DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Information Technology Management Letter for the FY 2003 DHS Financial Statement Audit

Notice: The Department of Homeland Security, Office of Inspector General, has redacted this report for pubic release. Those redactions are identified as (b)(2), comparable to 5 U.S.C. § 552(b)(2). A review under the Freedom of Information Act will be conducted upon request.

Office of Information Technology

OIG-04-038 September 2004

2001 M Street, NW
Washington, DC 20036

April 1, 2004

Office of Inspector General and Chief Information Officer,
U.S. Department of Homeland Security,
Washington, DC

Ladies and Gentlemen:

We have audited the consolidated balance sheet of the U.S. Department of Homeland Security (DHS) as of September 30, 2003, and the related statement of custodial activity for the seven months then ended and have issued our report thereon dated January 30, 2004. Further, we were engaged to audit the related consolidated statements of net cost and changes in net position, combined statement of budgetary resources, and consolidated statement of financing for the seven months ended September 30, 2003. In planning and performing our audit, we considered DHS's internal controls over financial reporting in order to determine our auditing procedures for the purpose of expressing our opinion on the consolidated balance sheet and the related statement of custodial activity. Audit procedures may not include examining the effectiveness of internal controls and an audit does not provide assurance on internal control. We have not considered internal control since the date of our report.

During our audit we noted certain matters involving information technology (IT) internal controls that are presented herein for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve IT internal controls.

These comments are also presented in the *Independent Auditors' Report* Appendix I, Comment C, "Financial Systems Functionality and Technology", included in the FY 2003 DHS *Performance and Accountability Report*, dated February 13, 2004. Comments related to financial management have been presented in a separate letter to the Office of Inspector General and the DHS Chief Financial Officer dated April 1, 2004.

Our audit procedures were designed primarily to enable us to form an opinion on the consolidated balance sheet and the related statement of custodial activity described above and therefore may not bring to light all weaknesses in policies and procedures that may exist. We aim, however, to use our knowledge of DHS's organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

This report is intended for the information and use of DHS' management, the Office of Inspector General, the U.S. Office of Management and Budget, the U.S. Congress, and the Government Accountability Office, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

Department of Homeland Security

Table of Information Technology Management Comments (ITMC)

September 30, 2003

INFORMATION TECHNOLOGY MANAGEMENT COMMENTS (ITMC)

Section/ FISCAM General Control Area

APPENDICES

INFORMATION TECHNOLOGY OBJECTIVE, SCOPE AND METHODOLOGY APPROACH

KPMG performed a review of DHS IT general controls in support of the FY 2003 DHS financial statement audit. The overall objective of our review was to evaluate the effectiveness of IT general controls of DHS' financial processing environment and related IT infrastructure as necessary to support the audit. The Federal Information System Controls Audit Manual (FISCAM), issued by the Government Accountability Office, formed the basis of our review. The scope of the IT general controls assessment included testing at DHS' Office of the Chief Financial Officer (OCFO) and all significant DHS Bureaus.

FISCAM is designed to inform financial auditors about IT controls and related audit concerns to assist them in planning their audit work. FISCAM also provides guidance to IT auditors when considering the scope and extent of review that generally should be performed when evaluating general controls and the IT environment of a federal agency. FISCAM defines the following six control functions to be essential to the effective operation of the general IT controls environment.

- Entity-wide security program planning and management (EWS) – Controls that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related security controls.
- Access control (AC) – Controls that limit and/or monitor access to computer resources (data, programs, equipment, and facilities) to protect against unauthorized modification, loss, and disclosure.
- Application software development and change control (ASDCC) – Controls that help to prevent the implementation of unauthorized programs or modifications to existing programs.
- System software (SS) – Controls that limit and monitor access to powerful programs that operate computer hardware.
- Segregation of duties (SD) – Controls that constitute policies, procedures, and an organizational structure to prevent one individual from controlling key aspects of computer-related operations, thus deterring unauthorized actions or access to assets or records.
- Service continuity (SC) – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

To complement our general IT controls review, we also performed technical network and system security testing at certain DHS Bureaus. This technical security testing was performed both over the Internet and from within select DHS facilities, and was focused on test, development, and production devices that directly support DHS financial processing and key general support systems.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

We found IT general control weaknesses at DHS and its Bureaus across all FISCAM control areas. Collectively, these weaknesses limit DHS' ability to ensure that critical financial and operational data is maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impact the internal controls over DHS financial reporting and its operation, and we consider them to collectively represent a material weakness under standards established by the American Institute of Certified Public Accountants. A material weakness is a condition in which the design or operation of one or more of the internal control components does not reduce, to a relatively low level, the risk that misstatements, in amounts that would be material in relation to the financial statements being audited, may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions.

A key contributing factor to these issues is the challenge of merging numerous entities into DHS. These various entities have had their own IT functions, controls, and processes. DHS has taken some steps to begin addressing these issues, such as implementing the *Information Technology Security Program Publication*, which contains many requirements for maintaining a DHS-wide information security program. In addition, DHS is currently designing a Department-wide IT architecture, and plans to complete the architecture by the end of FY 2005. Until the architecture is complete and the related IT infrastructure, controls, and processes are implemented, DHS' IT control environment will continue to primarily consist of the IT processes and controls in place at the entities that have been transferred to DHS.

To address these weaknesses DHS needs to design and implement DHS-wide policies and procedures related to IT controls, and to enforce the policies and procedures through the performance of periodic control assessments and audits. Focus should be made on implementing and enforcing a DHS-wide security certification and accreditation (C&A) program, and IT training for administrators and users. Many of the technical issues identified during our review, such as weak technical security controls and the lack of contingency planning strategies, can be addressed through an effective security certification and accreditation program and security training program.

FINDINGS BY FISCAM AREA

Entity-Wide Security Program Planning and Management

DHS needs to improve entity-wide security program planning and management at many of its Bureaus. Collectively, the identified entity-wide security planning and management issues, coupled with the access control issues described later in this management letter, reduce the overall effectiveness of the entity-wide security programs for the individual DHS Bureaus, and the overall Department.

Conditions we cited in the FY 2003 *DHS Performance and Accountability Report* (PAR) regarding entity-wide security program planning and management at DHS and its Bureaus were:

- EWS-03-01 – Security certification and accreditation (C&A) programs were not consistently and thoroughly implemented. Complete system inventories were not maintained, and reviews of controls had not been conducted for many systems.
- EWS-03-02 – Security training and awareness programs were inconsistent.
- EWS-03-03 – Security plans did not consistently document existing system security controls, were incomplete, or otherwise did not meet requirements set forth in Office of Budget and Management (OMB) Circular A-130, *Management of Federal Information Resources*.
- EWS-03-04 – Security risk assessments were not regularly performed and were not performed consistently.

Recommendations:

Entity-wide security program planning and management controls should be in place to establish a framework and continuing cycle of activity to manage security risk, develop security policies, assign responsibilities, and monitor the adequacy of computer security related controls. We recommend that the DHS Chief Information Officer (CIO), in coordination with the OCFO, design and implement a DHS-wide security C&A program to ensure that:

a. A DHS-wide security training and awareness program is designed and implemented consistent with OMB and NIST guidance.
b. Information security planning efforts more consistently follow relevant Federal guidance (OMB and NIST).
c. Security risk assessments are completed in a consistent manner per OMB and NIST guidance.
d. The above recommended entity-wide security efforts are implemented in a consistent manner across Bureaus.
e. Close linkage exists between the DHS C&A program to the DHS budget control mechanisms;
f. Evidence of sound IT controls can be demonstrated before systems and other IT efforts receive funding.

Access Controls

The significant access control vulnerabilities we identified during this audit were internal (i.e., inside the Bureaus' firewalls). Personnel inside the organization who best understood the organization's systems, applications, and business processes were able to make unauthorized access to some systems and applications. Some of the identified vulnerable devices were used for test and development purposes. In some cases, users were able to access test and development devices with group passwords, system default passwords, or the same passwords with which they log into production devices. As a result, test and development devices could be a target of hackers/crackers, as the information obtained from the devices (i.e., user password listings) can be used to attempt further access into DHS' IT environment.

Conditions we cited in the PAR regarding access controls at DHS and its Bureaus were:

- AC-03-01 – Instances of missing user passwords on key servers and databases, weak user passwords, and weaknesses in user account management were noted. Also, we noted several cases where user accounts were not periodically reviewed for appropriateness, including authorizations to use group user accounts and to identify excessive access privileges.
- AC-03-02 – Instances where workstations, servers, or network devices were configured without necessary security patches, or were not configured in the most secure manner. We also identified many user accounts that were not configured for automatic log-off or account lockout.

