

# DEPARTMENT OF HOMELAND SECURITY

## Office of Inspector General

### Information Technology Management Letter for the FY 2004 DHS Financial Statement Audit (Redacted)



Notice: The Department of Homeland Security, Office of Inspector General, has redacted this report for public release. The 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-05-27**

**July 2005**



**KPMG LLP**  
2001 M Street, NW  
Washington, DC 20036

December 15, 2004

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

Ladies and Gentlemen:

We were engaged to audit the consolidated balance sheet of the U.S. Department of Homeland Security (DHS) as of September 30, 2004, and the related consolidated statements of net cost, changes in net position, financing, and custodial activity, and combined statement of budgetary resources (hereinafter referred to as "financial statements"), for the year then ended. Because of matters discussed in our *Independent Auditors' Report*, dated November 8, 2004, the scope of our work was not sufficient to enable us to express, and we did not express, an opinion on the financial statements.

In connection with our fiscal year 2004 engagement, we were also engaged to consider DHS' internal control over financial reporting and to test DHS' compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements that could have a direct and material effect on these financial statements. Our procedures may not include examining the effectiveness of internal controls and do not provide assurance on internal control. We have not considered internal control since the date of our report.

We noted certain matters involving internal control and other operational matters with respect to information technology that are summarized in the Information Technology Management Comments starting on page 1. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies. These comments are in addition to the reportable conditions presented in our *Independent Auditors' Report*, dated November 8, 2004, and included in the FY 2004 DHS *Performance and Accountability Report*. A description of each internal control finding, and its disposition, as either a material weakness or an information technology management comment is provided in Appendix B. We have also included the current status of the prior year Notice of Findings and Recommendations in Appendix C. Our 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 December 15, 2004.

As described above, the scope of our work was not sufficient to express an opinion on the financial statements of DHS as of and for the year ended September 30, 2004, and accordingly, other matters involving internal control over information technology may have been identified and reported had we been able to perform all procedures necessary to express an opinion. We aim, however, to use our knowledge of DHS' organization gained during our work to make comments and suggestions that we hope will be useful to you.

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**  
*Information Technology Management Comments*  
 September 30, 2004

<b>INFORMATION TECHNOLOGY MANAGEMENT COMMENTS</b>		
<b>Section/ FISCAM General Control Area</b>		
<b>Comment Reference</b>	<b>Subject</b>	<b>Page</b>
<b>Information Technology Objective, Scope and Approach</b>		<b>1</b>
<b>Summary of Findings and Recommendations</b>		<b>2</b>
<b>Findings by Audit Area</b>		<b>2</b>
<b>Entity-Wide Security Program Planning and Management</b>		<b>2</b>
EWS-4-01	Certification and accreditation, system inventories, reviews of controls	<b>3</b>
EWS-4-02	Security training and awareness	<b>3</b>
EWS-4-03	Security plans	<b>3</b>
EWS-4-04	Security risk assessments	<b>3</b>
<b>Access Controls</b>		<b>3</b>
AC-4-01	Passwords, user account management, excessive access privileges	<b>4</b>
AC-4-02	Configuration of workstations and user accounts	<b>4</b>
<b>System Software</b>		<b>4</b>
SS-4-01	Restricting and monitoring access to operating system software	<b>4</b>
SS-4-02	Documentation of operating system setting changes	<b>4</b>
<b>Segregation of Duties</b>		<b>5</b>
SD-4-01	Incompatible functions	<b>5</b>
SD-4-01	Position description documentation	<b>5</b>
<b>Service Continuity</b>		<b>5</b>
SC-4-01	Business continuity / disaster plans	<b>5</b>
SC-4-02	Testing of service continuity plans and training of professionals	<b>6</b>
<b>Application Software Development and Change Controls</b>		<b>6</b>
ASDCC-4-01	Software changes need to be better documented	<b>6</b>
<b>Application Controls</b>		<b>6</b>
APC-4-01	Outdated application user guide of a key financial system.	<b>6</b>
APC-4-02	Not consistently performing verification of data input and output, including the reconciliation of data between applications	<b>6</b>

<b>APPENDICES</b>		
<b>Appendix</b>	<b>Subject</b>	<b>Page</b>
<b>A</b>	Description of Financial Systems and IT Infrastructure within the Scope of the FY 2004 DHS Financial Statement Audit	<b>7</b>
<b>B</b>	FY 2004 Detail Notice of IT Findings and Recommendations by DHS Organizational Element	<b>13</b>
<b>C</b>	Cross-Walk – Status of Prior Year Notice of Findings and Recommendations to Current Year Notice of Findings and Recommendations	<b>37</b>
<b>D</b>	Management Response to Draft IT Management Letter	<b>43</b>

## **INFORMATION TECHNOLOGY OBJECTIVE, SCOPE AND APPROACH**

KPMG performed a review of DHS IT general controls in support of the FY 2004 DHS financial statement engagement. 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 engagement. 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 as described in Appendix A.

FISCAM is designed to inform financial auditors about IT controls and related audit concerns to assist them in planning their audit work and to integrate the work of auditors with other aspects of the financial audit. 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.
- *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.
- *Application software development and change control (ASDCC)* – Controls that help to prevent the implementation of unauthorized programs or modifications to existing programs.
- *Application Controls (APC)* - Application controls are the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, payroll, grants, or loans.

To complement our general IT controls review, we also performed technical security testing for key network and system devices, as well as testing over key financial application controls. The 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. The application control testing was performed to assess the controls that support the financial system's internal controls over the input, processing, and output of financial data and transactions.

A draft version of this IT Management Letter was provided to the DHS Chief Information Officer, who generally agreed with the comments and recommendations and his response is included as Appendix D of this document.

## **SUMMARY OF FINDINGS AND RECOMMENDATIONS**

During FY 2004 DHS took corrective action to address many prior year IT control weaknesses. However, also during FY 2004, we continued to find IT general control weaknesses at each Bureau. The most significant weaknesses from a financial statement audit perspective relate to information security (entity-wide security, access controls, and systems software). Collectively, the IT control 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 weaknesses under standards established by the AICPA.

Although we noted improvement, many of the conditions identified in FY 2003 have not been corrected because DHS still faces challenges related to the merging of numerous entities that have had their own IT functions, controls, processes, and overall organizational shortages. During FY 2004 DHS took steps to help address these conditions, such as restructuring DHS' Chief Information Officer's role and function, improving its IT security program by completing DHS-wide training and awareness sessions, continued having bi-weekly Information Systems Security Board (ISSB) meetings, and awarding a contract for the Electronically Managing Enterprise Resources for Government Efficiency and Effectiveness (EMERGE2) program, which will help consolidate IT functions across DHS. In addition, during FY 2004, DHS implemented additional policies and procedures related to IT controls. For example, DHS updated its *Department of Homeland Security Sensitive Systems Handbook Publication*, which is intended to provide DHS organizational element CIOs, Information Systems Security Managers (ISSMs) and Information Systems Security Officers (ISSOs) with the necessary guidance to develop specific policies and procedures for their individual application systems.

