DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Information Technology Management Letter for the FY 2006 DHS Financial Statement Audit (Redacted)

Notice: The Department of Homeland Security, Office of Inspector General, has redacted this report for public release. A review under the Freedom of Information Act will be conducted upon request.

OIG-07-53 June 2007

Office of Inspector General

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

Homeland Security

June 20, 2007

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' financial statement audit as of September 30, 2006. 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-07-10, November 2006) and represents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit of DHS' FY 2006 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated December 15, 2006, 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, 2006

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 balance sheet and statement of custodial activity of the U.S. Department of Homeland Security (DHS) as of September 30, 2006. We were not engaged to audit the consolidated statements of net cost, changes in net position, and financing, and combined statement of budgetary resources for the year ended September 30, 2006. Because of matters discussed in our *Independent Auditors' Report*, dated November 15, 2006, 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 or the statement of custodial activity for the year ended September 30, 2006.

In connection with our fiscal year 2006 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 the consolidated balance sheet. Our procedures did 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 on the next page, and presented for your consideration in the sections that follow. 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 15, 2006, 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, 2006.

As described above, the scope of our work was not sufficient to express an opinion on the balance sheet or statement of custodial activity of DHS as of September 30, 2006, and we were not engaged to audit the statements of net cost, changes in net position, and financing, and combined statement of budgetary

As described above, the scope of our work was not sufficient to express an opinion on the balance sheet or statement of custodial activity of DHS as of September 30, 2006, and we were not engaged to audit the statements of net cost, changes in net position, and financing, and combined statement of budgetary resources for the year ended September 30, 2006. 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, 2006 balance sheet and statement of custodial activity, and had we been engaged to audit the other fiscal year 2006, 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

We performed an audit of DHS IT general controls in support of the FY 2006 DHS balance sheet and statement of custodial activity audit 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, we 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 focused

on test, development, and production devices that directly support DHS financial processing and key general support systems.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

Material weaknesses are reportable conditions in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements caused by error or fraud, in amounts that would be material in relation to the balance sheet or statement of custodial activity being audited, may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. Because of inherent limitations in internal control, misstatements due to error or fraud may nevertheless occur and not be detected.

Controls over IT and related financial systems are essential elements of financial reporting integrity. Effective general controls in an IT and financial systems environment are typically defined in six key control areas: entity-wide security program planning and management, access control, application software development and change control, system software, segregation of duties, and service continuity. In addition to general controls, financial systems contain application controls, which are the structure, policies, and procedures that apply to control access to an application, separate individuals from accessing particular application modules such as accounts payable, inventory, payroll, grants, or loans, and assess if the specific interface and edit controls are in place, as defined by management.

During fiscal year 2006, DHS as an agency, improved its Federal Information Security Management Act results, as reported by the DHS-Office of Inspector General. In addition, a few DHS components took actions to improve their IT general and application control environments and to address prior year IT control issues; however, a number of DHS components did not make necessary improvements during the year. During the 2006 IT testing, we identified over 200 separate findings, covering each DHS component. DHS closed approximately 44% of our prior year IT findings; however, we identified over 150 new IT findings through our test work this year. A significant number of findings were repeated in fiscal year 2006.

The control areas where the increases in the IT Notification of Findings and Recommendations (NFRs) present an increased risk of impacting financial data integrity include: 1) excessive access to key DHS financial applications, 2) misconfigured logical security controls to key DHS financial applications and support systems; and 3) application change control processes that are inappropriate, and in other locations not fully defined, followed, or effective. The re-issuance and the additionally identified internal control weaknesses were the result of a lack of needed prioritization of taking the necessary corrective actions. Despite the improvements in a few DHS components, several significant general IT and application control weaknesses remain that collectively limit DHS' ability to ensure that critical financial and operational data is maintained in a manner to ensure confidentiality, integrity, and availability.

FINDINGS BY IT AUDIT AREA

1 Entity-wide security program planning and management – we noted:

- Despite continued improvements in the process of performing Certification and Accreditation (C&A) of IT systems, nine DHS component financial and associated feeder systems, at three DHS components, were not properly certified and accredited, in compliance with DHS 4300A.
- Instances of incomplete or inadequate policies and procedures associated with computer incident response capabilities at four DHS components.
- Instances where background investigations of contractors employed to operate, manage and provide security over IT systems were not being properly conducted at three DHS components.
- Instances of lack of compliance with DHS computer security awareness training requirements, and/or lack of component policies for IT-based specialized security training at three DHS components.

2 Access controls – we noted:

- A large number of instances of missing and weak user passwords on key servers and databases which process and house DHS financial data at six DHS components.
- A large number of instances where user account lists were not periodically reviewed for appropriateness, and inappropriate authorizations and excessive user access privileges were allowed at nine DHS components.
- Instances where workstations, servers, or network devices were configured without necessary security patches or were not configured in the most secure manner at five DHS components.
- Instances where physical access to sensitive computer operations were not adequate at four DHS components.

3 Application software development and change control – we noted:

- One DHS component implemented a separate and secondary change control process outside of and conflicting with the established change control process. During our testing of this separate process, we identified it to be informal, undocumented, and not effective.
- Instances where policies and procedures regarding change controls were not in place to prevent users from having concurrent access to the development, test, and production environments of the system at four DHS components.
- Instances where changes made to the configuration of the system were not always documented through System Change Requests (SCRs), test plans, test results, or software modifications at seven DHS components. 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.

4 System software – we noted:

- Instances where policies and procedures for restricting and monitoring access to operating system software were not implemented or were inadequate at six DHS components. In some cases, the ability to monitor security logs did not exist.
- Instances where changes to sensitive operating system settings and other sensitive utility software and hardware were not always documented.