Recommendations:

In close concert with an organization's entity-wide information security program, access controls for general support systems and applications should provide reasonable assurance that computer resources such as data files, application programs, and computer-related facilities and equipment are protected against unauthorized modification, disclosure, loss, or impairment. Access controls are facilitated by an organization's entity-wide security program. Such controls include physical controls, such as keeping computers in locked rooms to limit physical access, and logical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files. Inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of information.

We recommend that the DHS CIO, in coordination with the OCFO, ensure that:

a. Password controls meet DHS password requirements and are enforced on all systems.
b. A password account management process is implemented within the Bureaus to ensure the periodic review of user accounts.
c. A DHS-wide patch and security configuration process is designed and implemented.
d. A vulnerability assessment process is implemented, whereby systems are periodically reviewed for security weaknesses.
e. The above recommendations are included as part of the DHS C&A program.

Application Software Development and Change Control

DHS needs to improve application software development and change control to better manage and control the changes that are made to software applications in operation. We noted weaknesses in controls, and policies and procedures used to modify application software programs that would enable unauthorized programs and modifications to be implemented. Without proper controls, there is a risk that security features could be inadvertently or deliberately omitted or turned off, or that processing irregularities or malicious code could be introduced into the IT environment. Application change controls are also an important component of an organization's information security program.

Conditions we cited in the PAR regarding application software development and change control at DHS and its Bureaus were:

- ASDCC-03-01 – Instances where Bureaus did not document changes made to applications and related change approvals. Procedures for documenting, approving, and implementing application changes were not consistently in place and applied.
- ASDCC-03-02 – Changes to software were not always tested prior to implementation, and movement of changes into the production environment was not always controlled.

Recommendations:

We recommend that the DHS CIO, in coordination with the OCFO, ensure that:

a. An entity-wide application change control policy is implemented that requires changes to be authorized and tested prior to implementation.
b. A policy is adopted requiring documentation of specific changes and related approvals.
c. A policy is adopted requiring the analysis of change requests to ensure consistency with agency policy, user requirements, and implementation schedules.

System Software

We noted weaknesses in programs designed to operate and control the processing activities of computer equipment. These weaknesses increase the likelihood that unauthorized individuals using system software could circumvent security controls to read, modify, or delete critical or sensitive information and programs. Authorized users of the system could gain unauthorized privileges to conduct unauthorized actions; and/or systems software could be used to circumvent edits and other controls built into application programs.

Conditions we cited in the PAR regarding system software at DHS and its Bureaus were:

- SS-03-01 – Instances where policies and procedures for restricting and monitoring access to operating system software were not implemented, or were inadequate. In some cases, the ability to monitor security logs did not exist.
- SS-03-02 – Changes to sensitive operating system settings were not always documented.

Recommendations:

We recommend that the DHS CIO, in coordination with the OCFO, ensure that:

a. Policies and procedures are in place for monitoring, use, and changes related to operating systems.
b. Bureau personnel comply with the established policies and procedures.

Segregation of Duties

We noted instances where an individual controlled more than one critical function within a process, increasing the risk that erroneous or fraudulent transactions could be processed, improper program changes could be implemented, and computer resources could be damaged or destroyed. Additionally, we noted a lack of segregation of duties among major operating and programming activities, including duties performed by users, application programmers, and data center staff.

Conditions we cited in the PAR regarding segregation of duties at DHS and its Bureaus were:

- SD-03-01 – Instances where individuals were able to perform incompatible functions, such as the changing, testing, and implementing software, without sufficient compensating controls in place.
- SD-03-02 – Instances where key security positions were not defined or assigned, and descriptions of positions were not documented or updated.

Recommendations:

We recommend that the DHS CIO, in coordination with the OCFO, ensure that:

a. Responsibilities are documented so that incompatible duties are consistently separated. If this is not feasible given the smaller size of certain functions, then sufficient compensating controls, such as periodic peer reviews, should be implemented.
b. Policies and procedures are developed and documented to address segregation of duties for IT and accounting functions.

Service Continuity

Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency’s ability to accomplish its mission.

Conditions we cited in the PAR regarding service continuity at DHS and its Bureaus were:

- SC-03-01 – Several Bureaus had incomplete business continuity plans and systems with incomplete disaster recovery plans. Some plans did not contain current system information, emergency processing priorities, procedures for backup and storage, or other critical information.
- SC-03-02 – Some Bureau service continuity plans were not consistently tested, and individuals did not receive training on how to respond to emergency situations.

Recommendations:

We recommend that the DHS CIO, in coordination with the OCFO, ensure that:

a. Bureaus develop and implement complete business continuity plans and system disaster recovery plans.
b. Bureau specific and DHS-wide testing of key service continuity capabilities are performed.
c. A DHS-wide service continuity training program is designed and implemented.
d. Backup and recovery processes more consistently follow relevant Federal guidance (OMB and NIST).

MANAGEMENT COMMENTS AND OIG EVALUATION

We obtained written comments on a draft of this report from the DHS CIO. Generally, the DHS CIO agreed with all of the report's findings and recommendations. We have incorporated the comments where appropriate and included a copy of the comments in their entirety at Appendix C.

In his response, the DHS CIO stated that guidance for the majority of the issues identified in this report has been developed at the DHS CIO level and is documented in the Department of Homeland Security Sensitive Systems Handbook Publication 4300A and Department of Homeland Security National Security Systems Handbook Publication 4300B, Version 2.0, dated March 31, 2004. These handbooks provide DHS organizational element CIOs, Information Systems Security Managers (ISSMs) and Information Systems Security Officers (ISSOs) the necessary guidance to develop specific policies and procedures for their individual application systems.

In addition, the DHS CIO identified a number of areas where DHS is making progress towards establishing and maintaining a DHS-wide security program. For example, according to the DHS CIO:

- To ensure that DHS employees and contractors receive initial and annual security awareness training, the Chief Information Security Officer has a dedicated Training Program Director who has produced an information systems security training awareness course for the Department. The training is available on the Internet, through compact disc and through the DHS Information Systems Security Policy and Handbook.
- DHS is procuring and installing an enterprise-wide C&A tool that will have the ability to generate test plans that are mapped to DHS policy and ensure that policy compliance is actually tested during the security test and evaluation phase of the C&A process. In addition, DHS policy requires that all information systems, including financial systems, undergo a security self-assessment in accordance with the guidance in NIST 800-26, Security Self-Assessment Guide for Information Technology Systems, on an annual basis. The status of this activity is monitored in the DHS Information Security Digital Dashboard.
- DHS' password policy has been published and is required as part of any new or ongoing information technology development and deployment initiatives. These password requirements are being enforced from a management perspective through the use of the Enterprise Architecture Board reviews as well as through C&A efforts.
- DHS has developed section 5.4.8 of the DHS Information Security Program Handbook that identifies the vulnerability assessment process for organizational elements. In addition, this policy has been supplemented with a more complete agency-wide vulnerability assessment program that is currently being finalized for inclusion in the Security Program Handbook.
- DHS has ISSMs in place for each organizational element who are responsible for ensuring bureau personnel comply with established policies and procedures. These ISSMs meet with the DHS Chief Information Security Officer on a regular basis to discuss issues and risks associated with rolling out a comprehensive Information Security Program. To help support the ISSMs a Digital Dashboard and a balanced scorecard have been developed to provide adequate management visibility to the issue of bureau compliance.

DHS agrees that DHS systems and applications should have complete and current contingency and disaster recovery plans. Toward that end, the CISO has developed the Digital Dashboard that includes a Continuity Planning metric. This metric is based on the percentage of systems with business contingency plans and the percentage of business contingency plans that have been tested.

OIG Response

Although the DHS CIO has taken the necessary steps to develop these entity-wide policies, the organizational element ISSMs and ISSOs need to continue to ensure that employees are made aware of the policies and procedures in place over the DHS security program and any updates made to them. In addition, ISSMs and ISSOs should continue to periodically monitor compliance with these polices and procedures through the use of such tools as the digital dashboard and the balanced scorecard.