Despite these improvements, DHS needs further emphasis on the monitoring and enforcement of the policies and procedures through the performance of periodic security control assessments and audits. Further improvements are needed on implementing and enforcing a DHS-wide security certification and accreditation (C&A) program, and technical security control training for system administrators and security officers. Many of the technical issues identified during our review, which were also identified during FY 2003, such as weak system access controls and the lack of contingency planning strategies, can be addressed through a more effective security C&A program and security training program.

### **FINDINGS BY AUDIT AREA**

#### **Entity-Wide Security Program Planning and Management**

During FY 2004 DHS improved its level of entity-wide security program planning and management. For example, DHS implemented an enterprise-wide security C&A tool that provides 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, as noted earlier, DHS-wide security training and awareness efforts were made. However, continued efforts are needed, especially in the areas of program management related to the detection and monitoring of technical information security weaknesses. Collectively, the identified entity-wide security planning and management issues, coupled with the access control issues described later in this management

**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

comment letter, reduce the overall effectiveness of the entity-wide security programs for the individual DHS Bureaus, and the overall Department.

Conditions noted in FY 2004 regarding entity-wide security program planning and management at DHS and its Bureaus were:

- EWS-4-01 – Despite the implementation of a security C&A tool, security C&A efforts were still not completely implemented in such a manner to ensure the detection and prevention of technical security weaknesses.
- EWS-4-02 – Security training and awareness programs, especially those related to the detection and prevention of technical weaknesses, can be improved.
- EWS-4-03 – Security plans 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* (e.g. Did not consistently document existing system security controls)
- EWS-4-04 – 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 CFO and other DHS functional leaders, continue efforts to fully implement a security program to ensure that:

- a. Implementation and enforcement of the C&A program continues;
- b. A DHS-wide security training and awareness program is designed and implemented consistent with OMB and NIST guidance. A key focus of the training program should be on the detection and prevention of technical weaknesses identified earlier in this management letter;
- c. Information security planning efforts follow applicable Federal guidance (OMB and NIST);
- d. Security risk assessments are completed in a consistent manner per OMB and NIST guidance; and
- e. The above recommended entity-wide security efforts are implemented in a timely and consistent manner throughout the agency.

**Access Controls**

During FY 2004 we noted significant access control vulnerabilities with internal IT devices (i.e., inside the Bureaus' firewalls). These are significant issues because personnel inside the organization who best understand the organization's systems, applications, and business processes are able to make unauthorized access to some systems and applications. Some of the identified vulnerable devices are used for test and development purposes. In some cases, users are 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 to obtain information (i.e., user password listings) that can be used to attempt further access into DHS' IT environment.

**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

Conditions noted in FY 2004 regarding access controls at DHS and its Bureaus were:

- AC-4-01 – Instances of missing user passwords on key servers and databases, weak user passwords, and weaknesses in user account management. 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-4-02 – 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 and other DHS functional leaders:

- a. Ensure that password controls meet DHS password requirements and are enforced on all systems;
- b. Implement a password account management process within the Bureaus to ensure the periodic review of user accounts;
- c. Design and implement a DHS-wide patch and security configuration process;
- d. Implement a vulnerability assessment process, whereby systems are periodically reviewed for security weaknesses; and
- e. Include the output of these recommendations in the DHS C&A program.

## **System Software**

We noted weaknesses in programs designed to operate and control the processing activities of computer equipment. Weaknesses in this control area, closely linked to entity-wide security and access controls, 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 noted regarding system software at DHS and its Bureaus were:

- SS-4-01 – 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-4-02 – Changes to sensitive operating system settings were not always documented.

**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

*Recommendation:* We recommend that the DHS CIO, in coordination with the OCFO and other DHS functional leaders, ensure that Bureau personnel comply with the established policies and procedures for monitoring, use, and changes related to operating systems.

### **Segregation of Duties**

During FY 2004, we continued to note 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, without detection. Additionally, we noted a lack of segregation of duties between major operating and programming activities, including duties performed by users, application programmers, and data center staff.

Conditions noted regarding segregation of duties at DHS and its Bureaus were:

- SD-4-01 – Instances where individuals were able to perform incompatible functions, such as the changing, testing, and implementing software, without sufficient compensating controls in place.
- SD-4-02 – 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 and other DHS functional leaders, ensure that:

- a. Policies and procedures are developed and implemented to address segregation of duties for IT and accounting functions; and
- b. 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.

### **Service Continuity**

During FY 2004 we noted that DHS took some corrective actions to address IT control issues related to the back-up and protection of critical system data. In addition, the DHS OCIO implemented the use of a 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. Despite these improvements, weaknesses related to disaster recovery plans and business continuity plans continue to exist. These issues are important because losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission.

Conditions noted regarding service continuity at DHS and its Bureaus were:

- SC-4-01 – 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.



**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

- SC-4-02 – 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 and other DHS functional leaders:

- a. Develop and implement complete business continuity plans and system disaster recovery plans;
- b. Perform bureau specific and DHS-wide testing of key service continuity capabilities; and
- c. Design and Implement a DHS-wide service continuity training program..

### **Application Software Development and Change Control**

During FY 2004 we noted that DHS took corrective actions to address IT control issues related the application software changes. However, we noted that in some cases the application software change control documentation was still not consistent with Bureau systems development life cycle (SDLC) guidance.

- ASDCC-4-01 – Software changes need to be documented in a more consistent manner.

*Recommendation:*

- a. We recommend that the DHS CIO, in coordination with the OCFO and other DHS functional leaders, ensure that Bureaus improve documentation software changes to ensure compliance with Bureau SDLC guidance.

### **Application Controls**

During FY 2004, we noted instances where application policies and procedures were not kept current, and incomplete verification of data input and output, including the reconciliation between applications was not consistently being performed. These issues are important because securing the capability to input, process, reconcile, and retrieve information maintained electronically can significantly affect an agency's ability to accomplish its mission.

Conditions noted regarding application controls at DHS and its Bureaus were:

- APC-4-01 – One bureau utilized an outdated application user guide of a key financial system.
- APC-4-02 – Several bureaus' were not consistently performing verification of data input and output, including the reconciliation of data between applications

*Recommendations:*

We recommend that the DHS CIO, in coordination with the OCFO and other DHS functional leaders, ensure that:

- a. Bureaus keep input, processing and output control policy and procedures current; and
- b. Perform regular period verification of data input and output, including the reconciliation between applications.

**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

**Appendix A - Description of Financial Systems and IT  
Infrastructure within the Scope of the FY 2004 DHS Financial  
Statement Audit**

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

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 twelve months ended September 30, 2004.

***United State Citizen and Immigration Services (USCIS)/Immigration and Customs Enforcement (ICE)***

Locations of Review: USCIS/ICE Headquarters in Washington, D.C., as well as offices in Texas, California, Vermont, and Nebraska.

Systems Subject to Review:

- *Federal Financial Management System (FFMS)* – FFMS supports all USCIS/ICE core financial processing. FFMS runs on an Oracle database. FFMS uses a Standard General Ledger (SGL) for the accounting of agency financial transactions.
- *Claims 3* – Claims 3 is a database used to track pending applications, and is accessible by the various USCIS service centers. Claims 3 contains totals of pending immigration applications (by application type). 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.

