DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Information Technology Management Letter for the FY 2005 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-06-49 **July 2006**

Office of Inspector General

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

Homeland
Security

July 10, 2006

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (*Public Law 107-296*) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports published by our office as part of our DHS oversight responsibility to promote economy, effectiveness, and efficiency within the department.

This report presents the information technology (IT) management letter for DHS' FY 2005 financial statement audit. It contains observations and recommendations related to information technology internal control that were not required to be reported in the financial statement audit report (OIG-06-09, November 2005) and represents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit of DHS' financial statement as of September 30, 2005, and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated December 15, 2005, and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control or conclusion on compliance with laws and regulations.

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

Richard L. Skinner

Richard L. Skinner
Inspector General

KPMG LLP
2001 M Street, NW
Washington, DC 20036

December 15, 2005

Inspector General
U.S. Department of Homeland Security

Chief Information Officer
U.S. Department of Homeland Security,

Chief Financial Officer
U.S. Department of Homeland Security,

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, 2005. We were not engaged to audit the consolidated statements of net cost, changes in net position, and financing, combined statement of budgetary resources, and statement of custodial activity for the year ended September 30, 2005. Because of matters discussed in our *Independent Auditors' Report*, dated November 14, 2005, the scope of our work was not sufficient to enable us to express, and we did not express, an opinion on the consolidated balance sheet for the year ended September 30, 2005.

In connection with our fiscal year 2005 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 control 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 14, 2005, and included in the FY 2005 DHS *Performance and Accountability Report*. A description of each internal control finding, and its disposition, as either a significant finding contributing to the material weakness for financial systems security, any remaining findings contributing to the material weakness for financial systems security, 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, 2005.

As described above, the scope of our work was not sufficient to express an opinion on the consolidated balance sheet of DHS as of September 30, 2005, and we were not engaged to audit the consolidated statements of net cost, changes in net position, and financing, combined statement of budgetary resources, and statement of custodial activity for the year ended September 30, 2005. Accordingly, other internal control matters and other instances of non-compliance may have been identified and reported had we been able to perform all procedures necessary to express an opinion on the September 30, 2005 consolidated balance sheet, and had we been engaged to audit the other fiscal year 2005 consolidated financial statements. 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.

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

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE AND APPROACH

KPMG performed an audit of DHS IT general controls in support of the FY 2005 DHS financial statement engagement. The overall objective of our audit 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 audit. The scope of the IT general controls assessment included testing at DHS' Office of the Chief Financial Officer (OCFO), and all significant DHS component as described in Appendix A.

FISCAM was 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.
- *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.

In addition to testing DHS' general control environment, KPMG performed application control tests on a limited number of DHS financial systems and applications. The application control testing was performed to assess the controls that support the financial systems' internal controls over the input, processing, and output of financial data and transactions.

- *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 audit, 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.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2005 DHS took corrective action to address many prior year IT control weaknesses. However, during FY 2005, we continued to find IT general control weaknesses at each DHS component. The most significant information security weaknesses from a financial statement audit perspective relate to entity-wide security, access controls, and service continuity. Collectively, these 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 weakness for financial system security under standards established by the AICPA and accepted by the GAO.

During fiscal year 2005, DHS took several actions to improve its IT general control environment, and to address many prior year general IT control issues. For example, the Coast Guard has begun performing regular technical vulnerability scans on their information technology network and key systems. These scans resulted in the reduction of the number of conditions our audit team identified during our testing. In addition, DHS issued an update to DHS Policy 4300A, *Sensitive System Handbook*. The purpose of this Handbook update was to provide specific techniques and procedures for implementing the requirements of DHS' *IT Security Program for Sensitive Systems*. These actions resulted in the correction of some conditions we reported in 2004. DHS needs further emphasis on the monitoring and enforcement of the policies and procedures through the performance of periodic security control assessments and audits.

FINDINGS BY IT AUDIT AREA

Entity-Wide Security Program Planning and Management

During FY 2005 DHS continued to make progress in having all of its financial systems certified and accredited. 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 letter, reduce the overall effectiveness of the entity-wide security programs for the individual DHS components and the overall Department.

Conditions noted in FY 2005 regarding entity-wide security program planning and management at DHS were:

- EWS-05–1: Despite improvements in the process of performing Certification and Accreditation (C&A) of IT systems, five DHS component financial and associated feeder systems were not properly certified and accredited.
- EWS-05-2: Instances of fragmented, incomplete, or missing security policies and procedures relating to the hiring and termination of employees, reviewing of access to key financial systems, computer incident response capabilities, and interconnectivity agreements exist.

Recommendations:

We recommend that the DHS Office of Chief Information Officer in coordination with the OCFO:

a) Ensure adherence to a DHS C&A program across all DHS components, which should include an emphasis on a consistent and thorough approach to the testing of key technical controls during the certification process; and

b) Ensure the consistent implementation of security programs, policies, and procedures.

Access Controls

During FY 2005 we noted significant access control vulnerabilities with internal IT systems (i.e., inside the components' firewalls). These are significant issues because personnel inside the organization who best understand the organization's systems, applications, and business processes are able to have 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.

Conditions noted in FY 2005 regarding access controls at DHS were:

- AC-05-1: Instances of missing and weak user passwords on key servers and databases.
- AC-05-2: User account lists were not periodically reviewed for appropriateness, and inappropriate authorizations and excessive access privileges for group user accounts were allowed.
- AC-05-3: Instances where workstations, servers, or network devices were configured without necessary security patches, or were not configured in the most secure manner.
- AC-05-4: Application and operating system settings were not configured for automatic log-off or account lockout.

Recommendations:

We recommend that the DHS Office of Chief Information Officer in coordination with the OCFO:

a) Ensure that password controls meet DHS password requirements on all key financial systems;

b) Implement an account management certification process within all the components, to ensure the periodic review of user accounts for appropriate access;

c) Implement a DHS-wide patch and security configuration process, and ensure compliance with the requirement that systems are periodically tested by individual DHS components and the DHS-CIO; and

d) Conduct periodic vulnerability assessments, whereby systems are periodically reviewed for access controls not in compliance with DHS and Federal guidance.

Application Software Development and Change Control

During FY 2005 we noted that DHS took corrective actions to address IT control issues related to application software changes. However, we noted that in some cases the application software change control documentation was still not consistent with DHS systems development life cycle (SDLC) guidance.

Conditions noted in FY 2005 regarding application system development and change control at DHS and its components were:

- ASDCC-05-1: Instances where policies and procedures regarding configuration management controls were not in place to prevent users from having concurrent access to the development, test, and production environments of the system.
- ASDCC-05-2: Changes made to the configuration of the system were not always documented through System Change Requests (SCRs), test plans, test results, or software modifications. Additionally, documented approval did not exist, or was not always retained, for emergency enhancements, "bug" fixes, and data fixes, and in some cases, audit logs for tracking changes to the data or systems were not activated.

Recommendations:

We recommend that the DHS Office of Chief Information Officer in coordination with the OCFO:

a) Develop and implement policies and procedures regarding configuration management controls, and ensure that users do not have concurrent access to development, test, and production environments; and

b) Ensure adherence to policies that require changes to the configuration of the system are approved and documented, and audit logs are activated and reviewed on a periodic basis.

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 were:

- SS-05-1: 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-05-2: Changes to sensitive operating system settings and other sensitive utility software and hardware were not always documented.

Recommendation:

We recommend that the DHS Office of Chief Information Officer, in coordination with the OCFO, monitor the use, and changes related to operating systems, and other sensitive utility software and hardware.

Segregation of Duties

During FY 2005, 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 were:

- SD-05-1: Instances where individuals were able to perform incompatible functions, such as the changing, testing, and implementing of software, without sufficient compensating controls in place.
- SD-05-2: 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 Office of Chief Information Officer in coordination with the OCFO:

a) Document user responsibilities 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; and

b) Assign personnel to key security positions, and ensure that position descriptions are kept current.

Service Continuity

During FY 2005 we noted that DHS took some corrective actions to address IT control issues related to developing contingency plans and the back-up and protection of critical system data. Despite these improvements, weaknesses related to 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 were:

- SC-05-1: Five DHS components had incomplete or outdated business continuity plans and systems with incomplete or outdated disaster recovery plans. Some plans did not contain current system information, emergency processing priorities, procedures for backup and storage, or other critical information.
- SC-05-2: Five DHS component's service continuity plans were not consistently and/or adequately tested, and individuals did not receive training on how to respond to emergency situations.

Recommendations:

We recommend that the DHS Office of Chief Information Officer in coordination with the OCFO:

a) Develop and implement complete and current business continuity and system disaster recovery plans, and

b) Perform component-specific and DHS-wide testing of key service continuity capabilities, and assess the need to provide appropriate and timely emergency training.

Application Controls

During FY2005, we noted several instances of weak access and segregation of duty controls associated with key DHS financial applications, such as a DHS component's core financial application, as well as procurement and payable applications. These weaknesses include weak or expired user passwords, user accounts that were not kept current, and certain users with access privileges to certain key processes of an application. Many of these weaknesses were identified during our general control testing of access controls and segregation of duties; however, since these same issues also impact controls over specific key financial applications, they are reported here as well.

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

- APC-05-1: Instances of missing and weak user passwords on key application servers and databases.
- APC-05-2: User account lists were not periodically reviewed for appropriateness, and inappropriate authorizations and excessive access privileges for group user accounts were allowed.
- APC-05-3: Instances where individuals were able to perform incompatible functions, such as the changing, testing, and implementing of software, without sufficient compensating controls in place.

Recommendations:

We recommend that the DHS Office of Chief Information Officer in coordination with the OCFO:

a) Ensure that password controls meet DHS password requirements on all key financial systems;

b) Implement an account management certification process within all the components, to ensure the periodic review of user accounts for appropriate access; and

c) Document the user responsibilities 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.

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. However as noted in the summary section of the status spreadsheet, components did not concur with ten (10) of the NFRs and the DHS CIO is currently working to fully document all "non-concurs." We have incorporated the comments where appropriate and included a copy of the comments at Appendix D.

OIG Response

We accept the DHS CIO's response to the recommendations in this report and are encouraged that the DHS CIO will work with each DHS component to ensure that a Plan of Action and Milestones (POA&M) is developed for each of the 88 NFRs. We are also encouraged by the DHS CIO's commitment to take corrective actions on these IT NFRs during the FY 2006 DHS Financial Statement Audit. However, the DHS CIO's response did not provide details on any planned corrective actions for each of the recommendations outlined in this report. KPMG will follow up on the corrective actions for these recommendations during the FY 2006 Financial Statement Audit.

Appendix A

Description of Key Financial Systems and IT Infrastructure within the Scope of the FY 2005 DHS Financial Statement Audit

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

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, 2005.

United States Citizen and Immigration Services (USCIS)

<u>Locations of Audit:</u> USCIS Headquarters in Washington, D.C., as well as offices in Texas, Vermont and Nebraska.

<u>Key Systems Subject to Audit:</u>

- *Federal Financial Management System (FFMS)* – The Immigration and Customs Enforcement (ICE) component owns and operates FFMS. ICE performs the financial reporting function for USCIS, using FFMS per the shared services agreement with USCIS. FFMS is a commercial off-the-shelf financial reporting system that was fully implemented in FY 2003. FFMS is the official system of record and is built in Oracle 8i Relational Database Management System. It includes the core system used by accountants, FFMS Desktop, which is used by average users, and a National Finance Center payroll interface. FFMS supports all USCIS core financial processing. FFMS uses a Standard General Ledger (SGL) for the accounting of agency financial transactions.

- *Claims 3 Local Area Network (LAN)* – Claims 3 LAN provides USCIS with a decentralized LAN based system that supports the requirements of the Direct Mail Phase I and II, Immigration Act of 1990 (IMMACT 90) and USCIS Forms Improvement projects. The Claims 3 LAN is located at each of the service centers (Nebraska, California, Texas, Vermont, and the National Benefits Center). The main purpose of Claims 3 is to enter and track immigration applications.

- *Claims 4* - The purpose of Claims 4 is to track and manage naturalization applications. Claims 4 resides on multiple platforms, including a Siemens E70 located in Dallas, Texas. Claims 4 data is centrally stored within one Oracle Database. Software is developed and maintained in the Oracle relational database (RDBMS) and Microsoft Visual Basic environments.