Department of Homeland Security
Information Technology Management Comments
September 30, 2003

INFORMATION TECHNOLOGY NOTICE OF FINDING AND RECOMMENDATION (NFR) CROSSWALK

Bureau	NFR No.	Control Area	Description	Page
CONS IT	03-01	Entity-Wide Security	Security requirements for service providers should be better documented	2
CONS IT	03-02	Entity-Wide Security	Lack of assessment or assurance of security controls in place over TIER and CFO Vision	2
CONS IT	03-03	Service Continuity	DHS TIER resides on a test server	6
CONS IT	03-04	Access Controls	TIER access controls can be improved	3
CONS IT	03-05	Entity-Wide Security	Lack of a comprehensive and accurate financial system inventory	2
(b)(2)High (b)(2)High	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

INFORMATION TECHNOLOGY NFR CROSSWALK, CONTINUED

(b)(2)High

Bureau	NFR No.	Control Area	Description	Page
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

INFORMATION TECHNOLOGY NFR CROSSWALK, CONTINUED

(b)(2)High

Bureau	NFR No.	Control Area	Description	Page
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

INFORMATION TECHNOLOGY -- DHS AND BUREAU COVERAGE

Below is a description of significant DHS financial management systems and supporting IT infrastructure included in the scope of the financial statement audit for the seven months ended September 30, 2003.

CIS/ICE

Locations of Review: Citizenship and Immigration Services (CIS)/ Immigration and Customs Enforcement (ICE) – Headquarters in Washington, D.C. and the Dallas Finance Center in Dallas, Texas.

Systems Subject to Review:

Federal Financial Management System (FFMS) – FFMS supports all of CIS/ICE core financial processing. FFMS uses a Standard General Ledger (SGL) for the accounting of agency financial transactions.

Claims 3 and Claims 4 – Claims 3 and Claims 4 are databases used to track pending applications, and are accessible by the various CIS/ICE service centers. Claims 3 contains totals of pending immigration applications (by application type), while Claims 4 contains totals of pending naturalization/citizenship applications. The Claims 3 mainframe acts as a central repository for entering data into the Claims 3 Local Area Network (LAN) via a daily upload process. The district offices do not have direct access to the Claims 3 mainframe platform.

Performance Analysis System (PAS) – PAS receives pending application information from Claims 3 and Claims 4 systems. The CIS/ICE Office of Immigration Statistics analyzes the PAS data and makes necessary adjustments to provide monthly statistics on pending and completed applications to interested parties.

PC Receipt and A-File Accountability and Control System (RAFACS) – RAFACS is used to track the status and location of applications within a service center. CIS uses bar code scanners to enter application information into RAFACS. Whenever an application is moved from one stage to another, CIS uses a bar code scanner to update the application's status in RAFACS. This system updates the application's status and location information into Claims 3 or Claims 4 (depending on application type).

Coast Guard

Locations of Review: United States Coast Guard (Coast Guard) – The Aviation Repair and Supply Center (ARSC) in Elizabeth City, North Carolina; the Coast Guard Finance Center (FINCEN) in Chesapeake, Virginia; the Operations Supply Center (OSC) in Martinsburg, West Virginia; and the Personnel Service Center (PSC) in Topeka, Kansas.

Systems Subject to Review:

Coast Guard Oracle Financials (CGOF) – During FY 2003 the Coast Guard converted to CGOF from the Department of Transportation's (DOT) core accounting system, the Departmental Accounting and Financial Information System (DAFIS). CGOF is hosted at FINCEN, the Coast Guard's primary data center.

Naval Electronics Supply Support System (NESSS) – Formerly named the Supply Center Computer Replacement System (SCCR), NESSS is hosted at OSC. NESSS is the primary financial application for the Engineering Logistics Command (ELC), the Supply Fund, and the Yard fund.

Aircraft Logistics Management Information System's (ALMIS) – Hosted at the ARSC, ALMIS is used to track and schedule aircraft maintenance and configuration, as well as provide support for the procurement, inventory management, accounting, aircrew qualifications, flight operations, and decision support functions for the ARSC and the 25 air stations. The Aviation Maintenance Management Information System (AMMIS) is a component of ALIMS, and provides the ability to track and schedule aircraft maintenance and configuration as well as provide support for procurement, inventory management, and accounting.

Several other key Coast Guard financial applications support military personnel and payroll, retired pay, and travel claims. These applications are hosted at the PSC, which was formerly known as the Human Resources Services and Information Center.

CBP

Locations of Review: Customs and Border Protection (CBP) National Finance Center in Indianapolis, Indiana and the Newington Data Center in Newington, Virginia.

Systems Subject to Review:

Asset Information Management System (AIMS) – AIMS is CBP's financial management system that supports primary financial accounting and reporting processes, and a number of additional subsystems for specific operational and administrative management functions. The core system consists of general ledger, accounts receivable, disbursements/payables, purchasing, and budget execution accounts. AIMS includes for its core pieces a customized version of American Management Systems' software – Federal Financial System (FFS).

Automated Commercial System (ACS) – ACS is a collection of applications used to track, control, and process all commercial goods, conveyances and private aircraft entering the United States territory, for the purpose of collecting import duties, fees, and taxes owed the Federal government.

Seized Assets and Cases Tracking System (SEACATS) – Used for tracking seized assets, customs forfeiture fund, and fines & penalties.

CBP also maintains personnel, payroll, and scheduling systems.

DHS Consolidated

Location of Review: DHS Consolidated - DHS Headquarters in Washington, D.C.

Systems Subject to Review:

Treasury Information Executive Repository (TIER) – The system of record for the DHS consolidated financial statements is TIER. The DHS Bureaus update TIER on a monthly basis with data extracted from their core financial management systems. TIER subjects Bureau financial data to a series of validation and edit checks before it becomes part of the system of record. Data cannot be modified directly in TIER, but must be resubmitted as an input file.

CFO Vision – CFO Vision interfaces with TIER, and is used for the consolidation of the financial data and the preparation of the DHS financial statements.

The TIER and CFO Vision applications reside on the Department of Treasury's (Treasury) network and are administered by Treasury. Treasury is responsible for the administration of the TIER server, database, and the TIER and CFO Visions applications. In October 2003 the TIER application was migrated from Treasury to a contractor site. The DHS Office of Financial Management (OFM) is responsible for the administration of user accounts within the TIER and CFO Vision applications.

Emergency Preparedness and Response

Locations of Review: Federal Emergency Management Agency (FEMA) - Headquarters in Washington, D.C. and Mount Weather Emergency Assistance Center (MWEAC) in Bluemont, Virginia.

Systems Subject to Review:

Integrated Financial Management Information System (IFMIS) – IFMIS is the key financial reporting system, and has several feeder subsystems (budget, procurement, accounting, and other administrative processes and reporting).

National Emergency Management Information System (NEMIS) – NEMIS is an integrated system to provide FEMA, the States, and certain other Federal agencies with automation to perform disaster related operations. NEMIS supports all phases of emergency management, and provides financial related data to IFMIS via an automated interface.

Limited Scope and Secret Service

Locations of Review: Limited Scope Entities – There were many entities transitioned into DHS that did not have a high enough financial dollar materiality to justify the performance of extensive IT testing. For these entities we performed limited procedures including questionnaires and interviews, and based on the results of the questionnaires and interviews, we decided to perform additional IT tests of controls supporting two entities: 1) Federal Law Enforcement Training Center (FLETC), and 2) United States Secret Service (Secret Service). We performed tests of controls in place and operating at Secret Service Headquarters in Washington, D.C., and FLETC Headquarters in Glynco, Georgia.

ODP

Location of Review: Office of Domestic Preparedness (ODP) – Headquarters in Washington, D.C.

Systems Subject to Review:
ODP's IT platforms are hosted and supported by the Department of Justice's Office of Justice Programs (OJP). The following is a list of key financial related applications supporting ODP.

IFMIS (same application as FEMA, but hosted at OJP) – IFMIS consists of five modules that include: budget, cost posting, disbursement, general ledger, and accounts receivable. Users access the system through individual workstations that are installed throughout ODP and OJP. The current IFMIS version does not have the ability to produce external federal financial reports (i.e., SF132 and SF133) and financial statements. IFMIS was updated in February 2002 with the version certified by the Joint Financial Management Improvement Program (JFMIP).

Grants Management System (GMS) – GMS supports the ODP grant management process involving the receipt of grant applications and grant processing activities. GMS is divided into two logical elements. There is a grantee and an administration element within the system. The grantee component provides the Internet interface and functionality required for all of the grantees to submit grant applications on-line. The second component, the administration component, provides ODP/OJP personnel the tools required to store, process, track and ultimately make decisions about the applications submitted by the grantee. This system does not interface directly with IFMIS.