***United States Coast Guard***

Locations of Review: Coast Guard Headquarters in Washington, DC; 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)* – CGOF is the core accounting system that records financial transactions and generates financial statements for the Coast Guard. 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. Also housed at OSC is the Fleet Logistics System (FLS), a web-based application designed to automate the management of CG vessel logistics by supporting the following functions: configuration, maintenance, supply and finance. In addition, OSC is responsible for CMPlus, the central repository for activities associated with maintaining Coast Guard assets at the unit level.
- *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

**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

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. These applications include the Personnel Management Information System (PMIS) and the Joint Uniform Military Pay System (JUMPS). Also housed at PSC is the PeopleSoft 8.3 Direct Access application, which is used by members for self-service functions, including updating and viewing personal information.

In addition, the Coast Guard maintains hosts on the Internet in thirteen Internet Protocol (IP) address ranges. Hosts within these ranges support various Web based applications, e-mail servers, and File Transfer Protocol (FTP) servers.

***United States Customs and Border Protection (CBP)***

Locations of Review: The CBP National Finance Center (NFC) in Indianapolis, Indiana and the National Data Center (NDC) in Newington, Virginia.

Systems Subject to Review:

- *Asset Information Management System (AIMS)* – AIMS is CBP's IBM mainframe-based 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 is hosted on a customized version of American Management Systems' software – Federal Financial System (FFS).
- *Automated Commercial System (ACS)* – ACS is a collection of mainframe-based 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.
- *SAP R/3* – SAP is a client/server-based financial management system that was implemented during FY 2004 to ultimately replace the AIMS mainframe-based financial system (FFS) using a phased approach. The SAP Materials Management module was implemented and utilized in FY 2004. Other SAP modules are to be implemented in FY 2005.

CBP also maintains personnel, payroll, and scheduling systems.

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

DHS Consolidated

Location of Review: 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 Windows NT server, Oracle 8i database, and the TIER and CFO Visions applications. 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 (EPR)***

Locations of Review: Federal Emergency Management Agency (FEMA) Headquarters in Washington, D.C., and the 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 support all phases of emergency management, and provides financial related data to IFMIS via an automated interface.

***Limited Scope***

Locations of Review: We performed follow-up on a FY 2003 finding at the Federal Law Enforcement Training Center (FLETC) Headquarters in Glynco, Georgia.

Systems Subject to Review:

The Momentum Financial System is FLETC's core computerized system that processes financial documents generated by various FLETC divisions in support of procurement, payroll, budget and accounting activities.

**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

***Office of State and Local Government Coordination and Preparedness (SLGCP, formerly the Office for Domestic Preparedness)***

Location of Review: SLGCP Headquarters in Washington, D.C.

Systems Subject to Review:

SLGCP'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 SLGCP.

- *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 SLGCP 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 SLGCP 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 SLGCP/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 SLGCP 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 draw down 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 (PAPRS)* – 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 draw down transaction information from PAPRS 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.
- *SF 269 Web Based System* – The web based system enables authorized users to view grant information, view previously submitted SF269's, and submit quarterly SF269's online. SF 269 web-based system is interfaced to the PAPRS and LOCES payment system.

SLGCP currently provides state and local agencies with grant funding services to acquire specialized response equipment, emergency responder training and technical assistance, and support to plan and

**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

conduct exercises tailored to the circumstances of the jurisdiction. Starting July 2004, SLGCP who currently relied on OJP for their network and IT platform support of applications; will begin to migrate all support over to the Department of Homeland Security. The plan for the transfer of all SLGCP functions to DHS will not be fully completed until January 2005. Currently the only SLGCP application that is supported fully by DHS is the Data Collection Toolkit. This application was previously hosted through OJP; now a third party contractor is hosting the application in Dallas, Texas.

***Transportation Security Administration (TSA)***

Locations of Review: TSA Headquarters in Washington, D.C. and the 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, calculates pay, wages, tax information and maintains service history and separation records. CUPS interfaces with the Integrated Personnel and Payroll System (IPPS), Little IPPS, CUPS National, CPMIS, DELPHI, and also receives other data inputs. CUPS is a mainframe application.
- *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 is a mainframe application. 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.
- *Integrated Personnel And Payroll System (IPPS)* – IPPS processes requests for personnel action, training enrollments, and time and attendance information. IPPS interfaces with CPMIS and CUPS to receive time and attendance and payroll information. IPPS also interfaces with the IPPS Management and Reporting (MIR) system. MIR is a client/server system that provides reporting capability through an Oracle database.
- *Delphi* – Delphi is the TSA core financial management system, which provides accounts payable, accounts receivable, general ledger, and budgeting functionality. Delphi is Oracle based and is a commercial off-the-shelf (COTS) software package that is certified to meet government accounting needs.

**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

**Appendix B – FY 2004 Notice of IT Findings and Recommendations  
- Detail by DHS Organizational Element**



**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

**Department of Homeland Security**  
**FY2004 Information Technology**  
**Notification of Findings and Recommendations – Detail**

- **Citizenship and Immigration Services**
- **Immigration and Customs Enforcement**

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

**Department of Homeland Security**  
**FY2004 Information Technology**  
**Notification of Findings and Recommendations – Detail**

**Citizenship and Immigration Services / Immigration and Customs Enforcement**

NFR #	Condition	Recommendation	Disposition Material Weakness (MW) or Management Comment (MC)
CIS-4-09	(b)(2) High [Redacted]	[Redacted]	MW
CIS-4-10	[Redacted]	[Redacted]	MW
CIS-4-19	[Redacted]	[Redacted]	MW
CIS-4-21	[Redacted]	[Redacted]	MC
CIS-4-27	The site C&A package for the California Service Center has expired.	ensure critical systems are accredited every three years or consider issuing an interim accreditation.	MW
ICE-4-17	Access control weaknesses were identified in the Federal Financial Management System.	Implement stronger password management requirements, regularly review access logon attempts, and educate users on password best practices.	MW
CIS/ ICE 4-18	CIS/ICE does not have procedures in place to periodically review System Time and Attendance Report (STAR) user access lists and could not provide a list of all authorized STAR users upon request.	Document and implement policies and procedures to perform a periodic review of STAR user accounts.	MW

**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

**Department of Homeland Security**  
**FY2004 Information Technology**  
**Notification of Findings and Recommendations – Detail**

- **Customs and Border Protection**

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

**Department of Homeland Security**  
**FY2004 Information Technology**  
**Notification of Findings and Recommendations - Detail**  
**Customs and Border Protection**

NFR #	Condition	Recommendation	Disposition - Material Weakness (MW) or Management Comment (MC)
CBP-4-01	(b)(2)High, (b)  (b)(2)High, (b)		MW
CBP-4-02			MW
CBP-4-03			MW
CBP-4-04			MW