Immigration and Customs Enforcement (ICE)

<u>Locations of Audit:</u> ICE Headquarters in Washington, D.C., as well as offices in Texas, Vermont and Nebraska.

<u>Key System Subject to Audit:</u>

- *Federal Financial Management System (FFMS)* – ICE owns and operates FFMS. ICE performs the financial reporting function for CIS, MGT, IAIP, and S&T using FFMS per the shared services agreement these agencies have with ICE. FFMS is a commercial off-the-shelf financial reporting system that was fully implemented in FY 2003. FFMS is the official system of record and is built in Oracle 8i Relational Database Management System. It includes the core system used by accountants, FFMS Desktop that is used by average users, and a National Finance Center payroll interface. FFMS supports all USCIS/ICE core financial processing and uses a Standard General Ledger (SGL) for the accounting of agency financial transactions.

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

United States Coast Guard

Locations of Audit: Coast Guard Headquarters in Washington, DC; the Aviation Repair and Supply Center (ARSC) in Elizabeth City, North Carolina; -- --- -------------- ----------------------------------- -- --------------------- -- -------------

Key Systems Subject to Audit:

- *Core Accounting System (CAS)* – CAS is the core accounting system that records financial transactions and generates financial statements for the Coast Guard. CAS is hosted at ---------- , the Coast Guard's primary data center.

- *Financial Procurement Desktop (FPD)* – The FPD application used to create and post obligations to the core accounting system. It allows users to enter funding, create PR's, issue procurement documents, perform system administration responsibilities, and reconcile weekly Program Element Status (PES) reports.

- *Workflow Imaging Network System (WINS)* - WINS is the document image processing system, which is integrated with an Oracle Developer/2000 relational database. WINS allows electronic data and scanned paper documents to be imaged and processed for data verification, reconciliation and payment. WINS utilizes MarkView software to scan documents and to view the images of scanned documents and to render images of electronic data received.

- *Naval Electronics Supply Support System (NESSS)* – Formerly named the Supply Center Computer Replacement System (SCCR), NESSS is hosted at------ NESSS is the primary financial application for the Engineering Logistics Command (ELC), the Supply Fund, and the Yard fund. Also housed at ----- is the Fleet Logistics System (FLS), a web-based application designed to automate the management of Coast Guard vessel logistics by supporting the following functions: configuration, maintenance, supply and finance. In addition, ----- is responsible for CMPlus, the central repository for activities associated with maintaining Coast Guard assets at the unit level.

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.

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

United States Customs and Border Protection (CBP)

Locations of Audit: [redacted]

Key Systems Subject to Audit:
Below is a description of significant CBP financial management systems and supporting IT infrastructure included in the scope of the September 30, 2005 CBP consolidated balance sheet audit.

- [redacted] was decommissioned in FY 2005 and replaced by SAP. It was CBP's IBM [redacted]-based financial management system that supported primary financial accounting and reporting processes, and a number of additional subsystems for specific operational and administrative management functions. The core system consisted of general ledger, accounts receivable, disbursements/payables, purchasing, and budget execution modules. [redacted] was hosted on a customized version of [redacted]

- [redacted] is a client/server-based financial management system that was implemented beginning in FY 2004 to ultimately replace the [redacted] using a phased approach. The [redacted] was implemented and utilized in FY 2004. In FY 2005, the Funds Management, Budget Control System, General Ledger, Internal Orders, Sales and Distribution, Special Purpose Ledger, and Accounts Payable modules were implemented.

- [redacted] 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.

- [redacted] – Used for tracking seized assets, Customs Forfeiture Fund, and fines & penalties.

DHS Consolidated

Location of Audit: DHS Headquarters in Washington, D.C.

Key Systems Subject to Audit:

- *Treasury Information Executive Repository (TIER)* – The system of record for the DHS consolidated financial statements is TIER. The DHS components update TIER on a monthly basis with data extracted from their core financial management systems. TIER subjects component 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 DHS user accounts within the TIER and CFO Vision applications.

Limited Scope

Location of Audit: We performed follow-up on a FY 2003 finding at the [redacted]

System Subject to Audit:
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.

Federal Emergency Management Agency (FEMA)

Locations of Audit: FEMA Headquarters in Washington, D.C., and the [redacted]

Key Systems Subject to Audit:

- *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.

- *Logistical Information Management System (LIMS III)* – LIMS III provides for material management, maintenance, and logistics reporting.

- *National Flood Insurance Program System* – The system provides loss projections, recovery rates, and, maintains customer records for the flood insurance program.

- *Quicktime* - *Time and Attendance Collection System* – A web-based system used to collect hours worked and leave used by all employees in FEMA. The data collected is transmitted to the National Finance Center for paycheck preparation.

Office of State and Local Government Coordination and Preparedness (SLGCP)

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

Key Systems Subject to Audit:

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's, 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.

Transportation Security Administration (TSA)

Locations of Audit: TSA Headquarters in Washington, D.C. ----- - ---
-------------- ---------- TSA's financial applications are hosted on the Coast Guard's IT platforms.

Key Systems Subject to Audit:
The Coast Guard is a service provider for Transportation Security Administration (TSA) by maintaining the Core Accounting System. This application is housed at the --------------- ---------
----

- *Core Accounting System (CAS)* – CAS is the core accounting system that records financial transactions and generates financial statements for TSA. CAS is hosted at ---------- the Coast Guard's primary data center.

- *Financial Procurement Desktop (FPD)* – The FPD application used to create and post obligations to the core accounting system. It allows users to enter funding, create PR's, issue procurement documents, perform system administration responsibilities, and reconcile weekly PES Reports.

- *Workflow Imaging Network System (WINS)* - WINS is the document image processing system, which is integrated with an Oracle Developer/2000 relational database. WINS allows electronic data and scanned paper documents to be imaged and processed for data verification, reconciliation and payment. WINS utilizes MarkView software to scan documents and to view the images of scanned documents and to render images of electronic data received.

- *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.

TSA payroll, time and attendance, and HR moved to the -- ----- -- -- -- on August 22, 2005. For payroll, TSA will be using a Kronos system called WebTA, a web-based system, which will interface with the------ system. The HRMaxEmpower system will be TSA's new HR system. The HRMaxEmpower system will also interface with the ------ system.

Appendix B

FY2005 Notice of IT Findings and Recommendations - Detail by DHS Organizational Element

Department of Homeland Security
FY2005 Information Technology
Notification of Findings and Recommendations – Detail

- **United States Citizenship and Immigration Services**

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

Department of Homeland Security
FY2005 Information Technology
Notification of Findings and Recommendations – Detail

Citizenship and Immigration Services

IT NFRs Which Contributed to the Overall DHS Material Weakness for Financial System Security

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
USCIS 05-02	The site Certification and Accreditation (C&A) package for the California Service Center, General Support System (GSS) - Local Area Network (LAN) is outdated and has expired.	Allocate sufficient resources to ensure that the proper implementation policy requirements for all systems used to process, store, or transmit classified or sensitive information to be accredited every three years. Also, consider issuing interim accreditations that represent the managers' explicit acceptance of risks.		**X**	**X**
USCIS 05-03	The C&A package for the Texas Service Center (TSC) GSS-LAN is outdated and has expired.	Allocate sufficient resources to ensure that the proper implementation policy requirements for all systems used to process, store, or transmit classified or sensitive information to be accredited every three years. Also, consider issuing interim accreditations that represent the managers' explicit acceptance of risks.	**X**		**X**
USCIS 05-04	Access control weaknesses such as account management, password length, and a lack of review over audit records were identified for the ------- --- system.	Ensure that---- ------- -- system passwords are established and maintained in accordance with DHS and Federal guidance and that warning banners are in place when users logon to the system.		**X**	**X**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
USCIS 05-05	A Novell NetWare server at USCIS' Texas Service Center (TSC) was identified as not having the correct vendor supplied patches installed.	Test and install vendor supplied patches in a timely manner and undertake frequent vulnerability scanning of all systems at TSC to verify that required patches have been installed.	**X**		**X**
USCIS 05-06	A vulnerability assessment over -- --------at USCIS TSC noted that multiple local administrator accounts had blank passwords including several accounts with supervisor level access.	Ensure that the documented password policy is enforced on all systems and undertake frequent vulnerability scanning on all systems at the TSC to verify that passwords have been assigned and implemented correctly.	**X**		**X**

Department of Homeland Security
FY2005 Information Technology
Notification of Findings and Recommendations – Detail

- **Immigration and Customs Enforcement**

Department of Homeland Security
FY2005 Information Technology
Notification of Findings and Recommendations – Detail

Immigration and Customs Enforcement

Management Comment: IT Notice of Findings and Recommendations

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Management Comment to DHS-CIO and CFO
ICE 05-07	ICE does not have procedures in place to periodically review -------- ---------- --- --------- ----------------- - user access lists and could not provide a list of all authorized ------- users upon request.	Document and implement policies and procedures for the periodic review of --- ---- user accounts, and ensure administrative personnel periodically perform reviews of ------- user accounts.		X	X

Department of Homeland Security
FY2005 Information Technology
Notification of Findings and Recommendations – Detail

- **Customs and Border Protection**

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

Department of Homeland Security
FY2005 Information Technology
Notification of Findings and Recommendations – Detail

Customs and Border Protection

Significant IT NFRs Which Contributed to the Overall DHS Material Weakness for Financial System Security

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
CBP-IT-05-02	The Top Secret mainframe account administration on the [redacted] had several weaknesses over unauthorized access to accounts [redacted] and inactive accounts.	Remove unnecessary central security administrator- [redacted] privileges and accounts or alternatively continue implementation of a [redacted] for use by authorized individuals during pre-determined circumstances.		X	X
CBP-IT-05-09	Improvements are needed in system logical access controls over network assets affecting [redacted]	Develop enterprise-wide solutions for improving network and host-based system configuration design(s), consider the use of security management monitoring tools to prevent possible intrusions, proceed with the implementation of [redacted] provide more robust system management security controls standards for Windows-based production servers, and consider the development of a compliance level policy for adherence to CBP password management policies at the [redacted]		X	X

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
CBP-IT-05-14	CBP management did not adequately implement procedures for restricting access to the data center located in---------- and several terminated employees did not have their badges deactivated in a timely manner.	Perform a formal review of all personnel that have access to the --------- ----- ------- to determine those that do not have a formal user access form in place, establish a formal user access form, and promptly remove physical access rights to the -------- facility when an employee is terminated.	X		X
CBP-IT-05-15	Eighteen (18) ----- ------ ---- -- were found with access to the production environment.	Develop a formally documented process for granting normal and emergency access for ------ ---- -- to the - --- production environment.	X		X
CBP-IT-05-17	CBP has not configured their version of---- -- to include a company code setting of "productive."	Perform a formal analysis of the company code setting to determine if it should be set to “productive”.	X		X
CBP-IT-05-18	Excessive sensitive functions and high-risk combinations have been assigned to ------ users.	Ensure that the assignment of sensitive functions and high-risk combinations of functions to non-supervisory users is based on a documented business need and approved by a supervisory official. Exceptions from guidance provided by the memorandum should be formally approved and documented		X	X
CBP-IT-05-19	Separated employees with active ------ accounts.	Delete the accounts of any confirmed terminated employees, and disable user accounts of separated employees and contractors as stated in CBP and Federal guidance.	X		X

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
CBP-IT-05-28	Access to the ------------ -- -- --- -- ------ ------- -- -------- ----------related dataset and-- - -- ---- -- --- ---- is excessive.	Recertify users with access -- -------- - --- -----------and document the evidence of the recertification.		X	X
CBP-IT-05-30	The number of users with access to Top Secret Audit, Recovery, and Backup datasets is excessive.	Recertify users with access to Top Secret Audit, Recovery, and Backup datasets and document evidence of the recertification.		X	X

Remaining IT NFRs Which Contributed to the Overall DHS Material Weakness for Financial System Security