5 Segregation of duties – we noted:

- Instances where individuals were able to perform incompatible functions, such as the changing, testing, and implementing of software, without sufficient compensating controls in place at four DHS components.
- An instance where the policy and procedures to define and implement segregation of duties were not properly developed and/or implemented at one DHS component.
- Access control weaknesses identified during our IT testing also contributed to numerous instances where access to data could lead to various incompatible function issues, including the override of transactions at five DHS components.

6 Service continuity – we noted:

- Instances where incomplete or outdated business continuity plans and systems with incomplete or outdated disaster recovery plans were noted at four DHS components. Some plans did not contain current system information, emergency processing priorities, procedures for backup and storage, or other critical information.
- Service continuity plans were not consistently and/or adequately tested, and individuals did not receive training on how to respond to emergency situations at four DHS components.

7 Application controls – we noted:

- Instances of weak or expired user passwords, user accounts that were not kept current, users with excessive access privileges to certain key processes of an application, and key edit and business rules not working as designed by management at nine DHS components. Many of the weaknesses that were identified during our general control testing of access and segregation of duties controls are also relevant to this area, since these same issues also impact controls over specific key financial applications, and are thus reported here as well.

Cause/Effect: Many of these weaknesses were inherited from the legacy agencies that came into DHS or system development activities that did not incorporate strong security controls from the outset and will take several years to fully address. At many of the larger components, IT and financial system support operations are decentralized, contributing to challenges in integrating DHS IT and financial operations. In addition, financial system functionality weaknesses, as discussed throughout our report on internal controls in various processes, can be attributed to non-integrated legacy financial systems that do not have the embedded functionality required by Office of Management and Budget (OMB) Circular No. A-127, *Financial Management Systems*.

Further, there is no consistent and thorough testing of IT security controls by individual DHS components and by the DHS Office of the Chief Information Officer (CIO) to identify and mitigate such weaknesses.

The effect of these numerous IT weaknesses identified during our testing reduces the reliability of DHS' financial data. Many of these weaknesses, especially those in the area of change control, may result in material errors in DHS' financial data that are not detected, in a timely manner, in the normal course of business. In addition, as a result of the continuous presence of serious IT deficiencies, there is added pressure on the mitigating manual controls to be operating effectively at all times. Since manual controls are operated by people, there cannot be a reasonable expectation that they would be able to be in place at all times and in all areas.

Criteria: The *Federal Information Security Management Act* (FISMA) passed as part of the *E - Government Act of 2002*, mandates that Federal entities maintain IT security programs in accordance with OMB and National Institute of Standards and Technology (NIST) guidance. OMB Circular No. A-130, *Management of Federal Information Resources*, and various NIST guidelines describe specific essential criteria for maintaining effective general IT controls. In addition OMB Circular No. A-127 prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems. In closing, for this year's IT audit we assessed the DHS component's compliance with DHS' *Information Technology Security Program Publication, 4300A.*

Recommendations: We recommend that the DHS CIO in coordination with the OCFO make the following improvements to the Departments financial management systems:

1. For entity-wide security program planning and management:

    - Enforce through the DHS C&A program across all DHS components, a testing process which goes beyond an assessment of in-place policies and procedures, to include tests of password "strength," access lists, and software patches, of an application.
    - Enforce the consistent implementation of security programs, policies, and procedures, including incident response capability and IT security awareness and training; and
    - Enforce DHS' policy to ensure that all contractors go through the appropriate background/suitability check.

2. For access control:

    - Enforce password controls that meet DHS' password requirements on all key financial systems;
    - Implement an account management certification process within all the components to ensure the periodic review of user accounts for appropriate access;
    - Implement a DHS-wide patch and security configuration process, and enforce the requirement that systems are periodically tested by individual DHS components and the DHS CIO; and
    - Conduct periodic vulnerability assessments, whereby systems are periodically reviewed for access controls not in compliance with DHS and Federal guidance.

3. For application software development and change control:

- Implement a single, integrated change control process over the DHS components' financial systems with appropriate internal controls to include clear lines of authority to the components' financial management personnel and to enforce responsibilities of all participants in the process and documentation requirements;
- Develop policies and procedures regarding change controls, and implement to ensure segregation of change control duties; and
- Enforce 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.

4. For system software, monitor the use of and changes related to operating systems and other sensitive utility software and hardware.

5. For segregation of duties:

   - 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; and
   - Assign key security positions, and ensure that position descriptions are kept current.

6. For service continuity:

   - Develop and implement complete current business continuity plans and system disaster recovery plans; and
   - Perform component-specific and DHS-wide testing of key service continuity capabilities, and assess the need to provide appropriate and timely emergency training.

7. For application controls:

   - Implement policies to ensure that password controls meet DHS password requirements on all key financial applications and feeder systems;
   - Implement an account management certification process to ensure the periodic review of user accounts for appropriate access,
   - 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; and
   - Implement the appropriate oversight over the edit and interface controls to ensure that the financial processes are operating as management had designed.

Management Comments and OIG Evaluation

We obtained written comments on a draft of this report from the DHS CIO and DHS CFO. Generally, the DHS CIO and CFO agreed with all of the report's findings and recommendations. The DHS CIO has developed a remediation plan to address these findings and recommendation. We have incorporated these comments where appropriate and included a copy of the comments at Appendix D.

Appendix A

Description of Key Financial Systems and IT Infrastructure within the Scope of the FY 2006 DHS Financial Statement Audit

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, 2006.