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

NFR #	Condition	Recommendation	Disposition - Material Weakness (MW) or Management Comment (MC)
CBP-4-05	(b) (2) High [Redacted]	[Redacted]	MW
CBP-4-06	[Redacted]	[Redacted]	MW
CBP-4-07	Weaknesses in the C&A process at field sites.	all field sites, continue to develop a formal site selection plan that prioritizes sites by criticality, and resolve common issues in the corrective action plan.	MW
CBP-4-08	Improvements are needed in system logical access controls over network assets affecting headquarters and the National Data Center.	Coordinate with DHS in developing enterprise-wide solutions for improving network and host-based system logical access controls.	MW
CBP-4-09	Interconnection Security Agreements (ISA) are not documented for 92 partners that connect with ACS.	Complete efforts to identify all trading partners where ISAs have not been formally documented and approved, and complete ISAs for identified (b) (2) High	MW
CBP-4-10	(b) (2) High [Redacted]	[Redacted]	MC
CBP-4-11	Weaknesses with the SAP R/3 Release 2 Risk Assessment.	Update the SAP R/3 Release 2 Risk Assessment as appropriate.	MC
CBP-4-12	Improvements needed in restricting access to sensitive system level transactions through the On-Line Transaction Processing System Security (CICS).	Remove unnecessary privileges, base access on the principles of least privilege, and consider use of a temporary account for privileges infrequently required by users.	MW
CBP-4-13	SAP R/3 Release 2 segregation of duties issues were identified with several users.	Take action to mitigate the segregation of duties violations identified or accept the risk of the issue, in which case additional documentation is required.	MW

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

NFR #	Condition	Recommendation	Disposition - Material Weakness (MW) or Management Comment (MC)
CBP-4-14	The incident handling and response capability needs improvement regarding incident detection and initiation, response, recovery, and closure.	Implement access controls over incident response tickets, develop a risk-based approach to responding to incidents, ensure workstation compliance, and develop a standard real-time automated reporting process.	MC
CBP-4-15	Audit logs are not appropriately monitored for the SAP R/3 Release 2.	Train all personnel responsible for reviewing audit logs on specific requirements for the task.	MW
CBP-4-16	Weaknesses in the access control process for the SAP R/3 Release 2 Materials Management.	Consistently document authorizations to SAP for all users.	MW
CBP-4-17	System access, user account management, and configuration weaknesses identified with the SAP general controls environment for materials management module.	Implement policies and procedures to address the access control and configuration weaknesses identified.	MW
CBP-4-18	Least privilege principles are not appropriately enforced for mainframe user groups' access to sensitive datasets/utilities.	Remove unnecessary privileges, base access on the principles of least privilege, and consider use of a temporary account for privileges infrequently required by users.	MW

**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

**Department of Homeland Security**  
**FY2004 Information Technology**  
**Notification of Findings and Recommendations – Detail**

- **United States Coast Guard**

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

**Department of Homeland Security**  
**FY2004 Information Technology**  
**Notification of Findings and Recommendations - Detail**  
**United States Coast Guard**

NFR #	Condition	Recommendation	Disposition Material Weakness (MW) or Management Comment (MC)
CG-4-01	(b) (2) High [Redacted]	[Redacted]	MW
CG-4-02	The Finance and Procurement Desktop (FPD) User Guide is outdated.	Review and update the FPD User Guide and develop a policy to ensure that application documentation is reviewed and updated regularly or when changes occur.	MC
CG-4-03	Comprehensive policies for conducting personnel suitability investigations or records to support the results of personnel suitability investigations do not exist.	Determine DHS status on publishing a policy on background checks and suitability requirements and, subsequent to this policy, document, and enforce procedures to ensure compliance (b) (2) High	MC
CG-4-04	(b) (2) High [Redacted]	[Redacted]	MW
CG-4-05	procedures to restrict access to the UNIX operating system and for monitoring access. No periodic reviews to determine if current monitoring is functioning as intended.	Develop policies and procedures to address access and monitoring in the UNIX operating system environment and periodically test the effectiveness of current monitoring procedures.	MW



**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

NFR #	Condition	Recommendation	Disposition Material Weakness (MW) or Management Comment (MC)
CG-4-06	Weaknesses associated with the UNIX system software change control process.	Develop change control policies and procedures and retain all risk assessment and testing documentation to provide an audit trail for changes.	MW
CG-4-07	(b) (7) High [Redacted]	[Redacted]	MW
CG-4-08	[Redacted]	[Redacted]	MW
CG-4-09	[Redacted]	[Redacted]	MW
CG-4-10	The security plans for the Naval Electronics Supply Support System (NESSS) and FLS are not in compliance with criteria.	Complete the security plans in compliance with criteria.	MW
CG-4-11	(b) (7) High [Redacted]	[Redacted]	MW
CG-4-12	The Operations Service Center (OSC) has not implemented a disaster recovery plan.	Complete the OSC disaster recovery plan to include Coast Guard-wide disaster recovery planning.	MW
CG-4-13	Entity wide security program planning is not in place for the Personnel Service Center (PSC).	Implement policies and procedures and complete documentation as necessary to develop entity wide security program planning for the PSC.	MC

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

NFR #	Condition	Recommendation	Disposition Material Weakness (MW) or Management Comment (MC)
CG-4-14	Weaknesses exist regarding PSC service continuity and resource classifications.	Complete a PSC Business Recovery Plan (BRP) including all necessary components, and move the computer room to a more environmentally controlled environment.	MW
CG-4-15	Weaknesses were identified at PSC relating to weak password settings, lack of monitoring of access lists or changes to security profiles, and lack of policies for monitoring operating system software.	Evaluate and ensure password compliance, implement account/access maintenance and monitoring procedures, and implement monitoring of operating system software.	MW
CG-4-16	Documented procedures do not exist at PSC to enforce segregation of duties principles.	Determine the sensitivity of positions supporting critical IT systems and applications and implement segregation of duties or background screening to mitigate the risks created by (b) (2) High	MW
CG-4-17	(b) (2) High [Redacted]	[Redacted]	MW
CG-4-18	[Redacted]	[Redacted]	MW
CG-4-19	[Redacted]	[Redacted]	MW
CG-4-20	[Redacted]	[Redacted]	MW
CG-4-21	[Redacted]	[Redacted]	MW
CG-4-22	[Redacted]	[Redacted]	MW

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

NFR #	Condition	Recommendation	Disposition Material Weakness (MW) or Management Comment (MC)
CG-4-23	(b)(7)(F) High [Redacted]	[Redacted]	MW
CG-4-24	Implementation and management oversight of Coast Guard's information security program remains fragmented.	Continue developing the implementation and management oversight functions and responsibilities for the Coast Guard information security program.	MC
CG-4-25	Interface controls do not ensure that record counts match as data is transferred from CGOF into CheckFree.	Modify CheckFree code to include null values to maintain data integrity. Until system controls are implemented, develop manual compensating controls.	MC
CG-4-26	Three of the four Database Administrators at FINCEN also have System Administrator rights and responsibilities.	Separate the critical roles of Database Administrator and System Administrator.	MW

**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

**Department of Homeland Security**  
**FY2004 Information Technology**  
**Notification of Findings and Recommendations - Detail**

- **Emergency Preparedness and Response**

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

**Department of Homeland Security**  
**FY2004 Information Technology**  
**Notification of Findings and Recommendations - Detail**