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Remaining Findings Contributing to the Overall DHS Material Weakness for Financial System Security
CBP-IT-05-01	Numerous-- ---- user IDs were identified as having segregation of duties issues.	Coordinate with each affected field office to either remove conflicting roles or sign a waiver to accept responsibility for associated risks and continue to prevent new IDs with segregation of duties conflict from being created.		X	X
CBP-IT-05-03	After the re-organization of the Office of Information Technology (OIT), security administration functions at the------ are not independent of the operations function.	Ensure that security administration functions remain independent of operations functions.	X		X

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

NFR #	**Condition**	**Recommendation**	**New Issue**	**Repeat Issue**	**Remaining Findings Contributing to the Overall DHS Material Weakness for Financial System Security**
CBP-IT-05-04	Certain controls can be overridden in ------ without supervisory approval.	Develop a process to ensure supervisory review of ----- overrides and ensure that the new --- - -- ---- ---- ----------- --- -- -- --- --- - ----- - system has the appropriate requirements for these controls and that the controls are applied prior to implementation.		**X**	**X**
CBP-IT-05-05	CBP management has not developed formal procedures for granting access to sensitive------ Technical Team member roles.	Formally establish a process for granting --- -- access to sensitive technical team roles that include procedures for documenting authorization requests, identifying roles to be granted, and recertification of user roles within ----- .		**X**	**X**
CBP-IT-05-06	The ------------------ ---- -- ----------- continuity of operations plan (COOP) is not updated to reflect the results of FY 2004 testing, and the upgrade of their financial system from--------- -- -- --- -- ------ - --------- -- -------- ------- - - mainframe to ------	Update------------ - COOP with the most recent FY 2004 test results and re-evaluate the COOP for overall contingency planning procedures on an annual basis and in the event of a major system change or upgrade.	**X**		**X**
CBP-IT-05-08	CBP management has not consistently applied the requirement for initial security awareness training for CBP employees and contractors.	Consistently apply the requirements for initial and refresher security awareness training,	**X**		**X**
CBP-IT-05-10	------security audit log reviews not evidenced for the majority of FY 2005.	Continue to review the audit logs daily, maintain documented evidence, and train backup personnel.	**X**		**X**

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Remaining Findings Contributing to the Overall DHS Material Weakness for Financial System Security
CBP-IT-05-11	CBP ----- Administrator staff have not documented Interconnection Security Agreements (ISA) for all entities that connect with ------	Complete efforts to identify - ------ - - --- ------ -- connections that are considered "legacy" connections as well as connections with ----- and formally establish ISAs with these entities.		X	X
CBP-IT-05-12	CBP alternate processing site agreement not finalized. Priority of service provision not in place.	Formally update the alternate processing site agreement to accurately reflect the current hardware and support that will be required of the alternate processing site vendor in the event of an emergency.	X		X
CBP-IT-05-13	No formal process to confirm or enforce compliance with the ------ ----------------- ---------------- ----- -------	Formalize the process to confirm or enforce compliance with the ------ recertification process at the field sites and document all recertifications.	X		X
CBP-IT-05-16	The incident handling and response capability needs improvement regarding incident detection and initiation, response, recovery, and reporting.	Develop a process to identify the workstations that have yet to install the ----- -------, continue to test and implement a standard real-time automated reporting process, and develop a consistent process to respond to system flaw notifications and track reported security incidents.		X	X
CBP-IT-05-20	CBP does not document changes to the ----- system including test plans, test cases, impact analysis, and test results.	Formally document test plans, test cases, and test results for all - ---- changes, and business and customer impact analysis for ------ changes requests.	X		X

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Remaining Findings Contributing to the Overall DHS Material Weakness for Financial System Security
CBP-IT-05-21	CBP management has not activated logging for critical tables within ----- .	Perform a formally documented assessment of the tables that should be logged by ------ and complete the implementation of table logging within ------	X		X
CBP-IT-05-22	CBP management has not completed a Certification and Accreditation package for all components of the ------ LAN, including no security control assessment and no formal risk assessment conducted.	Complete a security control assessment for all ------- LAN components and a risk assessment for all ------ LAN components.	X		X
CBP-IT-05-23	Lack of evaluation of the need for a separate C&As for applications included in the Administrative Applications C&A, and the improvements needed in risk assessment guidance.	Consider reviewing the sensitivity of applications and based upon results, perform separate C&As where appropriate. Consider establishing a relationship of identified risks to defined security requirements in ------ incorporate a risk-based approach for any re-certification efforts performed, and consider development of definitive guidance for risk assessment and security plan criteria		X	X
CBP-IT-05-24	CBP does not maintain a centralized listing of separated contract personnel.	Develop a formal centralized process for tracking the termination of contract personnel, immediately deactivating systems access of terminated contractors, and periodically assessment of contractor access to CBP systems.	X		X
CBP-IT-05-25	----- idle session lock inconsistent with CBP policy.	Change the setting --------- ----------- ------- to disconnect idle sessions after 20 minutes of inactivity.	X		X

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Remaining Findings Contributing to the Overall DHS Material Weakness for Financial System Security
CBP-IT-05-26	No procedures to detect and deactivate inactive ----- users.	Continue to review and deactivate inactive accounts on a monthly basis and implement an automated mechanism to detect and deactivate inactive accounts	**X**		**X**
CBP-IT-05-27	Virtual Private Network (VPN) access authorizations not documented and VPN accounts are not periodically recertified.	Continue to use the official authorization form for new VPN users and formally recertify all VPN employee accounts on a periodic basis and document results.	**X**		**X**
CBP-IT-05-29	CBP management did not provide information as to whether --- -- ----------- -- ----- - ---- -- are appropriately segregated.	Document that access to the --- -- - -- ------- --- ---- ----- (or equivalent) are properly segregated and perform a review of current granted accesses for appropriateness.		**X**	**X**
CBP-IT-05-31	Weaknesses in the C&A process at field sites including several missing site assessments.	Develop a formal process to ensure that all non-recommend field sites submit a NIST 800-26 LAN self-assessment in a timely manner.		**X**	**X**

Department of Homeland Security
FY2005 Information Technology
Notification of Findings and Recommendations – Detail

- **United States Coast Guard**

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

Department of Homeland Security
FY2005 Information Technology
Notification of Findings and Recommendations - Detail
United States Coast Guard

Significant IT NFRs Which Contributed to the Overall DHS Material Weakness for Financial System Security

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
CG-IT-05-001	The --------------------- ---- --- ------ has not completed a Business Recovery Plan (BRP).	Complete the BRP as planned, store a finalized copy off-site, train personnel in their assigned roles and responsibilities, test the BRP and document lessons learned.		X	X
CG-IT-05-002	----- has not completed a testing baseline and users were able to change their privileges to gain access to production.	Establish a testing detail baseline that defines the standard components that a developer should document in Profession Version Control Software (PVCS) Tracker, and enforce the procedure to implement testing as a component of change implementation.		X	X
CG-IT-05-003	Access control weaknesses exist in the------ ------ ----- ----- -- - ---- ------------ - -- ---------- -------- - including user account creation and termination procedures are not documented, and a recertification of accounts does not take place.	Document and implement RACF account management policies and procedures, perform periodic reviews of ------- accounts, and routinely monitor audit logs for unusual activity.		X	X

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
CG-IT-05-006	Coast Guard has not completed the process of filing the personal records that were recovered and recreating the records that were not found during the migration of records from the Department of Transportation to DHS. Comprehensive policies for conducting background investigations for contractors have not been finalized.	Complete the restoration of background investigation records not included during the migration of records from the Department of Transportation to DHS. Work with DHS to finalize policy for conducting contractor background investigations and document Coast Guard-specific procedures compliant with new DHS requirements.		X	X
CG-IT-05-008	The --------------- system does not require strong passwords and WANG is still being operated without vendor support.	Replace ----------with the Coast Guard Direct Access HRMS 8.9 upgrade, which will address vendor support and password strength.		X	X
CG-IT-05-009	Service continuity weaknesses for the -- --------- --- - --- ------ ---, ----- , and -----, including outdated Business Continuity Contingency Plan (BCCP), lack of disaster recovery procedure details, an off-site storage location in close proximity to the data center, and lack of BCCP testing exist.	Periodically reassess and, as appropriate, revise the -------- -- BCCP, develop disaster recovery procedures for ----- and -----, complete the relocation of the off-site storage location, and periodically test the BCCP.		X	X
CG-IT-05-010	-------- -- Unix change control process supporting ----- and ----- have weaknesses including: procedures in support of the finalized CM policy are not developed, documentation supporting risk assessments is not maintained, formal change requests are not used, and test plans and test results are not documented.	Develop and enforce configuration management procedures for developing test plans, documenting test results, implementing software, management approval of system changes, and retention of all risk assessments and testing documentation.		X	X

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
CG IT 05-011	------ - -- does not have documented procedures for controlling the processes associated with the granting, monitoring, and termination of user accounts within FPD have not been documented.	Develop formal entity wide procedures for granting, monitoring, and terminating ----- user accounts and the periodic revalidation of ----- user profiles by local security administrators.		X	X
CG-IT-05-012	-------- -- has not developed documented policies and procedures to restrict access to the UNIX operating system and for monitoring access, and periodic reviews are not performed to determine if monitoring of the UNIX operating system for---- - and ----- is functioning as intended.	Develop policies and procedures for restricting and monitoring access to the UNIX operating system for ----- and - - -- and perform periodic reviews to ensure the effectiveness of the monitoring process.		X	X
CG-IT-05-013	------------- Certification and Accreditations (C&A) for - - ------- -- --- ----- --- were not complete. Specifically, security testing and evaluations (ST&E) were incomplete and security plans had not been updated.	Update and complete the C&A process for ----- -------- - ---------- to include the completion of ST&Es and the update of security plans.		X	X
CG-IT-05-015	-------- -- has not implemented formal procedures for the periodic management review and monitoring activities of ----- database administrators and system administrators, or the Oracle SYS accounts.	Develop procedures for the regular and periodic monitoring of high-level ----- database administrator and system administrator activities, and the Oracle SYS account.	X		X

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
CG-IT-05-016	AppDetective identified vulnerabilities on the ----- database including weak passwords, excessive access permissions and missing patches.	Implement the individual fixes noted in the NFR for vulnerabilities identified and institute a formal process for performing periodic scans of the ------ - -- network environment, including the financial processing environment.		X	X
CG-IT-05-017	The Enterprise Security Management (ESM) tool identified configuration and account management weaknesses on -----	Implement the individual fixes noted in the NFR for vulnerabilities identified and institute a formal process for performing periodic scans of the ------ - -- network environment, including the financial processing environment.		X	X
CG-IT-05-018	Internet Security Systems Internet Scanner identified three hosts that were missing patches.	------ - -- management implemented immediate corrective action by removing the BrightStor agent from the three hosts.	X		X
CG-IT-05-021	Undelivered Orders – Transaction Codes: A report allowing users to review and manually re-establish obligations was not implemented as well as the manual review process.	Implement a system change request to automatically reestablish funds as obligated ------------------- ----- ---- ---- ------ -- are used, provide training to users, and require users to conduct reviews to determine when re-obligation to the associated UDO balances are required.		X	X
CG-IT-05-022	Disaster recovery plans for the Operations Service Center (OSC) Gold Business Systems, which include the ----------- ------ -------- ------) and --- --- ---- ----- - ----- ------ --------- --------- ------------ have not been completed.	Complete disaster recovery planning for the----------- -------- Gold Business Systems and periodically test disaster recovery and contingency plans.		X	X