United States Citizen and Immigration Services (USCIS)

Locations of Audit: USCIS Headquarters in Washington, D.C., as well as offices in Texas, and Vermont.

Key Systems Subject to Audit:

- *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 and Microsoft Visual Basic environments.

Immigration and Customs Enforcement (ICE)

Locations of Audit: ICE Headquarters in Washington, D.C., as well as offices in Texas, and Vermont.

Key System Subject to Audit:

Federal Financial Management System (FFMS) – ICE owns and operates FFMS. ICE performs accounting services for other DHS components, such as the USCIS, Management Directorate and US-Visit, 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 SGL for the accounting of agency financial transactions.

Departmental Operations

Locations of Audit: ICE Headquarters in Washington, D.C.

Key Systems Subjected to Audit:

Federal Financial Management System (FFMS) – ICE owns and operates FFMS. ICE performs the financial reporting function for USCIS and departmental operations 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 SGL for the accounting of agency financial transactions.

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 purchase requests, issue procurement documents, perform system administration responsibilities, and reconcile weekly Program Element Status 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.
- *Checkfree* - The Checkfree system is used to aid in the account reconciliations for the CAS. General Ledger extracts are imported into the system and automated passes are run to match transactions for reconciliation purposes. The results will later be loaded into CAS. This system is hosted on a Windows server and resides at the Coast Guard .
- *Naval Electronics Supply Support System (NESSS)* – Formerly named the Supply Center Computer Replacement System, NESSS is hosted at . NESSS is the primary financial application for the Engineering Logistics Command (ELC), the Supply Fund, and the Coast Guard Yard fund. Also housed at C is the Fleet Logistics System, 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 the Configuration Management Plus System, 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 Coast Guard's . These applications include the Personnel Management Information System and the Joint Uniform Military Pay System. Also housed at is the PeopleSoft 8.3 Direct Access application, which is used by members for self-service functions, including updating and viewing personal information.

United States Customs and Border Protection (CBP)

Locations of Audit: .

Key Systems Subject to Audit:

- – is a client/server-based financial management system that was implemented beginning in FY 2004 to ultimately replace the using a phased approach. The 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.
- – 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.

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 is responsible for the administration of DHS user accounts within the TIER and CFO Vision applications.

Federal Law Enforcement Training Center

Location of Audit: [redacted].

Key Systems Subject to Audit:

- *Momentum:* FLETC's core computerized system that processes financial documents generated by various FLETC divisions in support of procurement, payroll, budget and accounting activities.
- *Procurement Desktop:* Procurement Desktop is the procurement management system, which is used for the tracking of procurement activities at various FLETC locations. The system resides on an Oracle database and the front-end of the system is integrated with Momentum.

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.
- *Transaction Record Reporting and Processing* (*TRRP):* The TRRP application acts as a central repository of all data submitted by the Write Your Own (WYO) companies. TRRP also supports the WYO program, primarily by ensuring the quality of financial data submitted by the WYO companies to TRRP. TRRP is a mainframe-based application that runs on the National Flood Insurance Program (NFIP) mainframe logical partition in Norwich, CT.
- *Traverse:* The general ledger application used by CSC to generate the NFIP financial statements. Traverse is a client-server application that runs on a Windows server in Lanham, MD, which is secured in the local area network room. The Traverse client is installed on the desktop computers of the NFIP Bureau of Financial Statistical Control group members.

Grants and Training (G&T)

Location of Audit: G&T Headquarters in Washington, D.C.

Key Systems Subject to Audit:

G&T'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 G&T.

- *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 G&T 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.
- *Grants Management System (GMS)* – GMS supports the G&T 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. and the . TSA's financial applications are hosted on the Coast Guard's IT platforms.

Key Systems Subject to Audit:

- *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 is 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.
- *Sunflower:* The Sunflower system is the property management system, which is used for the tracking of property at TSA locations. The system resides on an Oracle database and the front-end of the system is integrated with the CAS user interface. Sunflower is hosted at the , the Coast Guard's primary data center.

Appendix B

FY2006 Notice of IT Findings and Recommendations - Detail by DHS Organizational Element

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 Information Technology
Notification of Findings and Recommendations – Detail

- **United States Citizenship and Immigration Services**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 Information Technology
Notification of Findings and Recommendations – Detail

Citizenship and Immigration Services

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
USCIS 06-01	The National Benefits Center (NBC) has not defined or documented the appropriate user permissions for the various roles granted to [redacted]3 Local Area Network (LAN).	Define and document the various [redacted] LAN roles and their associated user permissions as they pertain to NBC.	X		Low
USCIS 06-02	NBC does not perform periodic [redacted] LAN user access reviews to ensure that users' level of access remains appropriate.	• Ensure that the NBC IT Department annually review the list of [redacted]3 LAN system administrators and Database Administrators as well as review and approve access level list. • Ensure that NBC management annually review and approve the lists of employees stating the appropriate level of access for each NBC employee with access to [redacted] LAN. • Require the NBC IT Department to exercise its oversight role to ensure necessary adjustments in NBC [redacted] LAN account access levels are accomplished. based on the input.	X		Medium

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
USCIS 06-03	Management at the USCIS Headquarters and the Service Centers (Nebraska, California, Texas, and Vermont) has not completed or inadequately completed access forms for , and CISCOR system users.	Establish procedures for the completion and maintenance of user access forms for , and CISCOR users.	**X**		**Medium**
USCIS 06-04	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**	**Medium**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 Information Technology
Notification of Findings and Recommendations – Detail

▪ Immigration and Customs Enforcement

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 Information Technology
Notification of Findings and Recommendations – Detail