**Emergency Preparedness and Response**

NFR #	Condition	Recommendation	Disposition Material Weakness (MW) or Management Comment (MC)
EPR-4-11	Policies and procedures do not exist to perform period review of IFMIS user access lists.	Develop and implement policies and procedures regarding review of IFMIS user access lists.	MW
EPR-4-16	(b) (2) High		MW
EPR-4-17			MC
EPR-4-18	processes for ensuring that all general support system and application access, including NEMIS, is timely removed for terminated employees.	Periodically review user accounts and update termination policies and procedures to ensure compliance with criteria.	MW
EPR-4-19	Seven critical systems do not have a certification and accreditation (C&A).	Allocate sufficient resources towards completing C&As and continue to meet the timelines established in the FEMA Remediation Plan.	MW
EPR-4-20	No documented process for generating or communicating new or reset IFMIS passwords to users.	Document and implement a process for communicating passwords to users and update the Instruction 2200.7 as appropriate.	MW
EPR-4-21	IFMIS Table audit trail data is not reviewed periodically.	Perform and document review of critical IFMIS Table audit trail data.	MW
EPR-4-22	Insufficient documentation exists to fully explain IFMIS functions and user access capabilities (b) (2) High	Strengthen system documentation supporting the description of IFMIS user functions and their associated	MC
EPR-4-23	(b) (2) High		MW

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

NFR #	Condition	Recommendation	Disposition Material Weakness (MW) or Management Comment (MC)
EPR-4-24	(b)(7)(E) High [Redacted]	[Redacted]	MW
EPR-4-25	[Redacted]	[Redacted]	MW
EPR-4-28	and Collection System (IPAC provides for interagency billings and payments for supplies and services. Of five IPAC User Request Forms selected for testing, we noted one form on which the employee's access was not specifically indicated.	We recommend that EPR ensure that there is a clear indication of the level of IPAC access requested for any EPR employees granted access to IPAC.	MC
EPR-4-32	The Continuity of Operations Plans (COOP) for IFMIS and NEMIS are in draft.	Finalize and obtain management approval of the COOP plans and then periodically test the plans.	MW
EPR-4-35	Mt. Weather has not documented interagency agreements for alternate data processing and telecommunication facilities in the event of a disaster.	Establish interagency agreements for alternate data processing and telecommunication facilities in the event of a disaster and include agreement in the COOP once it is implemented.	MC
EPR-4-39	FEMA has not prioritized its critical data and operations, emergency processing priorities and procedures have not been documented, and all resources supporting critical operations have not been identified.	Identify and document all resources supporting critical operations, develop priorities of systems, data and operations to be recovered in the event of a disaster, and document information in the Project Step Matrix 1 Report.	MW

**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

**Department of Homeland Security**  
**FY2004 Information Technology**  
**Notification of Findings and Recommendation – Detail**

- **Limited Scope – Federal Law Enforcement Training Center**

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

**Department of Homeland Security**  
**FY2004 Information Technology**  
**Notification of Findings and Recommendations -Detail**  
**Limited Scope – Federal Law Enforcement Training Center**

<b>NFR #</b>	<b>Condition</b>	<b>Recommendation</b>	<b>Disposition Material Weakness (MW) or Management Comment (MC)</b>
LTD-4-01	Incident response policies and procedures are not in place and/or finalized for the FLETC Momentum Financial System (MFS).	Develop, finalize, and maintain incident response capabilities in accordance with criteria.	MC



**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

**Department of Homeland Security**  
**FY2004 Information Technology**  
**Notification of Findings and Recommendations – Detail**

- **Consolidated**

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

**Department of Homeland Security**  
**FY2004 Information Technology**  
**Notification of Findings and Recommendations - Detail**  
**Consolidated**

<b>NFR #</b>	<b>Condition</b>	<b>Recommendation</b>	<b>Disposition Material Weakness (MW) or Management Comment (MC)</b>
CONS-4-01	Excessive Treasury Information Executive Repository (TIER) system privileges were granted and a documented process does not exist to notify TIER application administrators of user termination or transfer for timely removal of system access.	Reevaluate TIER user privileges and restrict user account privileges to the minimum necessary to perform job duties, and document a process to timely notify TIER administrators of user termination or transfer.	<b>MC</b>
CONS-4-02	The interagency agreement between DHS and Treasury regarding use of TIER and the related reporting tool (CFO Vision) does not describe the information security controls that need to be implemented and managed by the data owner (DHS) or the system operator (Treasury).	Ensure that the interagency agreement for TIER and CFO Vision clearly specify the information security controls to be maintained by Treasury, consistent with criteria.	<b>MC</b>
CONS-4-03	Lack of compliance with FISMA in the areas of access controls, entity-wide security program planning and management, system software, segregation of duties, and service continuity.	Ensure timely submission of FISMA reports to OMB and implement stronger controls in all identified areas.	<b>MW</b>

**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

**Department of Homeland Security**  
**FY2004 Information Technology**  
**Notification of Findings and Recommendations - Detail**

- **Office of State and Local Government Coordination and Preparedness (SLGCP, formerly the Office for Domestic Preparedness)**

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

**Department of Homeland Security**  
**FY2004 Information Technology**  
**Notification of Findings and Recommendations - Detail**  
**Office of State and Local Government Coordination and Preparedness (SLGCP, formerly**  
**the Office for Domestic Preparedness)**

NFR #	Condition	Recommendation	Disposition Material Weakness (MW) or Management Comment (MC)
SLGCP-4-05	A system owner and security manager has not been identified to track background investigations and personnel clearances.	Assign the appropriate personnel to the system owner and security manager positions.	MC
SLGCP-4-06	A Service Level Agreement (SLA) is not in place with the third party hosting the Data Collection Toolkit (DCT).	Document, approve, and maintain an SLA with the third party hosting the DCT.	MC
SLGCP-4-07	A documented security awareness training program is not in place.	Develop and implement policies and procedures relating to IT security awareness training and ensure that IT personnel receive the proper training to perform job duties.	MC
SLGCP-4-08	Segregation of duties is not properly enforced and documented policies outlining segregation of duties controls or procedures do not exist.	Document segregation of duties policies and procedures for SLGCP information system functions and create and information systems department responsible for security and network administration of SLGCP (b) (2) High	MW
SLGCP-4-09	(b) (2) High [Redacted]	[Redacted]	MW
SLGCP-4-10	Application user accounts are not removed in a timely manner after user separation.	methods for improving the process to notify the security officer that an SLGCP employee or contractor has been transferred or has terminated employment and longer requires system access.	MW
SLGCP-4-22	A C&A does not exist for the SF 269 web based system.	Allocate sufficient funds to complete the necessary documentation and perform a C&A on the SF 269 web based system.	MW

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

NFR #	Condition	Recommendation	Disposition Material Weakness (MW) or Management Comment (MC)
SLGCP-4-25	The reconciliation process for financial transactions that occurred between IFMIS and the SF 269 web based system was not fully implemented throughout the fiscal year.	Develop a process to monitor, record, and track the financial transactions that occur between IFMIS and the SF 269 web based system.	MC
SLGCP-4-26	The SF 269 web based system captured transactions but did not capture user activity for three months of the fiscal year.	Develop a policy to explain in detail the methods for audit logging and monitoring, maintain clear records of system audit logs, and document, investigate, and close any questionable events.	MW