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
CG-IT-05-023	----- has not completed a security plan for CMPlus 5.	Fully implement planned corrective actions to complete the security plan for CMPlus during the system's C&A process.		**X**	**X**
CG-IT-05-024	ESM identified high and medium level vulnerabilities on the ---------- production database over account management, configuration management, password management, and patch management.	Implement the individual fixes noted in the NFR for vulnerabilities identified and institute a formal process for performing periodic scans of the ----- network environment.		**X**	**X**
CG-IT-05-025	AppDetective found vulnerabilities on the -------- production database over audit management, configuration management, password management, and patch management.	Implement the individual fixes noted in the NFR for vulnerabilities identified and institute a formal process for performing periodic scans of the ----- network environment.		**X**	**X**
CG-IT-05-026	------ has initiated required changes on the application code on the server side. However the required update to the user workstations has not been completed.	Complete planned corrective actions for the redesign of CMPlus/FLS data interfaces to include functionality to communicate data interface errors back to the CMPlus unit/user by deploying the patch to implement the required fix to users on client workstations.		**X**	**X**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
CG IT-05-027	Implementation and management oversight of Coast Guard's information security program remains fragmented including communication and enforcement of procedures for security information with the ISSOs, enforce strong passwords and keep system security policies and procedures and C&A packages.	Implement and enforce procedures for obtaining system security information from ISSOs. Coast Guard management should ensure the implementation of corrective actions to improve system security policies and procedures regarding the C&A process, patch management, account management, monitoring of system software, and contingency planning. Also, implement a background investigation process for CG contractors and hire needed personnel.		**X**	**X**

Remaining IT NFRs Which Contributed to the Overall DHS Material Weakness for Financial System Security

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Remaining Findings Contributing to the Overall DHS Material Weakness for Financial System Security
CG-IT-05-004	User account maintenance procedures for ----- civilian personnel were not documented and access lists were not reviewed periodically and audit trails are not reviewed on a regular basis.	Document and implement account maintenance policies and procedures policies, perform periodic account reviews, and regularly monitor Direct Access audit trails.		**X**	**X**
CG-IT-05-005	The------ General Support System (GSS) Certification and Accreditation (C&A) not completed.	Complete the C&A package for the GSS in compliance with DHS and Federal guidance.		**X**	**X**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Remaining Findings Contributing to the Overall DHS Material Weakness for Financial System Security
CG-IT-05-014	Results of reviews over ------ user access were not available and documentation of periodic reviews was not on file at -------- --	Retain, as evidence, documentation of regular reviews performed of the Windows 2000 CG ------ directory to ensure that the list of users and permissions is accurate.		**X**	**X**
CG-IT-05-019	Formal procedures regarding access to the ------ - -- data center have not been established and implemented.	Develop and implement formal data center access procedures and a formalized method to track information system-related items entering and exiting the facility.	**X**		**X**

Department of Homeland Security
FY2005 Information Technology
Notification of Findings and Recommendations - Detail

- **Federal Emergency Management Agency**

Department of Homeland Security
FY2005 Information Technology
Notification of Findings and Recommendations - Detail

Federal Emergency Management Agency (FEMA)

Significant IT NFRs Which Contributed to the Overall DHS Material Weakness for Financial System Security

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
EPR-IT-05-05	Three systems do not have a Certification and Accreditation (C&A). Also, the ------- security test and evaluation (ST&E) did not provide adequate documentation of results, and six systems with completed C&As did not include ST&E documentation.	Complete the C&A accreditation packages for FEMA.gov and----- - adequately document the results of the--------- ST&E, complete documentation for the ST&Es performed on ------------ -- -------------- ---- ------ -- and --- --------- and re-perform the C&A process for ------ -- due to the major changes the system has undergone.		X	X
EPR-IT-05-08	The ------- Contingency Plan needs to adequately test the IT components of the system/process and the ------ -- Contingency Plan needs to be completed to take into account the new Linux Operating system and Small Business Administration web interface.	Perform a full test of the -- --- - Contingency Plan when the ----- ----- ------------ ------- is prepared to be the functional alternate site for Mt. Weather and update the ------ -- Contingency Plan once the ------ --- migration is complete. Conduct annual contingency plan testing.		X	X
EPR-IT-05-09	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.	Update the FEMA continuity of operations plan to incorporate clearly the order of the 12 critical IT systems that would be brought back online at the -------- ------- -------------- alternate processing site in the event of a disaster associated with ---- ----------		X	X

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
EPR-IT-05-10	ESM identified high and medium level vulnerabilities on ----- ------- --- that supports the -------- application including: account management, configuration management and patch management.	Implement the individual fixes listed in the NFR for the vulnerabilities identified and undertake an annual vulnerability assessment as prescribed in DHS guidance.		**X**	**X**
EPR-IT-05-11	Two Oracle databases were identified with weak/default passwords.	Implement the DHS password policy on all databases and consider the implementation of an automated password checking tool to help ensure that a strong password policy has been implemented		**X**	**X**
EPR-IT-05-12	Internet Scanner identified high risk vulnerabilities on 6 hosts in the following areas: configuration management, and password management.	Implement the individual fixes listed in the NFR for the vulnerabilities identified and undertake an annual vulnerability assessment as prescribed in DHS guidance.		**X**	**X**
EPR-IT-05-13	AppDetective identified high risk vulnerabilities in the following areas on the -------- database: account management, configuration management, password management, and patch management.	Implement the individual fixes listed in the NFR for the vulnerabilities identified and undertake an annual vulnerability assessment as prescribed in DHS guidance.	**X**		**X**
EPR-IT-05-14	Access to the Account Mapping Tables in ------ -- is excessive.	Develop and implement a solution to limit excessive access to the -------- account mapping function, reevaluate and limit access rights to those with a business need to access the -- -- -- account mapping functions, and routinely monitor the account mapping functions and related changes made.	**X**		**X**

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

Remaining IT NFRs Which Contributed to the Overall DHS Material Weakness for Financial System Security

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Remaining Findings Contributing to the Overall DHS Material Weakness for Financial System Security
EPR-IT-05-01	Policies and procedures do not exist to perform periodic review of [redacted] user access lists.	Develop and implement procedures regarding periodic review of access lists.		X	X
EPR-IT-05-02	[redacted] access controls suspend a user's session after fifteen minutes of inactivity. However, the option is not deactivated so users have the ability to deactivate the screensaver. Furthermore, users are not locked out after three unsuccessful logon attempts.	Disable users' ability to change the inactivity threshold or disable the password protected screensaver and ensure that [redacted] users are locked out of the system after three invalid logon attempts.		X	X
EPR-IT-05-03	The [redacted] had multiple weaknesses including lack of raised floors, and IFMIS production and test servers in close proximity.	Transfer all critical equipment out of the room in [redacted] to an alternate secure site with capabilities to house IT equipment on raised floors and upon implementation of the [redacted] "real-time" back-up facility, create redundant servers at the [redacted] for the two [redacted] servers located at the [redacted]		X	X

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Remaining Findings Contributing to the Overall DHS Material Weakness for Financial System Security
EPR-IT-05-04	The employee termination process for removing system access policies or processes for ensuring that all general support system and application access, including --- -- --, is removed in a timely manner for the separated employees is in draft form.	Ensure that FEMA Instruction 1540.3 is finalized, signed by the Under Secretary, promulgated to all EP&R employees, and enforced and per the instruction perform a review of authorized accounts on a semi-annual basis and remove terminated employees' access to all systems.		X	X
EPR-IT-05-06	Password protected screensaver properties are not disabled. Therefore, the current method of distributing of -- --- -- passwords is not sufficient.	Complete the implementation of ------ -- ----------- and disable the user's ability to change the inactivity threshold or disable the password protected screensaver.		X	X
EPR-IT-05-07	Insufficient documentation exists to fully explain ----- -- functions and user access capabilities associated with those functions.	Enhance system documentation supporting the description of the -------- user functions, with their associated system capabilities and develop and implement procedures to update the documentation as functions are added or modified.		X	X

Department of Homeland Security
FY2005 Information Technology
Notification of Findings and Recommendations – Detail

- **Consolidated**

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

Department of Homeland Security
FY2005 Information Technology
Notification of Findings and Recommendations – Detail

Consolidated

Significant IT NFRs Which Contributed to the Overall DHS Material Weakness for Financial System Security

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
CONS-IT-05-02	DHS administrators do not consistently require new users to complete the ------ new user access form before granting access to ------ .	Ensure that - ---- user access is only granted upon completion of the TIER new user access request form and evidence of supervisory authorization. In addition, the access request forms should be retained for at least one year.	**X**		**X**
CONS-IT-05-03	No policies and procedures are in place to periodically review -------user access lists to determine if access is still needed and a documented process has not been established to notify--------administrators of terminated or transferred personnel.	Develop and implement policies and procedures for the periodic review of ------ access lists and develop and implement policies and procedures to promptly notify the -- ---- administrators of the termination or transfer of personnel with access.	**X**		**X**
CONS-IT-05-04	Informal processes are followed for making changes to ------ -------- and -------- ----- does not have a version manager tool for template changes made to the application.	Develop and implement a detailed SDLC or configuration management procedures for performing changes over ---------- ------- template process and implement a version manager tool in order to maintain previous versions of-- - ----- --- - reports.	**X**		**X**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
CONS-IT-05-05	------ configuration management controls can be improved including lead developers that have access to production, segregation of duties issues exist for system changes made outside of the schedule ------ quarterly releases, all system change requests (SCR) are not documented, and test documentation is not maintained.	Improve configuration management controls, ensure adherence with the Department of Treasury SCM and ASSC SDLC Workflow and Processes Handbook throughout DHS as they relate to opening an SCR, and maintain test documentation for changes implemented outside of the scheduled - -- -- quarterly releases.	**X**		**X**
CONS-IT-05-06	Discrepancies exist between the DHS Performance and Accountability Report (PAR) Guidance and the Analytical Report.	Implement recommended actions in order to make the analytic report code, equations, and PAR guide consistent and develop and implement a configuration management process over analytic report changes.	**X**		**X**
CONS-IT-05-07	Discrepancies Exist Between the United States Standard General Ledger (USSGL) and the DHS Standard General Ledger (DHS SGL) account classifications used to populate the Abnormal Balances Report.	Implement changes to the DHS SGL normal balance accounts for compliance with the USSGL and develop a procedure to verify the abnormal balance report logic after any changes in the DHS SGL or USSGL.	**X**		**X**
CONS-IT-05-08	No documented procedures are in place for DHS components to perform a formal review, by a separate approving individual, of financial data before moving the - ---- file from the Holding Area into the ------- Repository.	Document and implement procedures for DHS components to perform a formal review of financial data before moving it into the ------ Repository.	**X**		**X**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
CONS-IT-05-09	Lack of compliance with FISMA in the areas of access controls, entity-wide security program planning and management, application software development and change control, system software, segregation of duties, and service continuity.	The DHS Chief Information Officer (CIO), in coordination with the DHS Office of the Chief Financial Officer (OCFO) and other DHS functional leaders should ensure further emphasis on the monitoring and enforcement of policies and procedures through the performance of periodic security control assessments and audits.		**X**	**X**

Remaining IT NFRs Which Contributed to the Overall DHS Material Weakness for Financial System Security

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Remaining Findings Contributing to the Overall DHS Material Weakness for Financial System Security
CONS-IT-05-01	Treasury personnel access to DHS- - ---- ---- -- -- --- ------------------- ---- - ------ --------- continues to be excessive.	Reevaluate ------ privileges assigned to Department of Treasury users, and restrict user account permissions to only the minimum privileges necessary to achieve the principle of least privilege.		**X**	**X**

Department of Homeland Security
FY2005 Information Technology
Notification of Findings and Recommendations - Detail

- ## Office of State and Local Government Coordination and Preparedness (SLGCP)

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

Department of Homeland Security
FY2005 Information Technology
Notification of Findings and Recommendations – Detail

State and Local Government Coordination and Preparedness (SLGCP)

Significant IT NFRs Which Contributed to the Overall DHS Material Weakness for Financial System Security

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
SLGCP-2005-06	IT control environment of the Department of Justice Office of Justice Programs (OJP) needs strengthening over access controls, change controls, service continuity, and system software.	Implement a Memorandum of Understanding (MOU) agreement to include the minimum-security related responsibilities and continue to work with OJP to ensure all weaknesses that impact SLGCP's reliance on the OJP IT control environment are mitigated and corrected.	X		X
SLGCP-2005-12	Segregation of duties is not properly enforced. The SLGCP has not formed a separate Information Systems department and has yet to develop policies or procedures outlining segregation of duties controls or procedures.	Continue to finalize the policies and procedures that address segregation of duties for SLGCP information systems functions and create an Information Systems department that is responsible for all security and network administration of SLGCP systems.		X	X
SLGCP-2005-13	Application user accounts are not removed in a timely manner after user separation.	Improve the process for notifying the Security Officer or Administrator of employee or contractor transfers/terminations so that system access to the [redacted] and [redacted]s removed in a more timely manner.		X	X