Line of Credit Electronic System (LOCES) – The LOCES allows recipients of ODP funds to electronically request payment from OJP on one day and receive a direct deposit to their bank for the requested funds usually on the following day. Batch information containing drawdown transaction information from LOCES is transferred to IFMIS. The IFMIS system then interfaces with Treasury to transfer payment information to Treasury, resulting in a disbursement of funds to the grantee.

Paperless Request System – This system allows grantees to access their grant funds. The system includes a front and back end application. The front-end application provides the interface where grantees make their grant requests. The back end application is primarily used by accountants and certifying officials. The back end application also interfaces with the IFMIS application. Batch information containing drawdown transaction information from the Paperless Request System is interfaced with IFMIS. The IFMIS system then interfaces with Treasury to transfer payment information to Treasury, resulting in a disbursement of funds to the grantee.

Interior Department Electronic Acquisition System (IDEA) – This stand-alone system is used to authorize (approve), manage, and track various types of acquisition requests. This system does not interface with IFMIS. IDEA processes transactions that affect the procurement process.

TSA

Locations of Review: Transportation Security Administration (TSA) – Headquarters in Washington, D.C., and DOT data center in Oklahoma City, Oklahoma. TSA's financial applications are hosted on DOT IT platforms.

Systems Subject to Review:

Consolidated Uniform Payroll System (CUPS) – CUPS maintains TSA payroll data and archives calculates pay, wages, and tax information and maintains service history and separation records.

Consolidated Personnel Management Information System (CPMIS) – CPMIS is the DOT personnel management system. The system processes and tracks personnel actions and employee related data for TSA, including employee elections for the Thrift Savings Plan (TSP), life insurance, and health insurance as well as training data and general employee information (i.e. name, address, etc.). CPMIS is also used to maintain information related to budget, training, civil rights, labor relations and security. CPMIS interfaces with CUPS to allow CUPS to perform the calculation of pay, time and attendance reporting, leave accounting, and wage and tax reporting. CUPS also uses the information received from CPMIS to initiate payroll deductions for TSP, insurances, Combined Federal Campaign contributions, and savings bonds.

Delphi – Delphi is the TSA core financial management system, which provides accounts payable, accounts receivable, general ledger, and budgeting functionality. Delphi is a commercial off–the–shelf (COTS) software package.

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

Homeland
Security

May 11, 2004

MEMORANDUM

TO: Clark Kent Ervin
Acting Inspector General
Department of Homeland Security

FROM: Steve Cooper Steve Cooper
Chief Information Officer
Department of Homeland Security

SUBJECT: Response to Draft IT Management Letter

REFERENCE: Your memorandum to me dated March 22, 2004, Subject, "Draft Report: Review of IT Controls in Place over Department of Homeland Security' Financial Systems for the Year Ended September 30, 2003."

Thank you for the opportunity to comment on the referenced draft report. Information Technology systems do significantly facilitate Department of Homeland Security' financial processing activities as well as the Department's ability to maintain important financial data, and I look forward to working with you and your staff in resolving the recommendations from the FY 03 audit to the satisfaction of all concerned. I also look forward to working more closely with you and the Chief Financial Officer in the successful conduct of the FY 04 financial audit.

While this audit certainly establishes a solid baseline from which we can plan for and build good financial management processes in the future, I would like to provide some specific comments on the Draft Report. These comments fall in three areas. First, while the report necessarily focuses on the negative aspects of program issues requiring remediation, I would like to provide an overview of the significant and positive progress we have made to date. As you may be aware, we are already aggressively implementing the many required elements of a statutorily compliant Information Security Program for the Department, and I want you to know that we are committed to building a successful program as soon as possible. Second, I would like to provide a general comment and recommendation concerning the overall audit methodology used in the FY 03 audit. Third, I would like to provide specific comments for each of the 20 recommendations made by your team, again focusing on the positive progress we have made to date.

1. Program Status: As stated in the February 13, 2004 Independent Auditors' Report on Department of Homeland Security' Financial Statements, Audit Report No. OIG-O4-10, much of the FY 03 financial audit field work took place when the Department of Homeland Security program was in its infancy. Under my direction, the Department of Homeland Security Chief Information Security Officer is realigning the major information security functions of the 22 legacy agencies into a comprehensive Department-wide information security umbrella to increase and improve the Department's overall information security posture. This consolidation will ensure a consistent strategic approach to strengthen information security throughout the Department and will provide common goals and objectives for all current and future information security initiatives within the Department.

A *Department of Homeland Security Information Security Program Strategic Plan* (released September 15, 2003*)* and *Program Management Plan* (released November 12, 2003) represent a vision of a unified information security program for the Department by identifying major program areas, goals, and objectives for the next five years. As part of the Strategic Plan, the Chief Information Security Officer identified eight Department of Homeland Security Information Security Program areas that address the majority of the CIO recommendations in the Draft Information Technology Management Letter:

- Program Management and Integration
- Security Policy
- Compliance and Oversight
- Information Security Training, Education, and Awareness
- Security Architecture
- Security Operations
- Continuity Planning for Critical Department of Homeland Security Assets
- National Security Systems and Communications Security (COMSEC) Management.

For most of the information security program areas, oversight is the major focus of the Department of Homeland Security Headquarters activities. Strong oversight is required to ensure that the Department has enterprise-wide, repeatable, and robust processes for meeting federal information security requirements and to ensure accurate assessments of the aggregated security postures of each of the Organizational Elements (e.g., bureau).

Due to the extended geographic size, as well as the large scope of the Department's core mission areas, the responsibility for ensuring that all day-to-day security requirements are met are delegated to the Organizational Elements level to ensure that mission owners are directly involved with risk acceptance and mitigation decisions. Each Organizational Elements has an appointed Information Systems Security Manager to ensure that the information security requirements are implemented and security policies are enforced.

The Chief Information Security Officer Program Director for each of the Information Security Program areas have either completed or begun enterprise initiatives to support the Department of Homeland Security Organizational Elements in meeting their security responsibilities. These initiatives are summarized in Attachment 1.

In addition, the Department of Homeland Security Chief Information Security Officer has initiated internal assessments to verify, validate, and elaborate on the security posture at the agency-wide and Organizational Element-level. These internal assessments use a Balanced Scorecard and Digital Dashboard as tools to communicate compliance with the Department of Homeland Security Information Security Program, progress in meeting and sustaining the Department of Homeland Security Information Security Program goals and objectives, and status with senior Department of Homeland Security management of the individual programs and the organization as a whole.

- A Balanced Scorecard is the tool for aligning the Information Security Program strategy to the short-term actions necessary to successfully implement the program and to encourage accountability by the Department of Homeland Security Organizational Elements. The scorecard helps the Organizational Elements correlate short-term actions and initiatives with performance objective and measures of the overall Information Security Program. In addition, the scorecard provides a common reporting process to facilitate the alignment of the Information Security Program across the Organizational Elements. Attachment 2 contains a representation of the Department of Homeland Security Information Security Program Balanced Scorecard.
- The Digital Dashboard reports aggregated information security data at the Organizational Element and Department level. The dashboard serves as a management tool to ensure that Organizational Elements take a risk-based, cost-effective approach to secure their information and systems, identify and resolve current Information Technology security weaknesses and risks, as well as protect against future vulnerabilities and threats. The dashboard allows Department of Homeland Security management to monitor Organizational Element remediation efforts to more accurately identify progress and problems. Attachment 3 contains a representation of the Department of Homeland Security Information Security Program Digital Dashboard.

2. Audit methodology: An overall comment and concern is that the Draft Information Technology Management Letter does not provide linkage, or supporting analysis, between the detailed Notices of Findings and Recommendations and the specific weaknesses noted in the draft management letter. Additionally, the Draft Information Technology Management Letter Report does not provide any discussion of the rationale for determining significance or materiality. As a result, it is difficult for the Department to develop specific corrective actions at the Department and the Organizational Element level beyond what is outlined in the responses above

Discussion with you staff has indicated that supporting analysis showing the link between the NFRs and the weaknesses will be provided. Based on receipt of that analysis, detailed corrective action plans for remediation will be developed in coordination with your staff and the audit team as required. Once developed, the action plans be added to the Department of Homeland Security Plans of Action and Milestones database (Trusted Agent FISMA), in accordance with the Office of Management and Budget Federal Information Security Management Act reporting instructions as currently defined by OMB Memorandum M-03-19.