Immigration and Customs Enforcement

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
ICE 06-01	ICE-Office of the Chief Information Officer (OCIO) management has not defined or documented a formal plan to monitor security control compliance of third party providers of services.	Continue its efforts to define, document, and follow a formal plan to monitor security control compliance of third party providers of services.	**X**		**Medium**
ICE 06-02	The System Security Plan does not include procedures for distributing, maintaining, or tracking a user's signed Rules of Behavior (ROB) document. Additionally, not all users have signed the current ROB document reflecting DHS policies and procedures.	• Update the System Security Plan to include procedures for ensuring all users acknowledge and accept the DHS ROB when they login to ; • Develop and implement controls to ensure such procedures are enforced; and • Continue its efforts to append the DHS ROB to the initial login screen of .	**X**		**Medium**
ICE 06-03	At the time our procedures were performed, OCIO Management had not reviewed and updated the list of ICE users with wireless access. Several wireless broadband cards were issued to ICE users, but the OCIO was unaware of who the users are or where they are located. After communicating this issue to OCIO management, subsequently performed such a review and updated its list	Periodically review the list of ICE users with wireless access to ensure that all users with active accounts still require wireless access.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	of ICE users with wireless access. Furthermore, OCIO management indicated that it suspended and de-activated all cards not accounted for.				
ICE 06-04	ICE network traffic for the [redacted] client/server application does not pass through the ICE firewall, but rather goes directly to the ICE router at the Department of Commerce (DOC) Office of Computer Services (OCS) and then is handed off to DOC OCS' network.	Continue efforts to implement a second firewall for the protection of ICE's network, and more specifically, its financial information.	**X**		**High**
ICE 06-05	Users are not locked out of [redacted] or the ICE network after 20 minutes of inactivity.	Configure [redacted] and the ICE network to lock users out after 20 minutes of inactivity.	**X**		**Medium**
ICE 06-06	The [redacted] security audit log for the mainframe system housing the [redacted] databases can be modified by the [redacted] Security Administrator.	The ICE-CIO should work with DOC-OCS to prevent the [redacted] security audit log from being modified by the [redacted] Security Administrator.	**X**		**Medium**
ICE 06-07	ICE-CIO has not completed and authorized remote access forms for two of the five ICE users we selected for testing.	Ensure that all users with remote access have a completed and approved Remote Access Request form on file.	**X**		**Medium**
ICE 06-08	Two of the five [redacted] users we selected for testing have two accounts (eg - Jsmith, Jsmith1, same person with 2 accounts), but only one access form on file.	Complete and authorize user access forms for all [redacted] user accounts.	**X**		**Medium**
ICE 06-09	User profiles are not properly segregated within [redacted]. We noted the following: • 3 users can enter, approve, and make payments; • 157 users can create obligations and payments; and	• Clearly define and document [redacted] profiles that must be segregated. • Implement a timely and disciplined analysis (at least 2 times per year) of user access and segregate incompatible [redacted] user profiles whenever identified.	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• 7 contractors have access to the Desk Approving Official (AO) and Desk Funding Official (FO) profiles.				
ICE 06-10	User profiles have not been updated across all instances of [redacted] for the entities in which ICE, Office of Financial Management (OFM) provides accounting services to address the principles of least privilege and separation of duties. According to ICE management a business decision has been made to complete an overall update of user profiles, across all [redacted] instances. The business decision is to approach the full profile component, as ICE has determined it is the better long range solution.	Continue its efforts to review and update user profiles, across all [redacted] instances, to ensure that user profiles are adequately segregated and users only have access to profiles they need to perform their official duties.	**X**		**High**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 Information Technology
Notification of Findings and Recommendations – Detail

- **Departmental Operations**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 Information Technology
Notification of Findings and Recommendations – Detail

Departmental Operations

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
MGT 06-01	During our testing we noted that the user account for an individual who separated from MGT on May 24, 2006 had not been removed from [redacted] as of September 8, 2006. Although the user account was made inactive in [redacted] upon the employee's departure, the inactive account was not removed from [redacted]. Experienced system users/hackers can access systems via dormant/inactive accounts; therefore, it is important to remove all inactive accounts from the system.	• Request the ICE OCIO to remove the inactive user account from [redacted]. • Perform; in coordination with the ICE OCIO, periodic reviews of user accounts to ensure that all accounts are active and users require access to [redacted].	**X**		**Low**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 Information Technology
Notification of Findings and Recommendations – Detail

▪ Customs and Border Protection

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 Information Technology
Notification of Findings and Recommendations – Detail