Department of Homeland Security
FY2005 Information Technology
Notification of Findings and Recommendations – Detail

- **Transportation Security Administration**

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

Department of Homeland Security
FY2005 Information Technology
Notification of Findings and Recommendations – Detail

Transportation Security Administration

Significant IT NFRs Which Contributed to the Overall DHS Material Weakness for Financial System Security

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
TSA-IT-05-003	[redacted] Unix change control process supporting [redacted]) and [redacted] have weaknesses including: procedures in support of the finalized CM policy are not developed, documentation supporting a risk assessment is not maintained, formal change requests are not used, and test plans and test results are not documented.	TSA management should work with-[redacted] management to ensure the development and enforcement of configuration management procedures for developing test plans, documenting test results, implementing software, management approval of system changes, and retention of risk assessment and testing documentation.	X		X
TSA-IT-05-004	Service continuity weaknesses for [redacted] including outdated Business Continuity Contingency Plan (BCCP), lack of disaster recovery procedure details, an off-site storage location in close proximity to the data center, and lack of BCCP testing exist.	TSA management should work with [redacted] management to ensure the periodic reassessment and, as appropriate, revision of the [redacted] BCCP, development of disaster recovery procedures for [redacted] completion of the relocation of the off-site storage location, and periodic testing of the BCCP.	X		X

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
TSA-IT-05-005	No documented procedures exist for controlling the processes associated with the granting, monitoring, and termination of user accounts within------ have not been documented.	TSA management should work with - --------- management to ensure the development of formal entity wide procedures for granting, monitoring, and terminating ----- user accounts and periodic revalidation of------ user profiles by local security administrators.	X		X
TSA-IT 05-006	-------- -- has not developed documented policies and procedures to restrict access to the UNIX operating system, for monitoring access, and periodic reviews are not performed to determine if monitoring of the UNIX operating system for---- - -- ------- is functioning as intended.	TSA management should work with - --------- management to ensure the development of policies and procedures for restricting and monitoring access to the UNIX operating system for ------- - --- - -- and performance of period reviews of the monitoring process.	X		X
TSA-IT 05-007	Certification and Accreditations (C&A) for the ---- -- --- -------------- ---- ---- ----- --- -- ---- ---- - -------- - -------- were not complete. Specifically, security testing and evaluations (ST&Es) were incomplete and security plans had not been updated.	TSA management should work with - --------- management to ensure the update and completion of the C&A process for --- ---- ------ --- - ------ to include the completion of ST&Es, and the update of security plans.	X		X
TSA-IT-05-008	-------- -- has not implemented formal procedures for the periodic management review and monitoring of activities of ----- database administrators and system administrators or the Oracle SYS accounts.	TSA management should work with-- --------- management to ensure the development of procedures for the regular and periodic monitoring of high-level ----- database administrator and system administrator activities, and the -------- ----------------	X		X

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Significant Findings Contributing to the Overall DHS Material Weakness for Financial System Security
TSA-IT-05-009	The Enterprise Security Management tool identified world writeable directories without a sticky bit set, and account management weaknesses over DART.	TSA management should work with - --------- management to ensure the implementation of the individual fixes noted in the NFR for vulnerabilities identified and the institution of a formal process for performing periodic scans of the -- ----- -- network environment, including the financial processing environment.	X		X
TSA-IT-05-010	AppDetective identified vulnerabilities on the ----- database including weak passwords, excessive access permissions and missing patches.	TSA management should work with - --------- management to ensure the implementation of the individual fixes noted in the NFR for vulnerabilities identified and institution of a formal process for performing periodic scans of the -- ----- -- network environment, including the financial processing environment.	X		X
TSA-IT-05-011	Internet Security Systems Internet Scanner identified three hosts that were missing patches.	------ - -- management implemented immediate corrective action by removing the BrightStor agent from the three hosts.	X		X
TSA-IT 05-012	Inaccuracies exist within TSA personnel records which addresses both separated employee issue and other erroneous personnel records.	TSA management should ensure that personnel errors regarding separated employees cited during the prior year audit are corrected and documentation of corrective actions retained on file.		X	X

Remaining IT NFRs Which Contributed to the Overall DHS Material Weakness for Financial System Security

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Remaining Findings Contributing to the Overall DHS Material Weakness for Financial System Security
TSA-IT 05-001	Formal procedures regarding access to the [redacted] have not been established and implemented.	TSA management should work with [redacted] management to ensure the development and implementation of formal data center access procedures and a formalized method to track information system-related items entering and exiting the facility.	X		X

Appendix C

Status of Prior Year Notices of Findings and Recommendations And Comparison To Current Year Notices of Findings and Recommendations

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
USCIS	04-09	Access control weaknesses were identified in the---- ----- -------- and were not documented as part of the Certification and Accreditation (C&A) package.		05-04
USCIS	04-10	--------- users at the Vermont Service Center have the ability to adjudicate applications as well as process payments, which are considered incompatible duties.	**X**	
USCIS	04-18	USCIS does not have procedures in place to periodically review ------ ------ --- - ----------- - --- ----------------- - user access lists and could not provide a list of all authorized-------- users upon request.	**X**	
USCIS	04-19	------ ---------- at the Vermont Service Center have ability to adjudicate applications as well as process payments, which are considered incompatible duties.	**X**	
USCIS	04-21	Interface controls to ensure that data transmitted by the lockbox operation is accurately uploaded into the National Business Center's -- ---- ---------- --- --- ------- - --- ----- database need improvement.	**X**	
USCIS	04-27	The site C&A package for the California Service Center has expired.		05-02
ICE	04-17	Access control weaknesses were identified in the ---- ---- ----- ---- -- - -------- ------ - ----- .	**X**	
ICE	04-18	ICE does not have procedures in place to periodically review -------- ----- ----- --- ----------- - - - - ---- ----- user access lists and could not provide a list of all authorized-------- users upon request.		05-07
CBP	04-01	Nineteen individual user accounts on the ------ - -------- -------- mainframe security software had excessive privileges assigned to them.		05-02
CBP	04-02	Weaknesses in the C&A process for the --- -- -- - ------------------ -------- ----- - - lack of evaluation of the need for a separate C&As for applications included in the Administrative Applications C&A, the and improvements needed in risk assessment guidance.		05-23
CBP	04-03	Weaknesses in disaster recovery testing and continuity of critical operational functions for the ----- and the --------- -- ------- - -- - --------- -- - - ----- ------- - - at the alternate processing site.	**X**	
CBP	04-04	Excessive sensitive functions and high-risk combinations have been assigned to ACS users.		05-18
CBP	04-05	Certain controls can be overridden in ------ without supervisory approval.		05-04
CBP	04-06	Excessive access has been granted to ------ ------- - --------- - ----- -- -------------- ---- -- - ----- --- -- ------ -- ---------- ---- - ---- ----- ---------	**X**	
CBP	04-07	Weaknesses in the C&A process at field sites.		05-31
CBP	04-08	Improvements are needed in system logical access controls over network assets affecting headquarters and the----- - --- -------- ------		05-09
CBP	04-09	Interconnection Security Agreements (ISA) are not documented for 92 partners that connect with ----- .		05-11
CBP	04-10	Access is not appropriately restricted to ----- - vendor and bank tables.		05-29

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
CBP	04-11	Weaknesses with the [redacted] Risk Assessment.	X	
CBP	04-12	Improvements needed in restricting access to sensitive system level transactions through the On-Line Transaction Processing System Security [redacted]		05-28
CBP	04-13	[redacted] segregation of duties issues were identified with several users.		05-01
CBP	04-14	The incident handling and response capability needs improvement regarding incident detection and initiation, response, recovery, and closure.		05-16
CBP	04-15	Audit logs are not appropriately monitored for the [redacted].	X	
CBP	04-16	Weaknesses in the access control process for the [redacted] Materials Management.		05-05
CBP	04-17	System access, user account management, and configuration weaknesses identified with the [redacted] general controls environment for materials management module.		05-09
CBP	04-18	Least privilege principles are not appropriately enforced for mainframe user groups' access to sensitive datasets/utilities.		05-30
CG	04-001	Excessive access privileges were granted to the [redacted] Financial Reporting System.		05-014
CG	04-002	The [redacted] User Guide is outdated.	X	
CG	04-003	Comprehensive policies for conducting personnel suitability investigations or records to support the results of personnel suitability investigations do not exist.		05-006
CG	04-004	No documented procedures exist requiring local site administrators to control access to [redacted] 17 user accounts have not been appropriately removed for terminated employees, and local site administrators do not periodically revalidate user accounts.		05-011
CG	04-005	No documented policies and 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.		05-012
CG	04-006	Weaknesses associated with the UNIX system software change control process.		05-010
CG	04-007	Outdated and incomplete security plans, and C&As not performed for the [redacted].		05-013
CG	04-008	Service continuity weaknesses for the [redacted] including outdated Business Continuity Contingency Plan (BCCP), lack of disaster recovery procedure details, an off-site storage location in close proximity to the data center, and lack of BCCP testing.		05-009
CG	04-009	[redacted] and CMPlus interface errors are not automatically communicated back to the corresponding CMPlus unit/user.		05-026

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
CG	04-010	The security plans for the [redacted] are not in compliance with criteria.	X	
CG	04-011	CMPlus passwords do not automatically expire, CMPlus accounts are not locked out after successive invalid login attempts, and a documented CMPlus system security plan does not exist.		05-023
CG	04-012	The Operations Service Center (OSC) has not implemented a disaster recovery plan.		05-022
CG	04-013	Entity wide security program planning is not in place for the Personnel Service Center (PSC).		05-005
CG	04-014	Weaknesses exist regarding PSC service continuity and resource classifications.		05-001
CG	04-015	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.		05-003, 05-004, 05-008
CG	04-016	Documented procedures do not exist at PSC to enforce segregation of duties principles.	X	
CG	04-017	Database Scanner identified vulnerabilities on the Supply Center Computer Replacement (SCCR) database supporting [redacted].		05-025
CG	04-018	The Enterprise Security Manager (ESM) tool identified high and medium level vulnerabilities on three hosts supporting [redacted]		05-024
CG	04-019	Database Scanner identified vulnerabilities on the [redacted]		05-016
CG	04-020	ESM identified high and medium level vulnerabilities on three hosts supporting [redacted]		05-017
CG	04-021	Change control weaknesses exist at the PSC, including lack of documented test plans, test results, and software modification audit trails.		05-002
CG	04-022	Several network-based vulnerabilities were identified on the external Information Technology resources for Coast Guard.	X	
CG	04-023	Weaknesses were self-identified by Coast Guard on two hosts supporting the [redacted] and were not subsequently addressed.	X	
CG	04-024	Implementation and management oversight of Coast Guard's information security program remains fragmented.		05-027
CG	04-025	Interface controls do not ensure that record counts match as data is transferred from [redacted] into CheckFree.	X	
CG	04-026	Three of the four Database Administrators at [redacted] also have System Administrator rights and responsibilities.	X	
CG	04-063	Undelivered Orders – Transaction Codes: A report allowing users to review and manually re-establish obligation was not implemented as well as the manual review process. (prior year Financial Notice of Finding and Recommendation)		05-021
CONS	04-01	Excessive [redacted] system privileges were granted and a documented process does not exist to notify [redacted] application administrators of user termination or transfer		05-01