**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

**Department of Homeland Security**  
**FY2004 Information Technology**  
**Notification of Findings and Recommendations – Detail**

- **Transportation Security Administration**

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

**Department of Homeland Security**  
**FY2004 Information Technology**  
**Notification of Findings and Recommendations - Detail**  
**Transportation Security Administration**

<b>NFR #</b>	<b>Condition</b>	<b>Recommendation</b>	<b>Disposition Material Weakness (MW) or Management Comment (MC)</b>
TSA-4-01	Segregation of duties is not properly enforced in the Delphi Application within FFMS.	Implement controls to restrict access based on the principles of least privilege.	<b>MW</b>
TSA-4-02	Weaknesses in Delphi access controls, network security, and system security controls.	Ensure that system controls will be appropriately implemented in the version of FFMS to which TSA will be migrating.	<b>MW</b>
TSA-4-03	System financial integrity issues identified in the Delphi application.	Continue holding meetings to identify system integrity problems and track corrective action in the form of reconciliation and manual controls.	<b>MW</b>
TSA-4-04	Inaccuracies exist within TSA personnel records which addresses both separated employee issue and other erroneous personnel records	Correct issues regarding separated employees and continue reconciliation efforts to correct erroneous personnel information in CUPS and CPMIS.	<b>MW</b>

**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

**Appendix C - Cross-Walk of Previous Year's Notice of Findings  
and Recommendations to Current Year**



**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

Bureau	NFR No.	Description	Disposition	
			Closed	Repeat
CIS/ICE	03-02	Benefits Systems Division has no risk assessment for the Claims 3 mainframe	<b>X</b>	
CIS/ICE	03-03	BCIS needs to complete and strengthen security plans for Claims 3 Mainframe and Claims 4	<b>X</b>	
CIS/ICE	03-04	BCIS security training polices not implemented	<b>X</b>	
CIS/ICE	03-10	(b) (2) High		04-19
CIS/ICE	03-12			04-09
CIS/ICE	03-13	BCIS Access Control Weaknesses	<b>X</b>	
CIS/ICE	03-14	BCIS/BICE service continuity weaknesses	<b>X</b>	
CIS/ICE	03-15	Implementation of Corrective Actions for Claims 3 and Claims 4 from the Security Test and Evaluation (ST&E) not implemented	<b>X</b>	
CBP	03-01	(b) (2) High		04-01
CBP	03-02	Functions	<b>X</b>	
CBP	03-03	Non-existent/Incomplete NDC Fire Evacuation Plans and Procedures	<b>X</b>	
CBP	03-04	(b) (2) High		04-04
CBP	03-05			04-18
CBP	03-06			04-02
CBP	03-07			04-09
CBP	03-08			04-08
CBP	03-09			04-02
CBP	03-10			04-14
CBP	03-11	Lack of Certification & Accreditation of CBP's Data Telecommunications Network	<b>X</b>	
CBP	03-12	(b) (2) High		04-10
CBP	03-13	Application Change Control Documentation Process is not Consistent with Published Guidance	<b>X</b>	
CBP	03-14	(b) (2) High		04-07
CBP	03-15			04-03
CBP	03-16			04-05
CBP	03-17			04-12
CBP	03-18			04-06

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

Bureau	NFR No.	Description	Disposition	
			Closed	Repeat
CBP	03-19	(b) (2) High [Redacted]		04-03
CG	03-001	(b) (2) High [Redacted]		04-022
CG	03-002	[Redacted]		04-013
CG	03-003	[Redacted]		04-014
CG	03-004		X	
CG	03-005	No documentation of system software changes; same staff makes changes and moves into production. – AR&SC -	X	
CG	03-006	Infrequent back up, weaknesses in DRP – AR&SC	X	
CG	03-007	Application changes do not follow procedures – AR&SC	X	
CG	03-008	(b) (2) High [Redacted]		04-020
CG	03-009	[Redacted]		04-004
CG	03-010	[Redacted]		04-005
CG	03-011	[Redacted]		04-006
CG	03-012	Telecommunications—weak password allowed access to Dataline card reader application. (War Dial)	X	
CG	03-013	(b) (2) High [Redacted]		04-007
CG	03-014	information technology support positions within FINCEN are not up-to-date	X	
CG	03-015	FINCEN personnel are not currently using PVCS® Tracker/Version Manager to maintain and track application changes for CGOF or LUFS.	X	
CG	03-016	System Developer Access to Production Software and Files – AR&SC – BCCP not up to date, tested, no training in BCCP.	X	
CG	03-017	(b) (2) High [Redacted]		04-008
CG	03-018	configuration and changes not documented.	X	
CG	03-019	NESSS Access Administration – OSC/ELC—No process to ensure system access commensurate with responsibilities.	X	
CG	03-020	FLS (Fleet Logistics System) Access – OSC/ELC – weak passwords and log ins and no ability to track.	X	
CG	03-021	(b) (2) High [Redacted]		04-009

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

Bureau	NFR No.	Description	Disposition	
			Closed	Repeat
CG	03-022	(b) (2) High [Redacted]		04-011
CG	03-023	Development Life Cycle (SDLC) methodology and violate segregation of duties.	X	
CG	03-024	(b) (2) High [Redacted]		04-010
CG	03-025	[Redacted]		04-012
CG	03-026	[Redacted]		04-015
CG	03-027	[Redacted]		04-016
CG	03-028	[Redacted]		04-021
CG	03-029	[Redacted]		04-015
CG	03-030	[Redacted]		04-015
CG	03-031	[Redacted]		04-014
CG	03-032		X	
CG	03-033	PSC transmissions-- No confirmation of receipt of data.	X	
CG	03-034	(b) (2) High [Redacted]		04-003
CG	03-035		X	
CG	03-036	Service continuity—No DRP, no testing of COOP	X	
CG	03-037	Security Training – HQ—Training not tracked.	X	
CG	03-038	(b) (2) High [Redacted]		04-023
CG	03-039	[Redacted]		04-019
CG	03-040	Ledger Module during data conversion.	X	
CG	03-041	(b) (2) High [Redacted]		04-018
CG	03-042	[Redacted]		04-017
CG	03-043	[Redacted]		04-024
CONS	03-01	(b) (2) High [Redacted]		04-02
CONS	03-02	Lack of assessment or assurance of security controls in place over TIER and CFO Vision	X	
CONS	03-03	DHS TIER resides on a test server	X	