Customs and Border Protection

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-06-01	Due to the design of , certain controls can be overridden without supervisory approval. For example, when a CBP entry specialist attempts to liquidate an import entry in , the system displays a warning message, indicating that a drawback claim had been filed against the import entry. However, entry specialists could override the warning message without supervisory review and process a refund without investigating pending drawback claims We noted that there have been no changes in the status of the finding. CBP management agrees with the finding, but does not agree with the recommendation to correct this issue in . Instead, CBP management plans on implementing functionality in to prevent the override capability. We noted that although will eventually replace was not be implemented in FY 2006.	While we understand that the complete mitigation, via system-based controls, of this issue may require significant investment, we recommend that CBP management develop a process to mitigate the systemic weakness that certain controls can be overridden without supervisory approval. Drawback functionality is just an example of supervisory overrides in . This is prevalent throughout the environment. Considering the number of years necessary to fully replace functionality with , this process should be designed in a manner to ensure supervisory review of overrides while maintaining a minimal burden on management. Also, CBP should ensure that the new system has the appropriate requirements for such controls and that these controls are applied prior to implementation. CBP management has concurred that the new system will be designed with this functionality built in to the system.		**X**	**High**
CBP-IT-06-02	• CBP management has not established ISAs for legacy connections with . • Additionally, the majority of financial institutions connecting with do not have ISAs.	• Complete efforts to identify the remaining dial-up connections that are considered "legacy" connections and formally establish ISAs with these entities • Complete efforts to identify all connections		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		with the [redacted] and formally establish ISAs with these entities.			
CBP-IT-06-03	CBP management has not performed a formal certification and accreditation on the [redacted] LAN as a whole. Specifically, a formal security control assessment and a formal risk assessment have not been performed for components of the [redacted] LAN.	Complete the certification and accreditation of [redacted] LAN components and the [redacted] LAN as a whole.		**X**	**Medium**
CBP-IT-06-04	CBP does not maintain a centralized listing of separated contract personnel. The only method CBP employs to track terminated contractors is the use of a report of users that had their mainframe account deleted. We cannot acknowledge this list as representative of all terminated contractors. This is because terminated contract personnel might not have mainframe access or their access was not removed after their termination.	• Develop a formal centralized process for tracking the termination of contract personnel. • Deactivate all systems access of terminated contractors immediately upon separation from CBP. • Periodically distribute a listing of terminated contract personnel to information system administrators so they remove user access and periodically assess contractor access to CBP systems.		**X**	**Medium**
CBP-IT-06-05	• CBP management has not performed a formal review of individuals with physical access to the data center. • Additionally, CBP management has not established formal procedures for revoking physical access to [redacted] buildings.	• Perform a formal review of access to the data center, • Update the data center access listing based on the review of access, and • Formalize the procedures for granting and removing [redacted] building access.		**X**	**Medium**
CBP-IT-06-06	CBP has not performed a separate certification and accreditation for the applications remaining in the seven business process areas defined in the Administrative Applications C&A. These seven business process areas include the following:	Complete the formal certification and accreditation of all [redacted] Administrative applications.		**X**	**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• Disclosure Administrative Support Systems • Financial Administrative Support Systems • Field Operations Support Systems • Investigation Support Systems • OIT Administrative Support Systems • Personnel Administrative Support Systems • Training Support Systems				
CBP-IT-06-07	[redacted] does not have an automated mechanism to detect and deactivate users that have not logged on for 90 days per DHS policy.	Implement an automated mechanism to detect and deactivate inactive accounts that does not require manual initiation.		**X**	**Medium**
CBP-IT-06-08	Field offices are not consistently reporting the completion of [redacted] re-certifications at their ports to the OFO headquarters. Email confirmation of completion of [redacted] re-certifications were not available for Boston, Baltimore, New Orleans, Miami, and Calgary (Canada) field offices, and the Los Angeles field office only provided an email stating that re-certification process exists, but did not confirm that [redacted] re-certifications had been completed. The six field offices listed above represent 10 of 44 ports selected for testing.	• Communicate the directive to all the field sites so that the field sites are aware of the reporting requirement. • Periodically reconcile the received completion reports with the field sites to determine the field sites that have not reported [redacted] re-certifications to OFO.		**X**	**Medium**
CBP-IT-06-09	We could not obtain the requested evidence of [redacted] recertifications from CBP for any of the 44 selected field level ports to determine whether [redacted] accounts with sensitive and high-risk combination of functions are reviewed for appropriateness.	Field ports should maintain documented evidence of [redacted] recertifications for audit purposes. CBP should ensure that field sites submitting completion reports are maintaining the required [redacted] recertification records.		**X**	**Medium**
CBP-IT-06-10	Improvements are still needed in CBP's Incident Handling and Response Capability	• Continue to roll out [redacted] Endpoint Health to all CBP workstations.		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	which may potentially limit CBP's ability to respond to incidents in an appropriate manner. Specifically, we noted the following issues: • Health Endpoint will not be installed on all workstations for the majority of the fiscal year. • 3 of 8 selected system flaw notifications did not have an associated Service Center ticket.	• Develop procedures to respond to system flaw notifications in a consistent manner.			
CBP-IT-06-11	We noted that the process for deletion of accounts for terminated government and contractor personnel may be utilizing erroneous data. Specifically, we noted that the files being sent from the Mainframe Security group to the Security team to terminate accounts of separated employees do not display the true status of employees. The mainframe query producing the separated contractor file includes individuals with Mainframe accounts that have been locked after 30 days of inactivity. Additionally, the separated government employees file is not accurate due to the fact that many government employees are separated and return to CBP as contractors. Consequently, the Security Group does not deactivate the accounts for these instances.	• Determine whether the potential matches are actual matches. Delete the accounts of any confirmed terminated employees. • Continue to use the payroll feed to determine if a user has terminated employment. • Disable user accounts of separated employees and contractors as stated in CBP and NIST guidance. • Implement and monitor a formal employee separation process that removes all systems accounts for terminated or separated employees.	**X**		**High**