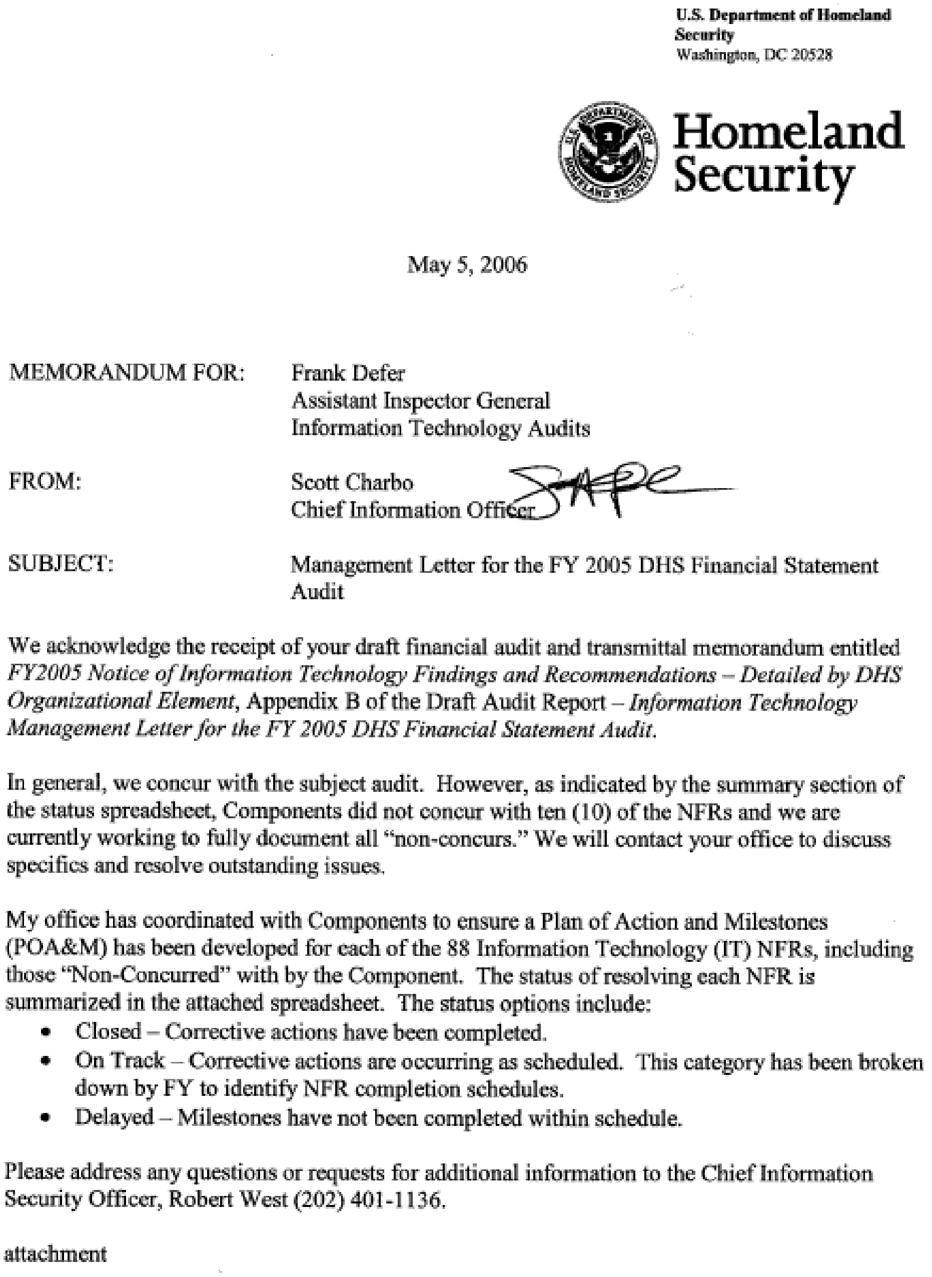
			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		for timely removal of system access.		
CONS	04-02	The interagency agreement between DHS and [redacted] does not describe the information security controls that need to be implemented and managed by the data owner (DHS) or the system operator (Treasury).	**X**	
CONS	04-03	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.		05-09
EPR	04-11	Policies and procedures do not exist to perform period review of [redacted] user access lists.		05-01
EPR	04-16	[redacted] access controls do not appropriately suspend a user's session after ten minutes of activity and user are not locked out after three unsuccessful logon attempts.		05-02
EPR	04-17	The [redacted] had multiple weaknesses including lack of raised floors, production and test servers in close proximity, lack of review of physical user access lists, and no procedures to periodically change keypad combinations.		05-03
EPR	04-18	Lack of consistent policies or processes for ensuring that all general support system and application access, including [redacted], is timely removed for terminated employees.		05-04
EPR	04-19	Seven critical systems do not have a C&A.		05-05
EPR	04-20	No documented process for generating or communicating new or reset [redacted] passwords to users.		05-06
EPR	04-21	[redacted] Table audit trail data is not reviewed periodically.	**X**	
EPR	04-22	Insufficient documentation exists to fully explain [redacted] functions and user access capabilities associated with those functions.		05-07
EPR	04-23	The ESM tool identified several high and medium level technical vulnerabilities on the [redacted]		05-10
EPR	04-24	Oracle databases, including the [redacted] production and development databases, contained weak or default passwords.		05-11
EPR	04-25	The [redacted] tool identified 88 technical vulnerabilities on 13 different FEMA hosts, the majority of which related to missing patches.		05-12
EPR	04-28	The Intra-governmental Payment 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.	**X**	
EPR	04-32	The Continuity of Operations Plans (COOP) for [redacted] are in draft.		05-08
EPR	04-35	[redacted] has not documented interagency agreements for alternate	**X**	

Department of Homeland Security
Information Technology Management Letter
September 30, 2005

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		data processing and telecommunication facilities in the event of a disaster.		
EPR	04-39	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.		05-09
LTD	04-01	Incident response policies and procedures are not in place and/or finalized for the FLETC---------- -------------------------------- .	**X**	
SLGCP	04-05	A system owner and security manager has not been identified to track background investigations and personnel clearances.	**X**	
SLGCP	04-06	A Service Level Agreement (SLA) is not in place with the third party hosting the Data Collection Toolkit (DCT).	**X**	
SLGCP	04-07	A documented security awareness training program is not in place.	**X**	
SLGCP	04-08	Segregation of duties is not properly enforced and documented policies outlining segregation of duties controls or procedures do not exist.		2005-12
SLGCP	04-09	Access privileges and profiles for the ------------------ --- - -- ------------ ------------------- ----- ---------- internal users are not properly administered, resulting in an unnecessary number of users with the ability to update the vendor table.	**X**	
SLGCP	04-10	Application user accounts are not removed in a timely manner after user separation.		2005-13
SLGCP	04-22	A C&A does not exist for the ------------ --------- -- -----	**X**	
SLGCP	04-25	The reconciliation process for financial transactions that occurred between ------- and the--- ---- ------------------- was not fully implemented throughout the fiscal year.	**X**	
SLGCP	04-26	The ----- - - --- ------- ---- ----- captured transactions but did not capture user activity for three months of the fiscal year.	**X**	
TSA	04-01	Segregation of duties is not properly enforced in the ------- ------------ - within---------	**X**	
TSA	04-02	Weaknesses in -------- access controls, network security, and system security controls.	**X**	
TSA	04-03	System financial integrity issues identified in the ------ application.	**X**	
TSA	04-04	Inaccuracies exist within TSA personnel records which addresses both separated employee issue and other erroneous personnel records		05-12

Appendix D

Management Response to Draft IT Management Letter



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

Homeland
Security

May 5, 2006

MEMORANDUM FOR: Frank Defer
Assistant Inspector General
Information Technology Audits

FROM: Scott Charbo
Chief Information Officer

SUBJECT: Management Letter for the FY 2005 DHS Financial Statement Audit

We acknowledge the receipt of your draft financial audit and transmittal memorandum entitled *FY2005 Notice of Information Technology Findings and Recommendations – Detailed by DHS Organizational Element*, Appendix B of the Draft Audit Report – *Information Technology Management Letter for the FY 2005 DHS Financial Statement Audit.*

In general, we concur with the subject audit. However, as indicated by the summary section of the status spreadsheet, Components did not concur with ten (10) of the NFRs and we are currently working to fully document all "non-concurs." We will contact your office to discuss specifics and resolve outstanding issues.

My office has coordinated with Components to ensure a Plan of Action and Milestones (POA&M) has been developed for each of the 88 Information Technology (IT) NFRs, including those "Non-Concurred" with by the Component. The status of resolving each NFR is summarized in the attached spreadsheet. The status options include:

- Closed – Corrective actions have been completed.
- On Track – Corrective actions are occurring as scheduled. This category has been broken down by FY to identify NFR completion schedules.
- Delayed – Milestones have not been completed within schedule.

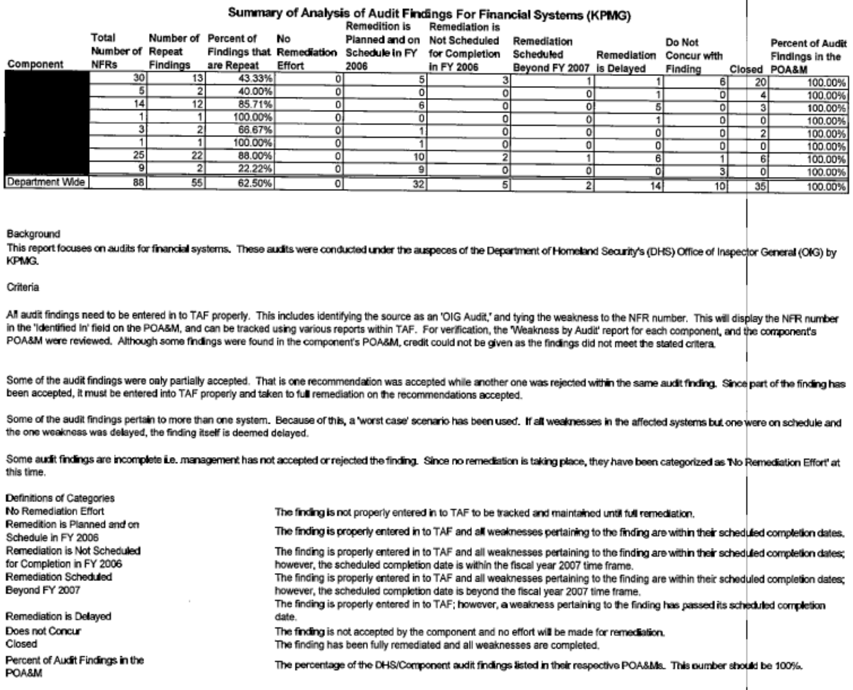
Please address any questions or requests for additional information to the Chief Information Security Officer, Robert West (202) 401-1136.

attachment

Department of Homeland Security

Information Technology Management Letter

September 30, 2005



Summary of Analysis of Audit Findings For Financial Systems (KPMG)

Component	Total Number of NFRs	Number of Repeat Findings	Percent of Findings that are Repeat	No Remediation Effort	Remedition is Planned and on Schedule in FY 2006	Remediation is Not Scheduled for Completion in FY 2006	Remediation Scheduled Beyond FY 2007	Remediation is Delayed	Do Not Concur with Finding	Closed	Percent of Audit Findings in the POA&M
[redacted]	30	13	43.33%	0	5	3	1	1	6	20	100.00%
[redacted]	5	2	40.00%	0	0	0	0	1	0	4	100.00%
[redacted]	14	12	85.71%	0	6	0	0	5	0	3	100.00%
[redacted]	1	1	100.00%	0	0	0	0	1	0	0	100.00%
[redacted]	3	2	66.67%	0	1	0	0	0	0	2	100.00%
[redacted]	1	1	100.00%	0	1	0	0	0	0	0	100.00%
[redacted]	25	22	88.00%	0	10	2	1	6	1	6	100.00%
[redacted]	9	2	22.22%	0	9	0	0	0	3	0	100.00%
Department Wide	88	55	62.50%	0	32	5	2	14	10	35	100.00%

Background

This report focuses on audits for financial systems. These audits were conducted under the auspeces of the Department of Homeland Security's (DHS) Office of Inspector General (OIG) by KPMG.

Criteria

All audit findings need to be entered in to TAF properly. This includes identifying the source as an 'OIG Audit,' and tying the weakness to the NFR number. This will display the NFR number in the 'Identified In' field on the POA&M, and can be tracked using various reports within TAF. For verification, the 'Weakness by Audit' report for each component, and the component's POA&M were reviewed. Although some findings were found in the component's POA&M, credit could not be given as the findings did not meet the stated critera.

Some of the audit findings were only partially accepted. That is one recommendation was accepted while another one was rejected within the same audit finding. Since part of the finding has been accepted, it must be entered into TAF properly and taken to full remediation on the recommendations accepted.