3. Specific recommendations: Comments on each of the 20 specific recommendations follow.

Recommendation #1 - The DHS CIO should ensure that a DHS-wide security C&A program is designed and implemented, and also encompasses recommendations 2-4.

In November 2003, Department of Homeland Security identified the procurement and installation of an enterprise Certification and Accreditation application as the number one security key initiative. Implementation of an enterprise Certification and Accreditation Tool, the first steps toward a Department of Homeland Security-wide Certification and Accreditation Program, was initiated by the Compliance and Oversight Program Director. An independent technical evaluation of commercial Certification and Accreditation Tools was completed on April 28, 2004. The independent technical evaluation resulted in a recommended Certification and Accreditation Tool and acquisition of the Certification and Accreditation Tool is in progress. The current implementation goal is to install the Certification and Accreditation tool at the Department of Homeland Security Battelle Operations Center in Stafford, Virginia by August 2004. A six-month pilot will be conducted that will develop and test the Concept of Operations for the Certification and Accreditation Tool and the implementation of an enterprise Certification and Accreditation process. At successful completion of the pilot, use of the Certification and Accreditation tool and the Department of Homeland Security Certification and Accreditation process will be mandatory for all systems, including financial systems.

The Department of Homeland Security Chief Information Security Officer is aware of the compelling need to improve the number of systems with completed Certification and Accreditation's. Percentage of completed Certification and Accreditation's is one of the metrics included in the Department of Homeland Security Information Security Program Digital Dashboard to highlight to Department of Homeland Security and Organizational Element management, the importance of adequate resources for Certification and Accreditation activities.

Recommendation #2 – A DHS side security training and awareness program is designed and implemented.

The Chief Information Security Officer has a dedicated Training Program Director[1] who has produced an information systems security awareness training course for the Department. The training reflects the Department of Homeland Security mission, culture, and security policy. The training is available in the following formats:

- Online Training via Department of Homeland Security Online and the Internet. To access it on Online the navigation is: Home Page → Management → Chief Information Officer → Chief Information Security Officer Page. The Internet URL is:https://www.brainbench.com/xml/dhs/logon.xml?promocode=Department of Homeland Security Awareness. The system automatically tracks users by Organizational Element, Training & Completion Date, Ranking among other users and strengths and weaknesses by topic. This training is available to all

[1] Currently, the Security Training Program Director position is vacant as of April 2004 and a new replacement is currently being sought.

Department of Homeland Security personnel and contractors that have been issued a Department of Homeland Security network account.

- Department of Homeland Security Information Systems Security Awareness CD. This is available to personnel that do not have network access.
- Department of Homeland Security Information Systems Security Policy and Handbook. These documents are available at http://www.dhs.gov.

At this time, most Organizational Elements are taking advantage of these resources. The exceptions are Immigration and Customs Enforcement and Transportation Security Administration. Immigration and Customs Enforcement and Transportation Security Administration have their own learning management systems but are required to add the Department of Homeland Security training to their systems.

The Department of Homeland Security Chief Information Security Officer is aware of the urgent need to improve the number of Department of Homeland Security employees and contractors that receive initial and annual security awareness training. Training metrics are included in the Department of Homeland Security Information Security Program Digital Dashboard to highlight to Department of Homeland Security and Organizational Element Management the requirement for annual information security awareness training.

Recommendation #3 – Security planning efforts and the implementation of security planning efforts more consistently follow relevant Federal guidance (i.e. OMB Circular A-130).

The Department of Homeland Security information security policies for sensitive systems and NSS are published as Management Directives 4300A and B, respectively, and are intended to consistently following relevant Federal guidance. Attachment A of the companion Handbooks is a Requirements Traceability Matrix that shows the relationship between the Department of Homeland Security requirements and the federal guidance that is the primary source of the requirement.

In addition, we have implemented a three prong approach to address the challenges of consistent security planning for legacy Information Technology systems, current Information Technology programs, and new Information Technology initiatives.

For legacy Information Technology systems, the Compliance and Oversight Program Director is using the results of the self-reporting results from our Trusted Agent Federal Information Security Management Act Reporting tool to identify gaps in our security planning and compliance efforts. Any gaps are reported to senior management and addressed to determine if any relevant corrective actions are necessary and practical. In addition, the Compliance and Oversight Program Director is performing periodic reviews to determine the validity of the self-reported data. I have authorized the Chief Information Security Officer to ensure adequate management visibility of any issues.

For current Information Technology programs under development, the Security Policy Program Director participates on the Department of Homeland Security Enterprise Architecture Board to ensure compliance of programs going forward in meeting the agency expectations for Security Planning and Federal guidance compliance. As I reported to Subcommittee on Cyber Security, Science, and Research & Development on

March 30, 2004, this group is now operational. The Program Director looks to ensure compliance of security planning for many of the key issues reported, including risk analysis, configuration management, security controls, and other factors.

For new Information Technology initiatives, the Chief Information Security Officer is included in all new projects reviews as part of the Department's Capital Investment Control process. The Security Policy Program Director reviews all new projects to ensure that they include adequate funding for information security during the life cycle of the project. The Information Security Policy Program Director has the authority to turn back projects that do not have appropriate and sufficient funding for information security.

Recommendation #4 – Security risk assessments are completed in a consistent manner.

As discussed in the response to Recommendation #1, Department of Homeland Security is in the process of procuring and installing an enterprise Certification and Accreditation Tool. One of the major benefits of the Certification and Accreditation Tool will be the ability to generate test plans that are mapped to Department of Homeland Security policy and ensure that policy compliance is actually tested during the Security Test and Evaluation Phase of the Certification and Accreditation process. Additionally, this application will help ensure uniform Certification and Accreditation quality (and address recommendations #3 and #4) and provide improved management reporting. It should be noted that due to the three year Certification and Accreditation life cycle and the cost and complexity of certifying systems, achieving the full benefits from the enterprise Certification and Accreditation Tool will be a long-term Department of Homeland Security objective.

In addition, Department of Homeland Security policy requires that all information systems, including financial systems, undergo a security self-assessment in accordance with the guidance in NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems,* on an annual basis. The status of this activity is monitored in the Department of Homeland Security Information Security Digital Dashboard.

Recommendation #5 – DHS implement the above entity-wide security efforts in a consistent manner (refers to recommendations 1-4).

As discussed in the second paragraph of this memorandum, Department of Homeland Security has implemented an entity-wide Information Security Program to realign the major information security functions of the 22 legacy agencies into a comprehensive Department-wide information security umbrella to increase. This consolidation will ensure a consistent strategic approach to strengthen information security throughout the Department and will provide common goals and objectives for all current and future information security initiatives within the Department.

Recommendation # 6 – The DHS C&A program should be closely linked to the Department's budget control mechanisms, to ensure that before systems and other IT efforts receive funding, evidence of sound IT controls can be demonstrated.

The Department of Homeland Security CPIC process was released as Department of Homeland Security Management Directive MD-1400 to address this issue. The Enterprise Architecture Board is responsible for reviewing all Information Technology investments with either annual costs greater than $1M or life-cycle costs greater than $5M. The Enterprise Architecture Board reviews all Information Technology programs currently under development or being initiated. The Security Policy Program Director participates on the Enterprise Architecture Board to ensure adequate visibility and compliance with the Department of Homeland Security life-cycle approach to Certification and Accreditation and sound Information Technology controls. Once the agency-wide Certification and Accreditation Tool is in place, more detailed reporting will be used to supplement the Enterprise Architecture Board review and strengthen this linkage. Any issues resulting from the Enterprise Architecture Board review are directed to the Investment Review Board, Management Review Council, and the Director of Program Analysis and Evaluation as appropriate.

For the legacy systems reviewed in the audit, the Compliance and Oversight Program Director is performing random reviews of the reported Certification and Accreditation compliance from the Federal Information Security Management Act self-reported results. Any gaps from this review are raised with senior management to determine if any corrective action is necessary. However, due to the need for maintaining operational systems until the new Department of Homeland Security architecture and infrastructure can be fully defined, we recognize that some actions are not as strong as desirable.

Recommendation #7 – Password controls that meet DHS password requirements are enforced on all systems.

Department of Homeland Security password policy has been published and is required as part of any new or ongoing Information Technology development and deployment initiatives. The password requirements are being enforced from a management perspective through the use of the Enterprise Architecture Board Reviews as well as Certification and Accreditation efforts. Any deviation from the Department of Homeland Security policy is addressed in the relevant Authorization to operate letter or Interim Authorization to Operate letter. At the time of the audit, the Enterprise Architecture Board process and policy documents were still being finalized and have now been fully released.