CBP-IT-06-12	We noted that 24 out of 45 selected individuals did not have formally documented VPN access authorization forms. Additionally, CBP has not implemented formal procedures for VPN recertification for the majority of FY 2006.	• Continue to use the official authorization form for new VPN users. • Formally re-certify all VPN employee accounts on a periodic basis and document results.		**X**	**Medium**
CBP-IT-	CBP System Security does not conduct reviews	Implement policies and procedures for monitoring	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
06-13	of powerful system utilities. Specifically, the utilities [redacted] are not reviewed by management.	and reviewing logs of powerful system utilities for suspicious activity.			
CBP-IT-06-14	• Multiple methods of termination of mainframe accounts are used by Systems Security personnel (i.e. electronic mail, phone calls, and termination checklists). • We selected 45 terminated employees to determine whether termination checklists had been consistently completed. Of the 45 employees, only 30 forms were provided. Of these 30 forms, we noted that 9 out of 30 forms did not have supervisory signature, which signifies completion of the form to include notification sent to System Security for removal of logical access to applications. We noted that termination checklists (CF-241) are not consistently completed for separating employees throughout the organization.	• Ensure that management understands the importance of completing CF-241 forms and receiving appropriate notification from System Security for removal of access to systems. • Implement and enforce a formal separation and review process that requires the CF-241 form to be complete, including signatures from direct supervisors, before the employee's final day of employment.	**X**		**Medium**
CBP-IT-06-15	Backup tapes do not have affixed external labels to indicate the sensitivity of the data contained in the tapes.	Apply external labels to the backup tapes and other storage devices with the sensitivity level of the information contained within the object.	**X**		**Medium**
CBP-IT-06-16	CBP System Security does not have formal policies and procedures in place for monitoring powerful/sensitive system utilities	Formally document, implement and monitor policies and procedures related to the use of such powerful/sensitive system utilities.	**X**		**Medium**
CBP-IT-06-17	• Improvements still needed in CBP's technical security controls. Related to issues reported in FY02, FY03 and FY04 findings regarding host and network based security system access deficiencies, we noted the following:	• Coordinate with DHS in developing enterprise-wide solutions for improving network and host-based system configuration design(s) to reduce the risks of compromise. • Consider use of system administrator level security management monitoring tools to		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• CBP has confirmed that they will not be implementing the Passfilt.dll system control program to enforce strong passwords or the Windows NT password protection feature enhancement upgrade referred to as ( ). • CBP has not made the configuration changes to the that was compromised in We FY03 intrusion tests. • Discovered key systems' domains in targeting for potential unauthorized access attempts where we were able to identify major CBP network domains. • Exploited a system vulnerability that had not been corrected. • We confirmed that the number of Domain Administrators on selected Domains has increased since 2005. • ESM identified weak passwords, expired passwords, misconfigurations, and missing patches. • Identified vulnerabilities on an Oracle database which had critical patches missing, week passwords and auditing is not enabled.	detect and correct security deficiencies in preventing possible intrusions • Proceed with the implementation of to replace the Windows NT domain configuration. • Provide and approve more robust standards for Windows-based production servers for a standard and sustainable baseline set of system management security controls. • Consider development of a compliance level policy that provides for adherence to CBP password management policies set at the domain controller level where local system administrators and help desk staff may alter users' password management policies resulting in non-compliance situations. • Review and justify the level of system administrators on critical domains to ensure that the level of access is based on strict adherence to least privilege principles where the absolute minimum level necessary is applied.			
CBP-IT-06-18	• We noted the following issues related to password parameters: • Mainframe minimum password length is set	• Continue to develop and implement the e security record to bring Mainframe password parameters in compliance with DHS and CBP policies.	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	to six characters • [redacted] LAN minimum password length is set to six characters • Password complexity is not set on the Mainframe • Password complexity is not set on [redacted] • Password complexity is not set on the [redacted] LAN	• Bring [redacted] password parameters in compliance with DHS and CBP policies. • Configure the [redacted] security parameter to enforce minimum password length of eight characters.			
CBP-IT-06-19	We noted the following issues related to automatic session disconnection: • CBP's policy states that sessions should be automatically disconnected after 30 minutes of inactivity, which is not consistent with DHS' policy. • CBP's policy states that the workstation should log off from all connections after 5 minutes of inactivity, which is a documentation error. According to applicable guidance, all system connections do not have to be terminated after 5 minutes of inactivity on the workstation. • [redacted] sessions are configured to terminate after 60 minutes of inactivity. • CBP workstations cannot enforce the activation of a password-protected screensaver after 5 minutes of inactivity. The settings can be disabled or changed by individual users.	• Modify CBP's automatic session disconnection policy so that it is consistent with DHS' policy or obtain a formal waiver from DHS. • Modify CBP documentation to reflect that only the password-protected screensaver must be activated after 5 minutes of inactivity. • Modify [redacted] session disconnection settings to terminate sessions after 20 minutes of inactivity. • Continue deployment of [redacted] and Windows 2003 in order to set up group policy and enforce password-protected screensaver settings on the workstations.	**X**		**Medium**
CBP-IT-	[redacted] is not configured to disable user accounts	• Modify [redacted] system parameters to lock users	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
06-20	after 3 consecutive failed logon attempts. Additionally, per observation, we noted [redacted] LAN accounts were not locked after three consecutive failed login attempts.	after three consecutive failed logon attempts as required by the relevant policy. • Modify intrusion detections parameters on all [redacted] LAN Novell Netware contexts to allow two failed logon attempts, which will enforce account lockout on the third failed logon attempt.			
CBP-IT-06-21	CBP does not document formal approval of system changes for the [redacted] system. We selected 8 [redacted] regularly scheduled changes to determine if formal approval was given and documented. Per inspection of documentation, we were informed that there is no formally documented approval for the 8 selected changes.	Implement and enforce formal policies and procedures for documenting [redacted] change approvals by end users and data processing staff.	**X**		**High**
CBP-IT-06-022	We noted weaknesses related to the deposit and withdrawal of backup tapes: • Tape deposit receipts for 2 of 25 selected dates were not available. • Withdrawal of backup tapes from the off-site storage facility is not logged.	• File the tape deposit receipts immediately following the transaction with the off-site storage vendor. • Implement and monitor a process to log the withdrawal of backup tapes from the off-site storage facility.	**X**		**Low**