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

Bureau	NFR No.	Description	Disposition	
			Closed	Repeat
CONS	03-04	(b) (2) High [Redacted]		04-01
CONS	03-05	Lack of a comprehensive and accurate financial system inventory	<b>X</b>	
EPR	03-04	(b) (2) High [Redacted]		04-11
EPR	03-05	[Redacted]		04-39
EPR	03-06	[Redacted]		04-32
EPR	03-07	[Redacted]		04-16
EPR	03-08	[Redacted]		04-17
EPR	03-09	[Redacted]		04-18
EPR	03-10	[Redacted]		04-19
EPR	03-11	not provided to newly hired employees and contractors as part of their orientation to Federal Emergency Management Agency (FEMA).	<b>X</b>	
EPR	03-12	(b) (2) High [Redacted]		04-20
EPR	03-13	[Redacted]		04-21
EPR	03-14	[Redacted]		04-22
EPR	03-22	[Redacted]		04-23
EPR	03-23	[Redacted]		04-24
EPR	03-24	[Redacted]	<b>X</b>	
EPR	03-26	(b) (2) High [Redacted]		04-25
LTD	03-01	(b) (2) High [Redacted]		04-01
SLGCP	03-01	(b) (2) High [Redacted]		Reissued under the DOJ OJP audit
SLGCP	03-02	[Redacted]	<b>X</b>	
SLGCP	03-03	(b) (2) High [Redacted]		Note 1

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

Bureau	NFR No.	Description	Disposition	
			Closed	Repeat
SLGCP	03-04	Access Controls, System Software - poor configuration management on OJP servers		Note 1
SLGCP	03-05	Access Controls - lack of compliance with security measures at workstation area	X	
SLGCP	03-06	Change Controls relating to service request signatures	X	
SLGCP	03-07	Security Program not updated for current conditions for FY2002 or FY2003 or FY2004	X	
SLGCP	03-08	Weakness in service continuity plans	X	
SLGCP	03-09	Access privileges and profiles for IFMIS.	X	
SLGCP	03-10	External network on the ODP web server contained default java scripts.	X	
TSA	03-01	Individuals can both initiate and approve SF52 personnel actions	X	
TSA	03-02	Resource constraints in maintaining personnel system	X	
TSA	03-03	(b) (2) High [Redacted]		04-04
TSA	03-04	[Redacted]		04-02

**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

**Management Response to Draft Information Technology  
Management Letter**

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

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

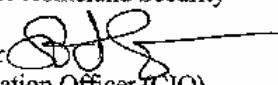
APR 14 2005

MEMORANDUM

TO: Inspector General  
 Department of Homeland Security



**Homeland  
 Security**

FROM: Steve Cooper   
 Chief Information Officer (CIO)  
 Department of Homeland Security

SUBJECT: Response to Draft Information Technology (IT) Management Letter

Thank you for the opportunity to review the draft "Information Technology Management Letter for the FY 2004 DHS Financial Statement Audit," IT-A-04-009, dated February 2005. The CIO office appreciates the recognition of the strides made in the development of the entity-wide Information Security Program. There is concurrence with the general remarks about the need for continuous growth and improvement as referenced in the draft report's recommendations. We have already initiated several projects in the later part of Fiscal Year (FY) 2004 that address most of these recommendations.

With respect to the specific recommendations, the Department's responses are provided below.

**Recommendation - The DHS CIO, in coordination with the Chief Financial Officer (CFO) and other DHS functional leaders, should continue to implement and enforce the C&A program.**

**Comments:** The DHS Office of the CIO identified the C&A program as the number one information security initiative for FY 2004. Led by the DHS Chief Information Security Officer (CISO), Bob West, and the Compliance and Oversight Program Director, Wayne Bavry, the Department plans on continuing the focus on C&A in FY 2005. In FY 2004, the Information Security Program initiated several key initiatives to ensure a sustainable C&A program within the Department. These activities included, but were not limited to:

- Identifying and implementing an enterprise-wide approach (e.g., tool) to ensuring a cost-effective and consistent approach to C&A activities throughout the Department.
- Developing a Plan of Action and Milestones (POA&M) for the C&A program to address an implementation path. This plan is currently being executed.
- Focusing CIO senior management on the need and requirements associated with a comprehensive Information Security Program, including a C&A program.

As of February 2005, these tasks have succeeded in increasing visibility and delivery of an effective C&A program. Although we have encountered numerous challenges, including procurement delays, several key milestones were completed related to the implementation of a Department C&A Tool to ensure compliance with DHS and National Institute of Standards and Technology (NIST) guidance in the C&A process as outlined in NIST SP 800-37:

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

- Completion of an independent technical evaluation of commercial C&A Tools on April 28, 2004. The independent technical evaluation resulted in a recommended C&A Tool, SecureInfo's Risk Management System (RMS).
- Implementation of a pilot of the C&A Tool from September through December 2004.
- Development of the DHS Working Capital Fund (WCF) and further assignment of the C&A Tool to this fund. Approval of WCF monies for C&A Tool implementation was closely coordinated with the OCFO. The C&A Tool was granted funding in January 2005. The final C&A Tool contract was awarded in February 2005.
- Alignment of the C&A process within the DHS Enterprise Architecture Board/Enterprise Architecture Center of Excellence (EAB/EACOE) processes for ensuring life cycle visibility for security implementation. In addition, OMB 300 information security subject matter experts review the appropriate security sections for alignment with funding submissions.
- Development and delivery of improved guidance and training in the C&A Process and the DHS selected tool.
- Development of a C&A remediation plan with each OE to focus on the completion of C&A for every unaccredited system at DHS.

As a direct result of the feedback and observations in FY 2004, my office has identified coordination with the CFO and DHS functional leaders as key to our long-term success in implementing a successful C&A program. Some of the specific actions that we are currently implementing include:

- Active participation in the EAB/EACOE process to ensure new projects receives the proper pro-active visibility and alignment with the C&A program. This process is a shared responsibility with CFO and functional leader representatives. This will help link funding with performance.
- Deployment of Information Security Digital Dashboard and Balanced Scorecard for raising the awareness of senior executives about the status of their program, including C&A, from a Department level. The Scorecard helps management hold OEs and people accountable to our overall success.
- Enterprise-wide deployment of the C&A Tool now that the final procurement actions have occurred. This deployment is scheduled to occur March 28, 2005 and will involve getting deployment beyond the pilot users completed in FY 2004.
- Development of OE "get well" plans to ensure C&A plans are updated and on track.
- Development of a program official's guide to information security to outline and assist them in implementing their responsibilities, including system C&A.

The DHS CISO is aware of the compelling need to improve the number of systems with completed C&As. Both Bob West and I are working to engage the CFO and functional



**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

leaders on understanding the need and priorities for the security program as mentioned in your report.

**Recommendation – A DHS-wide security training and awareness program is designed and implemented consistent with OMB and NIST guidance. A key focus of the training program should be on the detection and prevention of technical weaknesses identified in this management letter.**

**Comments:** A POA&M for a DHS-wide security training and awareness program has been developed and is being executed. Unfortunately, due to personnel turnover (twice in FY 2004), progress in this area has been limited. The CISO is working proactively with the Human Capital Office and Office of Security to resolve this issue and has established a Training Working Group aimed at resolving the training issues.

However, despite these challenges, the Department was able to improve its training performance with the assistance of the Organizational Elements. As shown in the table below, significant progress was made in training in FY 2004 compared to FY 2003. This progress represents significant cooperation between the DHS Headquarters and the Organizational Elements.

FISMA Performance Measures	FY 2003	FY 2004
• DHS system users that received IT security awareness training		85%
• Information security professionals that received specialized training		89%

In conjunction with the deployment of the entity-wide C&A Tool and ongoing efforts to improve the quality of the Annual DHS Security Conference, both the scope and quality of the training program is being refined and will begin taking a more active role in the Department in FY 2005.