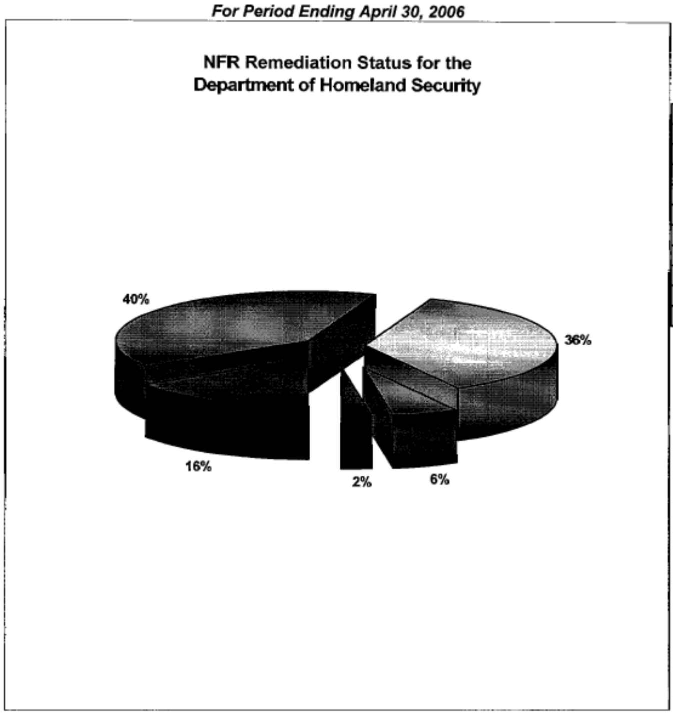
Some of the audit findings pertain to more than one system. Because of this, a 'worst case' scenario has been used. If all weaknesses in the affected systems but one were on schedule and the one weakness was delayed, the finding itself is deemed delayed.

Some audit findings are incomplete i.e. management has not accepted or rejected the finding. Since no remediation is taking place, they have been categorized as 'No Remediation Effort' at this time.

Definitions of Categories	
No Remediation Effort	The finding is not properly entered in to TAF to be tracked and maintained until full remediation.
Remedition is Planned and on Schedule in FY 2006	The finding is properly entered in to TAF and all weaknesses pertaining to the finding are within their scheduled completion dates.
Remediation is Not Scheduled for Completion in FY 2006	The finding is properly entered in to TAF and all weaknesses pertaining to the finding are within their scheduled completion dates; however, the scheduled completion date is within the fiscal year 2007 time frame.
Remediation Scheduled Beyond FY 2007	The finding is properly entered in to TAF and all weaknesses pertaining to the finding are within their scheduled completion dates; however, the scheduled completion date is beyond the fiscal year 2007 time frame.
Remediation is Delayed	The finding is properly entered in to TAF; however, a weakness pertaining to the finding has passed its scheduled completion date.
Does not Concur	The finding is not accepted by the component and no effort will be made for remediation.
Closed	The finding has been fully remediated and all weaknesses are completed.
Percent of Audit Findings in the POA&M	The percentage of the DHS/Component audit findings listed in their respective POA&Ms. This number should be 100%.

NFR Remedation Status for Fiscal Year 2005

For Period Ending April 30, 2006



NFR Remediation Status for the Department of Homeland Security

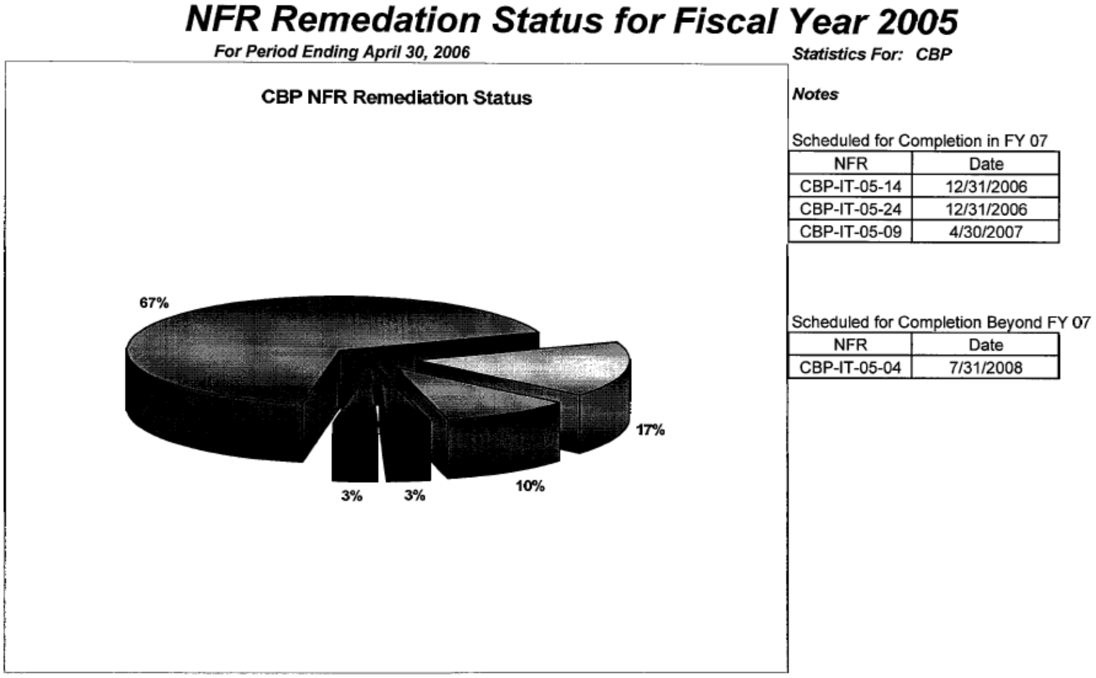
Statistics For: *DHS*

Component	*On Track FY 06*	*On Track FY 07*	*Beyond FY 07*	*Delayed*	*Closed*
			Status		
CBP	5	3	1	1	20
CIS	0	0	0	1	4
EPR	6	0	0	5	3
ICE	0	0	0	1	0
SLGCP	1	0	0	0	2
TSA	1	0	0	0	0
USCG	10	2	1	6	6
Consolidated	9	0	0	0	0
DHS	32	5	2	14	35
Percentage	36.4%	5.7%	2.3%	15.9%	39.8%
Total					88

Notes:

USCG and Consolidated / CFO have a high number of NFRs scheduled for completion on Sept 29, or Sept 30, 2006.

Department of Homeland Security
Information Technology Management Letter
September 30, 2005



NFR Remedation Status for Fiscal Year 2005

For Period Ending April 30, 2006

Statistics For: CBP

CBP NFR Remediation Status

Notes

Scheduled for Completion in FY 07

NFR	Date
CBP-IT-05-14	12/31/2006
CBP-IT-05-24	12/31/2006
CBP-IT-05-09	4/30/2007

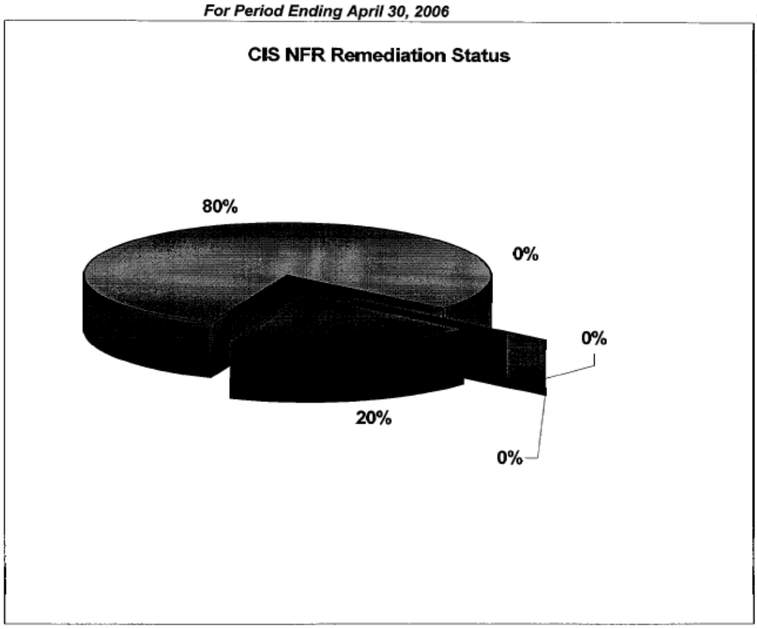
Scheduled for Completion Beyond FY 07

NFR	Date
CBP-IT-05-04	7/31/2008

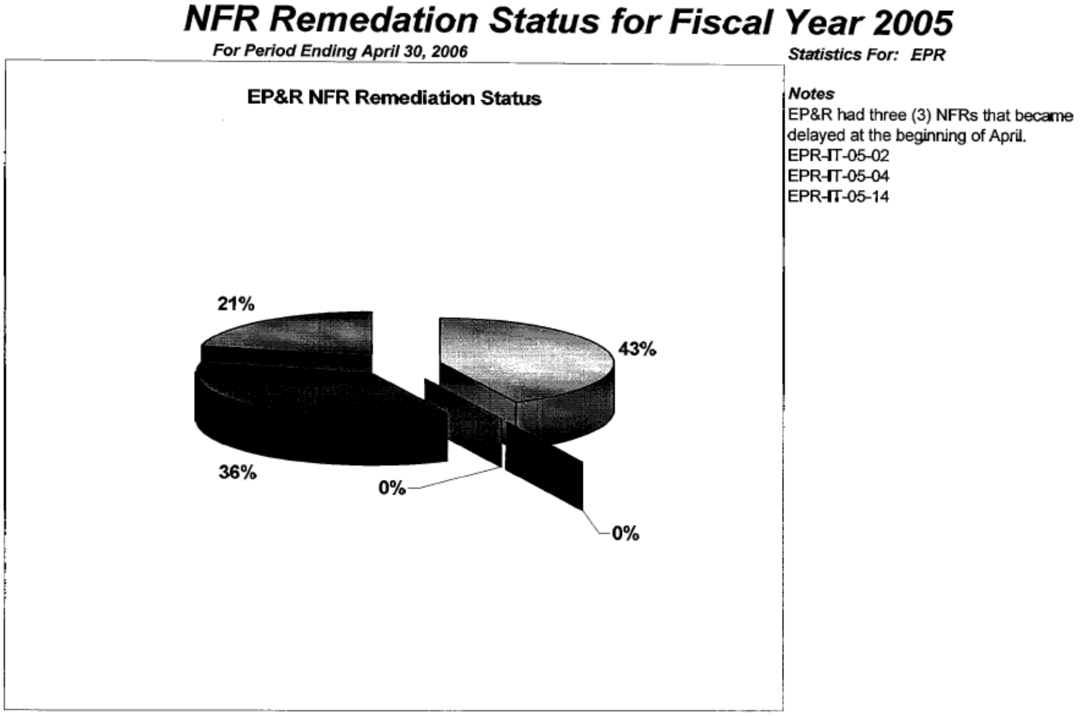
NFR Remedation Status for Fiscal Year 2005

For Period Ending April 30, 2006

Statistics For: CIS



Notes
CIS has one (1) NFR which is delayed, CIS-IT-05-04.