CBP-IT-06-023	CBP System Security does not consistently retain audit logs of powerful mainframe system utilities. Specifically, we selected 25 [redacted] reports to determine if powerful mainframe system utilities are being consistently logged. We determined that 5 out of the 25 selected logs were missing.	CBP management implement policies and procedures for retention of audit logs of powerful system utilities.	**X**		**Medium**
CBP-IT-06-024	We determined that [redacted] does not have the ability to prevent developers from	We recommend that CBP management implement procedures which prevent the overwrite of	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	overwriting existing code in the development environment. The developer is able to extract the code from the development environment and place it into a personal folder on the user's personal computer. If multiple users are modifying a program in their own personal folders they may be overwriting existing changes.	development code in the development environment.			
CBP-IT-06-025	Accounts are not deactivated after 90 days of inactivity with respect to the system. We determined through inspection of audit evidence acquired from that the defined deactivation period is, in fact, 180 days.	• Configure the setting within to automatically disable accounts that have been inactive after 90 days per DHS 4300A Sensitive Systems Handbook v3.3. • Review current accounts and disable and/or remove accounts that have been inactive for 90 or more days in .	**X**		**High**
CBP-IT-06-026	LAN Security Administrators do not keep audit logs for the prescribed period of time. Audit logs are only available for, at the most, the past three months. Logs are not maintained beyond the configured space for the log file. We also noted that LAN Security Administrators do not review audit logs.	• Configure the LAN to keep audit logs and track security events according to CBP and DHS policies. • Review LAN audit logs on a regular basis, according to CBP and DHS policy, to look for potential security events.	**X**		**Medium**
CBP-IT-06-027	We noted that accounts are not deactivated after 90 days of inactivity on the LAN. We determined that the removal of inactive LAN accounts is a manual process.	• Implement a control to automatically disable or remove accounts after ninety days of system inactivity in the system. • Review current accounts and disable or remove accounts that have been inactive for ninety or more days in the system.	**X**		**Medium**
CBP-IT-06-028	ISAs are not fully documented for . The ISA documenting the connection between America and CBP is currently out of date.	Complete and approve all connections with existing and new entities connecting with .	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	In addition, the connection that exists between Treasury and CBP is currently not officially documented.				
CBP-IT-06-029	The documentation of completed initial security awareness training is not properly maintained. We selected security awareness training documentation for 45 users. Per inspection of documentation, and noted that 13 of 45 did not have security awareness training certificates documented.	Consistently apply the requirements for initial and refresher security awareness training for all CBP employees and contractors upon initially establishing LAN/Mainframe accounts to CBP information systems.		**X**	**Low**
CBP-IT-06-30	Contractor access request forms for the LAN could not be adequately tested. We noted that no list of contractors hired to work at CBP is maintained, accordingly audit procedures requiring a sample of contractor access request forms could not be requested.	• Formalize policies and procedures that all employees, either government or contractor, are tracked by CBP personnel. • Implement a method of tracking those government employees and contractors that are currently employed at CBP.	**X**		**High**
CBP-IT-06-31	has excessive access to emergency processing capabilities. We noted that after an initial authorization to be added to an emergency user table in , a user can repeatedly request that their emergency access be reinstated, without being reauthorized. While emergency access in can expire in no more than nine days, some users renew their emergency access every nine days. We noted that CBP has not implemented an effective method of controlling this access, as users are not required to reauthorize their emergency access each time it is requested.	• Implement a policy and procedure that all users that require emergency access must have supervisory approval for each time they need their emergency access activated. • Recertify the users on the emergency access table to determine whether these are still users that may need emergency access as part of their operational duties at CBP.	**X**		**Medium**
CBP-IT-06-032	Access change audit logs are not reviewed in . CBP management does not independently review the changes that are put	• Implement policy that requires review of access level change logs for and . Ensure that personnel reviewing these logs are	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	into place by the [redacted] security administrators.	independent from the personnel that can make changes to the access. • Maintain documentation of the review of these logs and follow up on any anomalous issues discovered during a review.			
CBP-IT-06-34	An administrator account on the [redacted] LAN ("CMO NDS Administrator") is shared by four LAN administrators.	Ensure that the shared account is locked or deleted.	**X**		**High**
CBP-IT-06-036	We determined that the following documents have not been formally approved: • Systems Development Life Cycle (SDLC) Configuration Management Plan – No approval • Configuration Management Code Migration Procedures for [redacted]) has no authorization • Acquisition Planning and Selection and Development Process has no authorization • Configuration Management Code Migration Procedure for Systems, Applications, and Products has no authorization • Production Management Team Procedures – No approval, no change history • NDC Operations: Standard Operating Procedures – No approval	Ensure all documentation, outlining CBP policies, procedures and guidelines are appropriately coordinated and officially approved.	**X**		**High**
CBP-IT-06-37	User acceptance testing for Employee Self Service Solution (ESSS)/Remedy was not formally documented	• Ensure that user acceptance testing is performed for all systems developed or acquired at CBP. • Maintain formal documentation of user acceptance testing, including test plans and	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		results.			
CBP-IT-06-38	We noted that one individual with [redacted] LAN administrator privileges did not have justified access. We noted that there are instances where [redacted] locks security administrator accounts due to various reasons that do not require documented approvals for reinstating the user account. Additionally, we noted that instances where the [redacted] security administrator is new or reinstatement of suspended/deleted accounts is needed, a documented approval is required. We noted that due to a system limitation within [redacted], management cannot produce a system-generated list of field [redacted] security administrators that differentiates between the two cases.	• Delete [redacted] LAN administrator privileges from the individual without a documented need. • Perform periodic review of LAN accounts with [redacted] LAN administrator privileges to determine whether it is appropriate. • Formally document approvals every time a field [redacted] administrator privilege is requested regardless of whether it is due to new administrators, existing administrator that was suspended or deleted, or existing administrator that lost their profile, but is still active in the system. • Work towards identifying a solution in [redacted] that will allow system-generated listing of users that required formal field [redacted] administrator access approval documentation.	**X**		**High**
CBP-IT-06-39	We noted that 1 out of 3 selected batch job schedule changes did not have documented approval.	Management consistently document and maintain the OMS approvals for job schedule changes.	**X**		**Medium**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 Information Technology
Notification of Findings and Recommendations – Detail