**Recommendation – Information security planning efforts follow relevant Federal guidance (i.e. OMB and NIST).**

**Comments:** The DHS 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 DHS 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 IT systems, current IT programs, and new IT initiatives.

For legacy IT 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 (FISMA) Reporting tool to identify gaps in our security planning and compliance efforts. Any gaps are reported to senior management and addressed to

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

determine if any relevant corrective actions are necessary and practical. In addition, the Compliance and Oversight Program Director performs periodic reviews to determine the validity of the self-reported data. I have authorized the CISO to ensure adequate management visibility of any issues.

For current IT programs under development, the Security Policy Program Director participates on the DHS EAB to ensure compliance of programs going forward in meeting the agency expectations for Security Planning and Federal guidance compliance. 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 IT initiatives, the CISO is included in all new projects reviews as part of the Department's Capital Investment Control (CPIC) 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.

Finally, procurement delays hindered acquisition of a contractor responsible for keeping the DHS Management Directives updated. The contract was awarded in February 2005. With this new support, my office will be able to ensure our continued adherence to NIST and OMB guidance and expect a new release of DHS Security Policy in the spring of 2005. In addition, my office has been working proactively to help align DHS Policy with upcoming FISMA guidance being developed by NIST (e.g., NIST SP 800-53) with integration in the requirements and templates available via the enterprise C&A Tool.

**Recommendation – Security risk assessments are completed in a consistent manner per OMB and NIST guidance**

**Comments:** As discussed in the response to Recommendation #1, DHS is in the process of procuring and installing an enterprise C&A Tool. One of the major benefits of the C&A Tool will be the ability to conduct security risk assessments using a consistent methodology. Some of the supplemental support my office has implemented to ensure compliance with OMB and NIST guidance, is to:

- Generate test plan templates 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.
- Ensure uniform C&A quality and resulting risk assessments (and address recommendations #3 and #4) and provide improved management reporting. It should be noted that due to the three year C&A life cycle and the cost and complexity of certifying systems, achieving the full benefits from the enterprise C&A Tool will be a long-term DHS objective.
- Conduct pilot training for improving all aspects of the C&A process, including security risk assessments.
- Elaborate on security risk assessment guidance within the DHS IT Security Handbook and ISSO Guide for ensuring consistent application.

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

- Coordinate with OEs via the ISSB and ISSMs to ensure these materials are available and used by the system owners and ISSOs.

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 to provide management oversight.

**Recommendation – The above recommended entity-wide security efforts are implemented in a timely and consistent manner throughout the agency.**

**Comments:** DHS 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. 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. This can only be achieved with coordination from senior management, CFOs, CIOs, and functional leaders. As identified in recommendation number one, we are actively strengthening this relationship.

The challenges associated with any entity-wide security effort are daunting but my office is working to address these issues. Your reports and insights into the various OE security efforts also provide a valuable and insightful view into the programs on ways and methods we need to improve.

**Recommendation – Ensure that password controls meet DHS password requirements and are enforced on all systems.**

**Comments:** From a Departmental perspective, the monitoring or verification of specific operating system and application software controls implemented on OE systems is an OE or Program Owner responsibility. The Departmental security program will address this recommendation by implementing verification reviews to ensure that OEs have implemented a compliance program and also ensure that these compliance programs are conducting some verification of password controls.

**Recommendation – Implement a password account management process within the Bureaus to ensure the periodic review of user accounts.**

**Comments:** The Department will address this via Departmental policy and address compliance via the CIO compliance program.

**Recommendation – Design and implement a DHS-wide patch and security configuration process.**

**Comments:** On a DHS-wide basis, this recommendation realistically cannot be implemented across the current legacy environment of twenty two (plus) architectures with available funding as a constraint – particularly with the ongoing outsourcing of applications by program offices that is taking place across DHS outside of CIO control. Patch management is being addressed on a Department level Infrastructure basis by

**Department of Homeland Security**  
*Information Technology Management Comments*  
 September 30, 2004

ongoing emigration to a single DHS Infrastructure -- but this process is a long term solution.

**Recommendation** – Implement a vulnerability assessment process whereby systems are periodically reviewed for security weaknesses.

**Comments:** OMB has mandated yearly reviews of system using the 800-26 assessment methodology. DHS is looking into ways to modify the 800-26 assessment to include an associated vulnerability assessment.

**Recommendation** – Policies and procedures are developed and implemented to address segregation of duties for IT and accounting functions.

**Recommendation** – Responsibilities are documented so that incompatible duties are consistently separated.

**Comments: (for both recommendations above):** Policies are in place. The in-progress implementation of the DHS C&A tool (RMS) will ensure that testing performed as part of the C&A process ensures compliance with DHS policy. Use of RMS is being mandated for all SBU systems accredited after April 11, 2005.

**Recommendation** – Develop and implement complete business continuity plans and system disaster recovery plans.

**Comments:** A Departmental Disaster Recovery Plan (DRP) is currently being developed. The implementation of this plan is currently TBD.

**Recommendation** – Bureaus [sic] keep input, processing and output control policy and procedures current.

**Comments:** Clarification of this recommendation is requested. This recommendation appears to address procedures that would be issued and implemented by the Office of the CFO.

**Recommendation** – DHS CIO, in coordination with the OCFO perform annual testing of the input, output and processing controls of critical DHS financial systems to ensure that the controls are in place and operating as intended.

**Comments:** The activity described is really an audit of application controls as described by GAO/AIMD-12.19.6 January 1999, page 11. The Office of the CIO will discuss this with the Office of the CFO but the Office of the CIO is not resourced to perform this type of testing and does not have the financial background to perform this type of testing. The generation of test transactions and the use of test transactions to periodically verify the performance of financial systems are believed by the Office of the CIO to be an OCFO responsibility.

**Conclusion**

I agree that a key aspect of financial statement auditing includes an assessment of the DHS IT general controls as IT systems do significantly facilitate DHS' financial

**Department of Homeland Security**  
*Information Technology Management Comments*  
September 30, 2004

processing activities and ability to maintain important financial data. I look forward to working with you and your staff in resolving the recommendations from the FY 2004 audit to the satisfaction of all concerned. I also look forward to working more closely with you and the CFO in the successful conduct of the FY 2005 financial audit.

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

- The 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 DHS OEs. The scorecard helps the OEs 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 OEs.
- The Digital Dashboard reports aggregated information security data at the OE and Department level. The dashboard serves as a management tool to ensure that OEs take a risk-based, cost-effective approach to secure their information and systems, identify and resolve current Information Technology (IT) security weaknesses and risks, as well as protect against future vulnerabilities and threats. The dashboard allows DHS management to monitor OE remediation efforts to more accurately identify progress and problems.

## **Report Distribution**

### **Department of Homeland Security**

Secretary  
Deputy Secretary  
General Counsel  
Chief of Staff  
Executive Secretariat  
Under Secretary, Management  
Chief Information Officer  
Chief Financial Officer  
DHS Public Affairs  
DHS Audit Liaison  
Chief Information Office Audit 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](http://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 Security, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.