NFR Remedation Status for Fiscal Year 2005

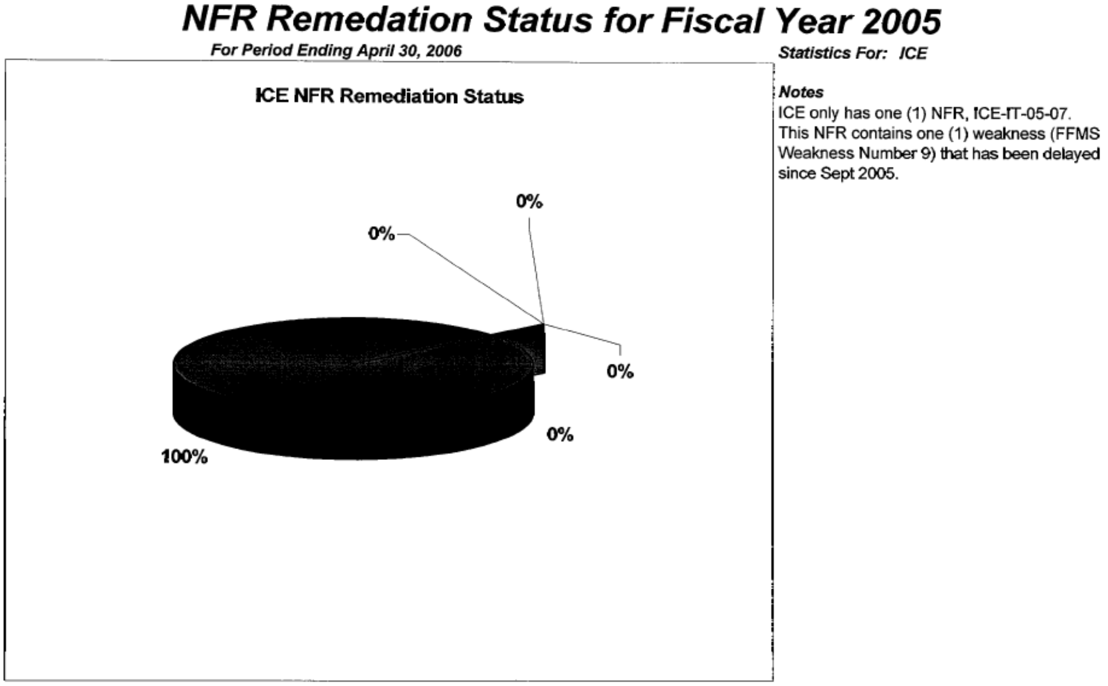
For Period Ending April 30, 2006

Statistics For: EPR

EP&R NFR Remediation Status

Notes

EP&R had three (3) NFRs that became delayed at the beginning of April.
EPR-IT-05-02
EPR-IT-05-04
EPR-IT-05-14



NFR Remedation Status for Fiscal Year 2005

For Period Ending April 30, 2006

Statistics For: ICE

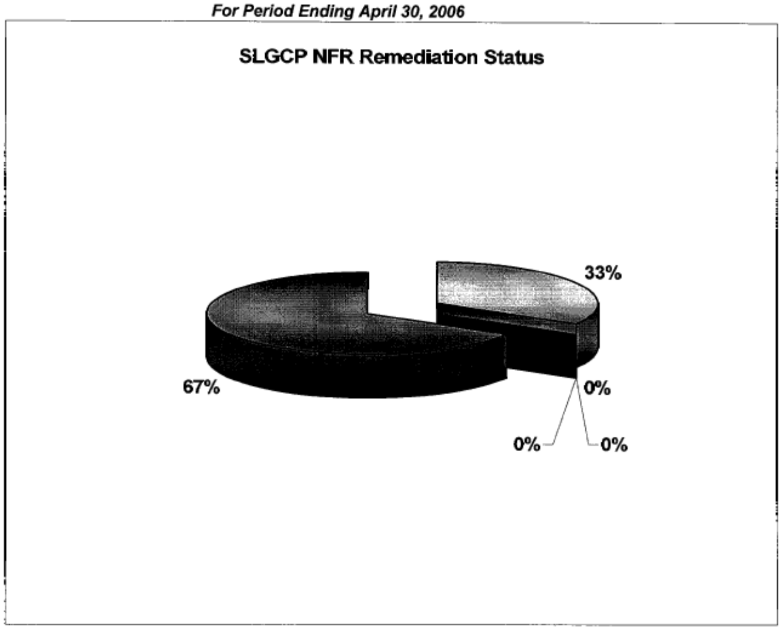
ICE NFR Remediation Status

Notes
ICE only has one (1) NFR, ICE-IT-05-07. This NFR contains one (1) weakness (FFMS Weakness Number 9) that has been delayed since Sept 2005.

NFR Remedation Status for Fiscal Year 2005

For Period Ending April 30, 2006

Statistics For: SLGCP

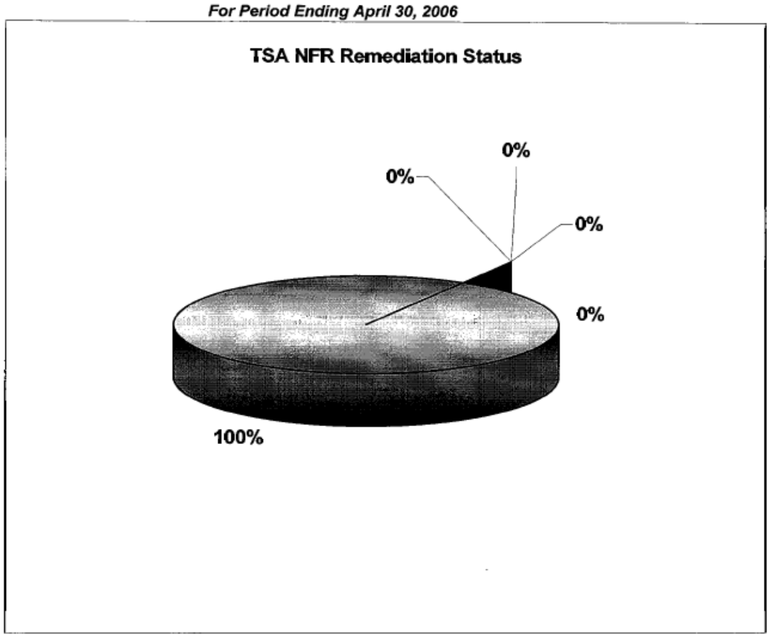


Notes
SLGCP-2005-06 is scheduled for completion June 30, 2006. It contains weaknesses that do not have milestones.

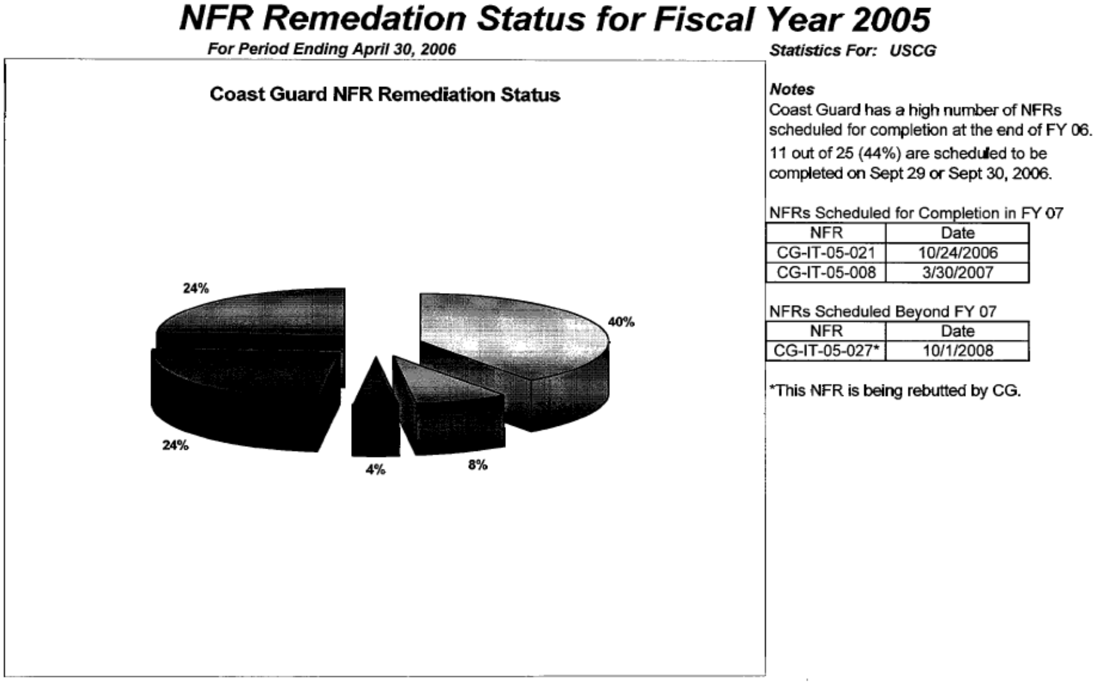
NFR Remedation Status for Fiscal Year 2005

For Period Ending April 30, 2006

Statistics For: TSA



Notes
TSA has only one (1) finding, TSA-IT-05-012. It is scheduled to be completed on July 24, 2006.



NFR Remedation Status for Fiscal Year 2005

For Period Ending April 30, 2006

Statistics For: USCG

Coast Guard NFR Remediation Status

Notes

Coast Guard has a high number of NFRs scheduled for completion at the end of FY 06. 11 out of 25 (44%) are scheduled to be completed on Sept 29 or Sept 30, 2006.

NFRs Scheduled for Completion in FY 07

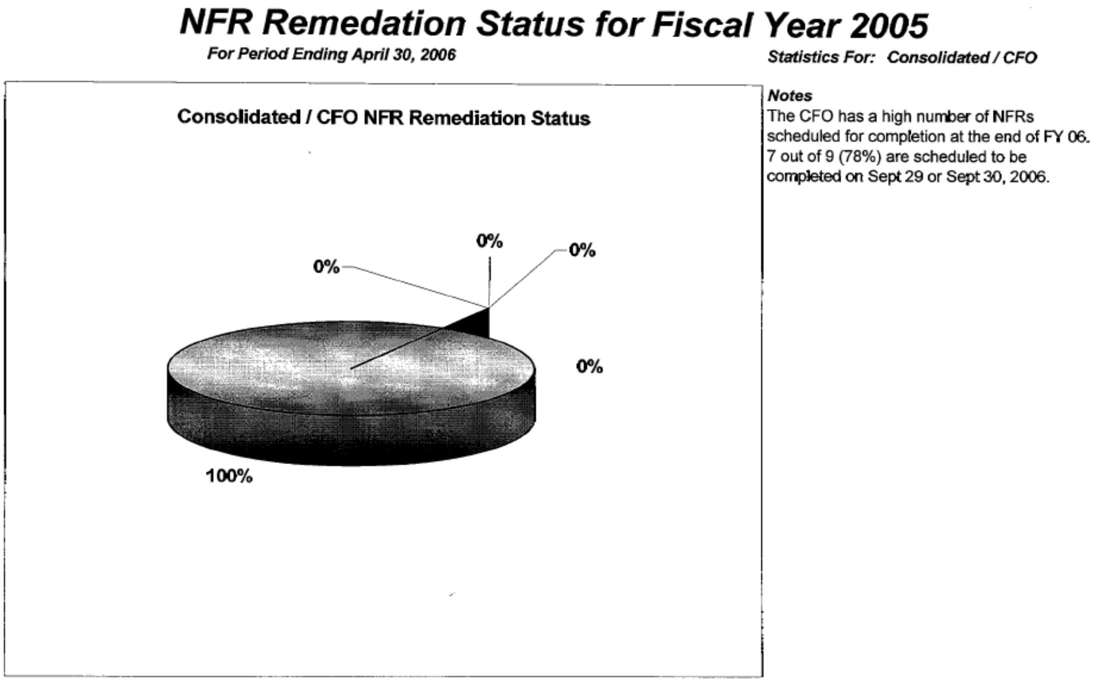
NFR	Date
CG-IT-05-021	10/24/2006
CG-IT-05-008	3/30/2007

NFRs Scheduled Beyond FY 07

NFR	Date
CG-IT-05-027*	10/1/2008

*This NFR is being rebutted by CG.

Department of Homeland Security
Information Technology Management Letter
September 30, 2005



NFR Remedation Status for Fiscal Year 2005

For Period Ending April 30, 2006

Statistics For: Consolidated / CFO

Consolidated / CFO NFR Remediation Status

Notes
The CFO has a high number of NFRs scheduled for completion at the end of FY 06. 7 out of 9 (78%) are scheduled to be completed on Sept 29 or Sept 30, 2006.

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Chief of Staff
Deputy Chief of Staff
Executive Secretary
Under Secretary, Management
Chief Information Officer
Chief Financial Officer
Chief Information Security Officer
Assistant Secretary, Public Affairs
Assistant Secretary, Legislative and Intergovernmental Affairs
Assistant Secretary, Policy
DHS Audit Liaison
Chief Information Officer, Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

Additional Information and Copies

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

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or email DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.