For legacy systems, which were deployed prior to the Department of Homeland Security password policy, and systems which may not have the capability to enforce the Department of Homeland Security password policy, the responsibility is placed more fully on the users. The Chief Information Security Officer is working with the Organizational Element Information Systems Security Managers, who work with the individual Information System Security Officer to get their end-users to comply with Department of Homeland Security passwords requirements. The Information System Security Officer obtain compliance through signed Rules of Behavior, improved security awareness training (which incorporates Department of Homeland Security password requirements), and on-going vulnerability assessments. Many of the automated vulnerability assessment tools in place are capable of evaluating password compliance and provide feedback for the Certification and Accreditation process. As legacy systems go through their 3-year review cycle, password requirements will be addressed on all Department of Homeland Security systems as well.

Recommendation #8 – A DHS-wide patch and security configuration process is designed and implemented.

At the present time Department of Homeland Security policy and guidance (Section 3.7), makes Information System Security Officers responsible for ensuring patch and security configuration management. Guidance on patch management is included in Department of Homeland Security Sensitive Systems Handbook Publication 4300A and Department of Homeland Security National Security Systems Handbook Publication 4300B, Version 2.0, dated March 31, 2004. Given the current Information Technology environment with numerous and disparate legacy Information Technology systems, this solution is appropriate for the Department at this time. As the Department of Homeland Security moves to "One Infrastructure," Department of Homeland Security-wide solutions will become more appropriate.

Recommendation #9 – DHS bureaus implement a password account management process to ensure the periodic review of accounts.

The implementation of Department of Homeland Security policy with regard to password account management is the responsibility of the Information System Security Officer assigned to a particular system. The Chief Information Security Officer has implemented numerous initiatives recently to help strengthen the implementation of policy at the Information System Security Officer level. These initiatives include:

- Development of the Information Systems Security Manager Guide to clarify the roles of the Organizational Element Information Systems Security Managers and the Information System Security Officers.
- Assigned responsibility to the Information Systems Security Managers to ensure all systems have an Information System Security Officer identified and trained to address issues such as password account management.
- Ensuring that information securing professional training is available and provided at the Information System Security Officer levels
- Managing the Information System Security Board to address issues related to moving the Department of Homeland Security Policy into the Organizational Element and system security plans and procedures.
- Directing the Compliance and Oversight Program Director to strengthen the process for defining System Security Plans in a consistent and repeatable manner where password account, change control management, etc. is more reliable.
- Raising visibility of non-compliance with Department of Homeland Security policy to senior management at the Organizational Element level through a digital dashboard and scorecard.
- Conducting periodic reviews of completed Certification and Accreditation Packages at the Organizational Element Level by the Compliance and Oversight Program Director to identify any gaps or corrective actions that would reduce risk to Department of Homeland Security Information Technology Systems.

Recommendation #10 – A vulnerability assessment process is implemented, where systems are periodically assessed for security vulnerabilities, especially before they enter production.

Section 5.4.8 of the Department of Homeland Security Information Security Program Handbooks identifies the vulnerability assessment process for Organizational Elements to employ. In addition, the Security Operations Program Director identified the need to supplement the existing policy with a more complete Vulnerability Assessment Program from an agency-wide perspective. This program was released for review in February 2004 and is currently begin finalized before final released as Appendix O to the Security Program Handbook.

The Security Operations Program Director is currently working with the Chief Information Security Officer to identify adequate resources, funding, and address coordination issues to fully support this process. In addition, the vulnerability assessment program is working to ensure any deployment will be compatible with the new controls and Department of Homeland Security architecture.

Recommendation #11 – The above recommendations should be included as part of the DHS C&A program.

This recommendation seems redundant as all of the recommendations #1 through 10 address the Department of Homeland Security Certification and Accreditation program to some degree.

Recommendation #12 – A DHS-wide application change control policy is developed and changes are consistently authorized and tested prior to implementation.

At the present time change control is an Organizational Element responsibility as prescribed in Section 3.7 in the Department of Homeland Security Sensitive Systems Policy and Handbook Publication 4300A and Department of Homeland Security National Security Systems Policy and Handbook Publication 4300B, Version 2.0, dated March 31, 2004. Given the current Information Technology environment with numerous and disparate legacy Information Technology systems, this solution is appropriate for the Department at this time. As the Department of Homeland Security moves to "One Infrastructure," Department of Homeland Security-wide solutions will become more appropriate. As Department of Homeland Security matures change control processes and procedures, change control management will be a focus to ensure consistency.

Recommendation #13 – Policies and procedures are in place for monitoring, use, and changes to operating systems.

The implementation of Department of Homeland Security configuration management policy (Section 3.7) is the responsibility of the Information System Security Officer assigned to a particular system. The Chief Information Security Officer has implemented numerous initiatives recently to help strengthen the implementation of policy at the Information System Security Officer level. These initiatives are addressed in the response to Recommendation #9.

Recommendation #14 – Bureau personnel comply with the established policies and procedures.

Due to the distributed nature of the organization, the Chief Information Security Officer has established the key role of Information Systems Security Manager for each Organizational Element. This role is responsible for ensuring bureau personnel comply with established policies and procedures. In addition, the Chief Information Security

Officer meets with these staff as part of regular Information System Security Board meetings to discuss issues and risks associated with rolling out a comprehensive Information Security Program for Department of Homeland Security. To help support the Information Systems Security Managers and garner management support, the Chief Information Security Officer has begun rolling out a Digital Dashboard and a comprehensive Balanced Scorecard to provide adequate management visibility to the issue of bureau compliance. By prioritizing and focusing attention on key issues, we can build the support and compliance necessary to address the issues identified in the audit report.

In addition, at the system level, the Information System Security Officer is accountable to the Information Systems Security Manager and respective CIO to implement the bureau requirements for compliance at the Organizational Element level. Through the use of Federal Information Security Management Act Reporting, an improved Certification and Accreditation process, on-going training and periodic Chief Information Security Officer level reviews, we are driving the responsibility and consistency necessary to support such a large Departmental need. The lessons learned from this process are then fed back by the Information Systems Security Manager to the Information System Security Board for broader dissemination within the organization.

Recommendation #15 – Responsibilities are documented so that incompatible duties are consistently separated. If this is not feasible given the smaller size of certain functions, then sufficient compensating controls, such as periodic peer reviews, should be implemented.

Separation of duties is addressed in Section 4.1.3 in the Department of Homeland Security Sensitive Systems Policy and Handbook Publication 4300A and Department of Homeland Security National Security Systems Policy and Handbook Publication 4300B, Version 2.0, dated March 31, 2004. Per Department of Homeland Security guidance, separation of duties is assigned to program officials and Information System Security Officers.

Recommendation #16 – Policies and procedures are developed and documented to address segregation of duties for IT and accounting functions.

Separation of duties for Information Technology functions is addressed in the Department of Homeland Security Sensitive Systems Policy and Handbook Publication 4300A and Department of Homeland Security National Security Systems Policy and Handbook Publication 4300B, Version 2.0, dated March 31, 2004.

The CIO will work with the Chief Financial Officer to ensure that specific policies and procedures are development and documented to address the segregation of duties for accounting functions.

Recommendation #17 – DHS systems and applications have complete and current contingency and disaster recovery plans.

Section 4.10 (a) of the Department of Homeland Security Sensitive Systems Policy and Handbook Publication 4300A and Department of Homeland Security National Security Systems Policy and Handbook Publication 4300B, Version 2.0, dated March 31, 2004 states “Organizational Elements shall develop and maintain disaster recovery and continuity of operations plans in the event that normal operations are disrupted**.”**

Because the Chief Information Security Officer recognizes the importance of ensuring that contingency plans and disaster recovery plans are documented and current, the Department of Homeland Security Digital Dashboard includes a Continuity Planning stop light. The continuity planning metric is based on the percentage of systems with business contingency plans and the percentage of business contingency plans that have been tested.

Recommendation #18 – Bureau specific and DHS-wide testing of key service continuity capabilities are performed.

Section 4.10 (c) of the Department of Homeland Security Sensitive Systems Policy and Handbook Publication 4300A and Department of Homeland Security National Security Systems Policy and Handbook Publication 4300B, Version 2.0, dated March 31, 2004 states “Organizational Elements shall test significant portions of their disaster recovery and business continuity plans quarterly. These tests should be planned and conducted so that the entire disaster recovery and business continuity program is evaluated annually.”

