Program
Environmental Measurements Laboratory

United States Coast Guard
United States Secret Service
Management
Office of Inspector General

Office of Information Technology
Information Security Division

Frank Deffer, AIG, Office Of Information Technology
Edward G. Coleman, Director, Information Security
Sharon Huiswoud, Audit Manager
Jeff Arman, Audit Manager
Ann Brooks, Audit Manager
Sharell Matthews, IT Auditor
Lane Melton, Computer Specialist
Anthony Nicholson, IT Auditor
George Prytula, IT Auditor
Tom Tsang, Referencer

Department of Homeland Security

Chief of Staff
Deputy Secretary
DHS OIG Liaison
DHS Chief Information Security Officer
DHS Chief Financial Officer
DHS Component Information Officers

Office of Management and Budget

Homeland Bureau Chief
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committee

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