Also see second paragraph of the response to Recommendation #17.

Recommendation #19 - A DHS-wide service continuity training program is designed and implemented.

Section 4.10 (b) of the Department of Homeland Security Sensitive Systems Policy and Handbook Publication 4300A and Department of Homeland Security National Security Systems Policy and Handbook Publication 4300B, Version 2.0, dated March 31, 2004 states “All personnel involved with disaster recovery/business continuity planning efforts shall be identified and trained in the procedures and logistics of the disaster recovery and business continuity plans.”

The Continuity Planning Program Director intends to develop and document additional guidance and Continuity of Operations document templates such as the Business Impact Analysis template, etc. These will be provided as part of the Department of Homeland Security Information Security Program Policy and Handbook.

Recommendation #20 – Backup and recovery processes more consistently follow relevant guidance (i.e., OMB Circular A-130).

Section 4.10.4. (a) of the Department of Homeland Security Sensitive Systems Handbook Publication 4300A and Department of Homeland Security National Security Systems Handbook Publication 4300B, Version 2.0, dated March 31, 2004 states “Organizational Elements shall implement and enforce backup procedures for all Sensitive Information Technology systems, data, and information.”

Attachment 1: DHS Information Security Program Enterprise Initiatives

Information Security Program Area	Enterprise Initiative	Content	Availability	Status
Management	Budget Handbook	Described budget process and OE responsibilities	*ISSM Guide to the DHS Information Security Program*	Completed
Management	Earned Value Management Plan	Describes Earned Value Program for DHS Information Security	Available from the CISO	Completed
Management	DHS Information Security Digital Dashboard	Reports aggregate security statistics at the OE and Department Level	https://www.fismamgr.dhs.gov	Under Development
Management	Balanced Scorecard	Reports the status of the DHS Information Security Program from five perspectives: • Customers • Stakeholders • Financial • Growth & Learning • Internal Processes	TBD	Under Development
Security Policy	DHS Policy On-line	Provides current DHS information security policies and standards	DHSOnline Internet CD	Operational
Compliance and Oversight	Trusted Agent FISMA	Web-based tool used to document: • Inventory • Deficiencies • Plans of Actions and Milestones • NIST 800-26 assessments • Security Metrics	Intranet: https://fismamgr.dhs.gov Account required	Operational
Compliance and Oversight	C&A Management Tool	Web-based tool that documents C&A results and manages the C&A work flow	TBD	To be implemented in mid-2004
Compliance and Oversight	Self-Assessment Jump Start	Funds up to 40 OE self-assessments in FY 04.	Compliance and Oversight Program Director	Operational
Training	Security Awareness Training	Provides basic security awareness training for all DHS personnel and contractors with accounts	DHSOnline Internet: https://ww.brainbench.com/xml/dhs/logon.xml?promocode=DHS_Awareness CD	Operational

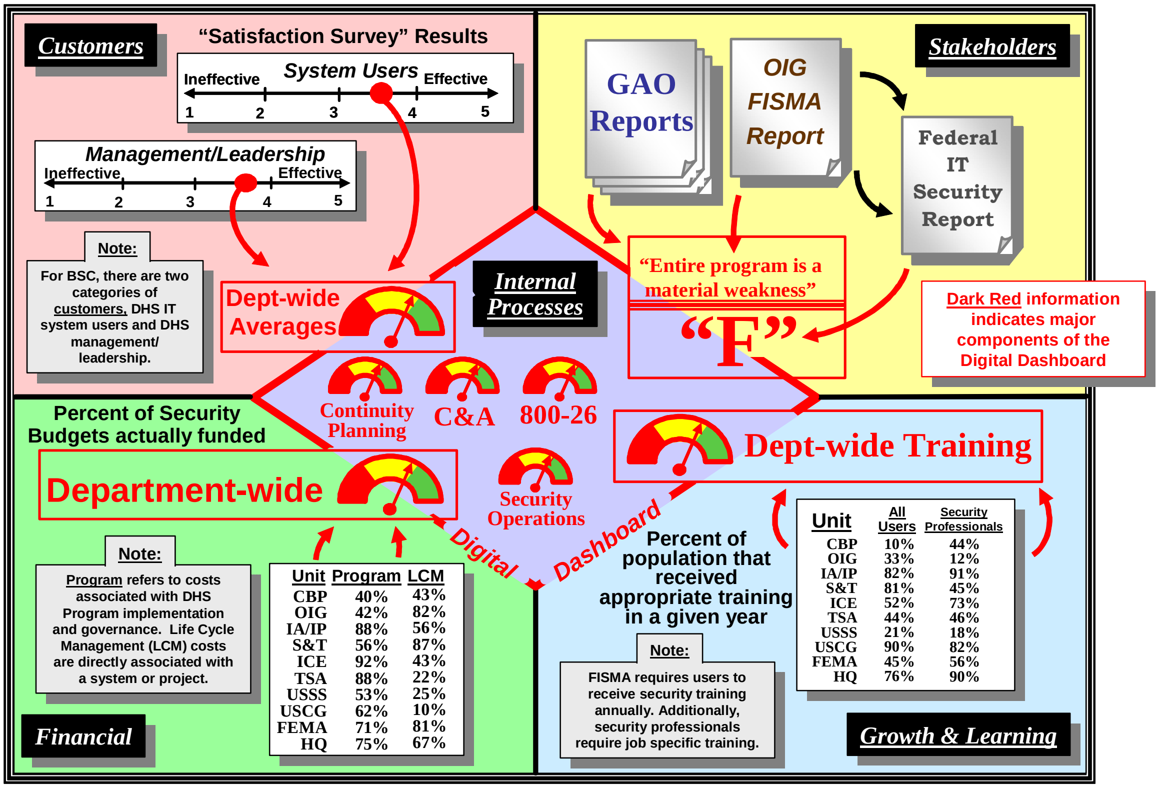
Information Security Program Area	Enterprise Initiative	Content	Availability	Status
Training	DHS Virtual Campus	Provides training for information systems security professionals	Internet or Intranet http://www.dsfirst.com	Operational
Security Architecture	DHS Security Architecture	High level view of how the DHS Security Design Guidance document can be used to support the business line enterprise architecture	Security Architecture Program Director	Under Development
Security Architecture	DHS Security Architecture Design Guidance	Provides specific requirements and best practices for the design and development of the security aspects of DHS systems	Security Architecture Program Director	Under Development
Security Architecture	Technical Reference Model	Identifies the mandated DHS security standards, specifications, and technologies	Security Architecture Program Director	Under Development
Security Architecture	EA Products Catalog	Identifies potential security solutions	Security Architecture Program Director	Under Development
Security Operations	On-Line Incident reporting capability	Provides capability to report security incidents on-line	dhs.csirc@dhs.gov	Operational
Security Operations	Centralized Incident Contact Information	Provides centralized DHS contact for reporting incidents	202-261-9523	Operational
Security Operations	Information Security Vulnerability Management Program	Provides bulletins, alerts, and technical advisories related to emerging vulnerabilities and threats Provides Red Team for OEs without internal capabilities and for independent verification as necessary	Security Operations Program Director	Under Development
Security Operations	Credentialing and Identification Management	PKI and smartcard services for DHS	Security Operations Program Director	Roll out underway
Security Operations	Enterprise Security Software Licenses	Provides enterprise security products The following products are currently under negotiation: • Vulnerability Assessment Tools • Anti-Virus Tools	Security Operations Program Director	Pending

Information Security Program Area	Enterprise Initiative	Content	Availability	Status
Continuity Planning	Project Matrix Step 1	Completes identification and prioritization of DHS nationally critical functions/services and assets	Continuity Planning Program Director	In progress
Continuity Planning	Project Matrix Step 2	Completes value chain and interdependency analysis for DHS nationally critical functions/services and assets	Continuity Planning Program Director	Pending
Continuity Planning	Continuity of Operations (COOP) Guidance	Provides guidance on Business Impact Assessment, and COOP Implementation and COOP Communications Plans	DHS Information Security Program Policy and Handbook	Under Development
Continuity Planning	OE CIP Risk Management Plan	Outlines requirements for CIP risk management plan	Continuity Planning Program Director	Under Development
NSS and COMSEC Management	COMSEC Tracking System	Provides for keymat inventory and account management	TBD	Pending
NSS and COMSEC Management	DHS Secure Phone Directory	A enterprise-wide directory of secure phone and fax numbers	NSS and COMSEC Program Director	Under Development
NSS and COMSEC Management	Secure Telephone Users Guide	Detailed instructions regarding the installation, use, and security of secure desk top and cell phones within DHS	NSS and COMSEC Program Director	Completed
NSS and COMSEC Management	PC and Laptop C&A Templates	Generic C&A documentation for stand alone PCs and laptop computers	NSS and COMSEC Program Director	Completed

Attachment 2. DHS Information Security Program Balanced Scorecard

A Balanced Scorecard is the tool for aligning the Information Security Program strategy to the short-term actions necessary to successfully implement the program and to promote accountability by the Department of Homeland Security Organizational Elements. The scorecard helps the Organizational Elements correlate, through Information Systems Security Manager management and direction, short-term actions and initiatives with performance objective and measures of the overall Information Security Program. In addition, the scorecard provides a common reporting process to facilitate the alignment of the Information Security Program across the Organizational Elements.

The Balanced Scorecard provides a framework for correlating the objectives, measures, and results necessary to move from strategy formulation to execution. The figure below illustrates this relationship framework.



Note:

For BSC, there are two categories of customers, DHS IT system users and DHS management/ leadership.

Note:

Program refers to costs associated with DHS Program implementation and governance. Life Cycle Management (LCM) costs are directly associated with a system or project.

Unit	Program	LCM
CBP	40%	43%
OIG	42%	82%
IA/IP	88%	56%
S&T	56%	87%
ICE	92%	43%
TSA	88%	22%
USSS	53%	25%
USCG	62%	10%
FEMA	71%	81%
HQ	75%	67%

Note:

FISMA requires users to receive security training annually. Additionally, security professionals require job specific training.

Unit	All Users	Security Professionals
CBP	10%	44%
OIG	33%	12%
IA/IP	82%	91%
S&T	81%	45%
ICE	52%	73%
TSA	44%	46%
USSS	21%	18%
USCG	90%	82%
FEMA	45%	56%
HQ	76%	90%

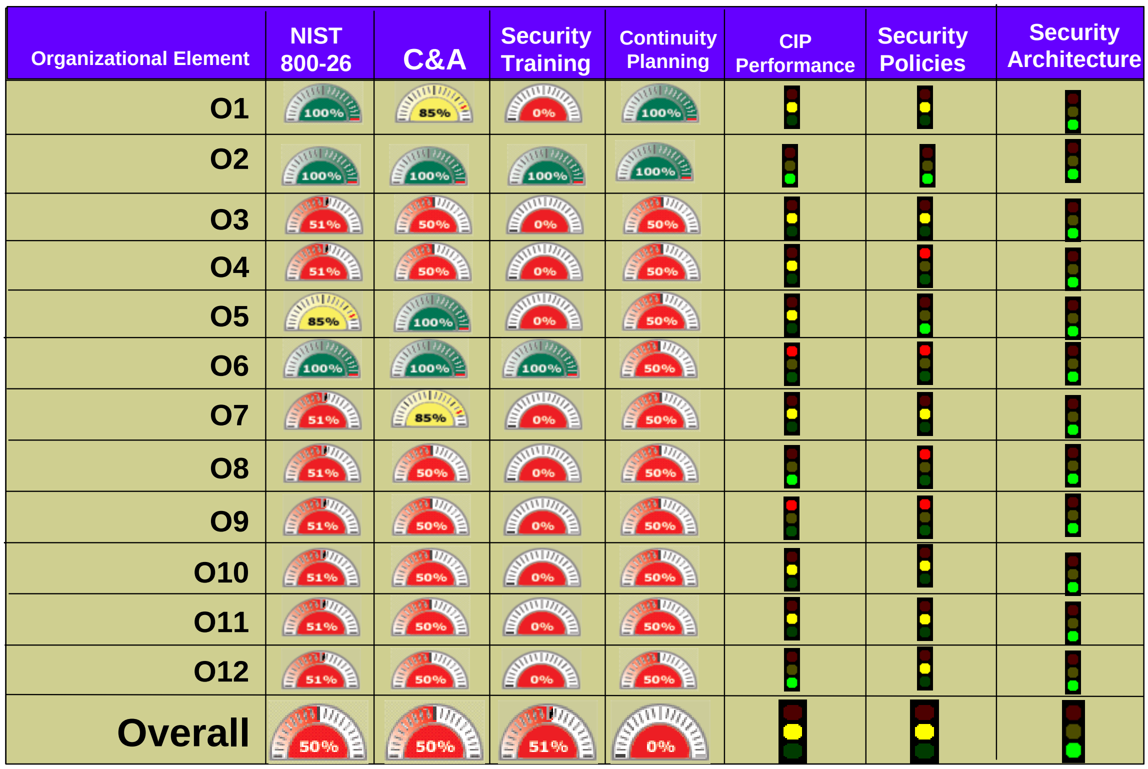
In support of this framework, the Chief Information Security Officer has identified five perspectives for viewing the success of the Department of Homeland Security Information Security Program. These perspectives help establish a balance for the objectives and measures by considering the perspective of the program from multiple directions. The following table describes these five perspectives.

Balanced Scorecard Perspectives

Customers	The customer perspective represents Department of Homeland Security information system users. The customers are the ultimate users of the Information Security Program and must trust in the Department of Homeland Security Information Technology infrastructure to store and use their information in a secure and protected manner. At this time, the customers have been segmented into two groups: System Users and Department Management. This separation has been identified to help identify the confidence at the desktop and program levels.
Stakeholders	The stakeholder perspective represents external perception of the Department of Homeland Security Information Security Program. This perspective attempts to capture the public and oversight drivers associated with the information security program. Some of these stakeholders include: IG, GAO, OMB, and Congress.
Financial	The financial perspective represents the funding associated with the Department of Homeland Security Information Security Program. This perspective attempts to capture funding and alignment with Future Years Homeland Security Program (FYHSP).
Growth & Learning	The growth and learning perspective represents enablers for closing the gap between current operations and future DHS Information Security Program goals. This perspective highlights the objectives and measures necessary to move from the current state to the future state of the program.
Internal Processes	The internal processes perspective represents the areas DHS must excel at in order to drive value for DHS customers. The CISO has embodied these internal processes in the eight key Program Areas, including: • Program Management and Integration • Security Policy • Compliance and Oversight • Information Security Training, Education and Awareness • Security Architecture • Security Operations • Continuity Planning • National Security Systems (NSS) and Communications Security (COMSEC) Management

Attachment 3. DHS Information Security Program Digital Dashboard

The Department of Homeland Security Chief Information Security Officer uses a Digital Dashboard tool for reporting the aggregate data at the Organizational Element and Department Level associated with the Balanced Scorecard approach described above. The Digital Dashboard provides a mechanism for visualizing the progress of the Department of Homeland Security Information Security Program on a progressive schedule. The figure below illustrates the Department of Homeland Security Digital Dashboard.



Organizational Element	NIST 800-26	C&A	Security Training	Continuity Planning	CIP Performance	Security Policies	Security Architecture
O1	100%	85%	0%	100%	🟡	🟡	🟢
O2	100%	100%	100%	100%	🟢	🟢	🟢
O3	51%	50%	0%	50%	🟡	🟡	🟢
O4	51%	50%	0%	50%	🟡	🔴	🟢
O5	85%	100%	0%	50%	🟡	🟢	🟢
O6	100%	100%	100%	50%	🔴	🔴	🟢
O7	51%	85%	0%	50%	🟡	🟡	🟢
O8	51%	50%	0%	50%	🟢	🔴	🟢
O9	51%	50%	0%	50%	🔴	🔴	🟢
O10	51%	50%	0%	50%	🟡	🟡	🟢
O11	51%	50%	0%	50%	🟡	🟡	🟢
O12	51%	50%	0%	50%	🟢	🟡	🟢
Overall	50%	50%	51%	0%	🟡	🟡	🟢

The source of the dashboard metrics is a combination of Organizational Element reported information, output from tools, and audits (both internal and external). The dashboard gauges are based on data provided by the Organizational Elements in Trusted Agent FISMA. This includes, for example, percentage of systems with self-assessments, security training, and other metrics. The dashboard stoplights are subjective ratings based on Organizational Element deliverables and other reporting requirements.

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Chief of Staff
Under Secretary, Management
DHS Chief Financial Officer
DHS OIG Liaison
DHS Public Affairs

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees as Appropriate

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to 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.