- **United States Coast Guard**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 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	Risk Rating
CG-IT-06-001	The [redacted] Business Contingency and Disaster Recovery Plan is still in draft form and has not yet been tested.	• Finalize and implement the DRBC and ensure that it reflects changes in hardware and software and addresses disaster recovery procedures for [redacted]'s key financial systems. • Identify an alternate processing site and document associated restoration procedures. • Periodically test the DRBC and evaluate the results of the testwork so that the DRBC can be adjusted to correct any deficiencies identified in testing.		**X**	**High**
CG-IT-06-002	A comprehensive incident capability that includes designated response team members and procedures for incident handling to help ensure that the incident is properly handled has not been documented and implemented.	• Develop an incident response capability that includes: - Designation of response team members; - Training for team members; and - Procedures for incident handling, including preparation, containment, eradication, recovery and follow-up activities.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		• Approve and implement the incident response capability at the [redacted].			
CG-IT-06-003	Configuration weaknesses over [redacted] workstations allowed users to modify sensitive workstation system and security settings. During our test work, using a [redacted] network user account provided with ordinary privileges, we were able to successfully: • Disable the desktop's anti-virus; • Change the screen saver setting to remove the password-locking feature; and • Increase the time period for the screen saver activation significantly.	• Develop and implement a configuration checklist for the anti-virus server. • Perform periodic audits of the anti-virus and workstation security settings to ensure appropriate configurations are maintained.	**X**		**Medium**
CG-IT-06-004	Although backup tapes for [redacted] and the [redacted] are created on a regular basis, testing procedures have not been documented in accordance with [redacted] Instruction. Additionally, although [redacted] backup tapes are rotated offsite to the [redacted]), [redacted] backups have not been included in the tape rotation process to the [redacted]. Although a tape rotation schedule and tape rotation procedures have been documented, the tape transfer logs are not being completed in their entirety to note the tape numbers and the number of tapes being rotated offsite.	• Develop and document comprehensive backup procedures, which include testing the [redacted] and [redacted] backup tapes on a regular basis, at least annually. • Enforce the tape rotation procedures to ensure that tape transfer logs are completed and perform a weekly review to ensure that the logs are completed in their entirety before the tapes are sent to the [redacted]. • Include the [redacted] backup tapes in the weekly offsite tape rotation to the [redacted]. Update the tape transfer log to	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		include the [redacted] backup tapes that will be included in the rotation.			
CG-IT-06-005	Although a change control process has been established and documented for WINS, the process is not consistently followed. The appropriate approvals are not consistently documented within PVCS Tracker prior to implementation. Out of a selection of 30 [redacted] changes, 2 approvals were not documented. Additionally, evidence of testing, either through attached test plans and results or emails were not consistently attached to the selected SCRs within Tracker. As a result, evidence of testing for 7 out of the 30 selected changes were not available. Additionally, although criticality levels for [redacted] changes have been defined, procedures for making emergency changes to [redacted] have not been developed.	• Approve and complete each field related to the SCR within PVCS Tracker in accordance with the documented requirements of the Finance Center Staff Instruction 5232.1C; • Attach appropriate test plans, results, and approvals to the SCR forms within PVCS Tracker in accordance with Instruction 5232.1C; and • Document procedures for controlling emergency changes to the [redacted] application.	**X**		**Medium**
CG-IT-06-006	• [redacted] emergency procedures are in place for the evacuation of [redacted] and its Data Center. However, no emergency re-entry procedures exist within this directive. • No policies and procedures are in place to guide and document the emergency training of Data Center personnel. • Weaknesses exist in the implementation of least privilege regarding granting access to the Data Center personnel. Specifically, two out of the fifteen personnel forms selected, granted twenty-four hour access to	• Finalize and implement the emergency procedures that include re-entry procedures into the Data Center. • Develop and implement policies and procedures to train Data Center staff in emergency procedures pertaining, but not limited to fire, water, and alarm procedures. Additionally, formalize this training by retaining documentation that all staff has completed the	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	individuals on the janitorial staff.	training. • Continue to limit entry to the Data Center, especially after normal business hours, to critical personnel only.			
CG-IT-06-007	The passwords for [redacted] are not required by the system to be 8 characters in length or contain a combination of alphabetic, numeric and/or special characters. Due to lack of vendor support, there is uncertainty to the feasibility of implementing stronger password controls.	Complete planned corrective actions to replace [redacted] with the Coast Guard Direct Access HRMS 8.9 implementation, which will address vendor support and password strength.		**X**	**Medium**
CG-IT-06-008	A periodic review of Direct Access access lists was not conducted to ensure that users had the correct access privileges. Additionally, we determined that an applicant could be entered and hired by the same individual. The process of transitioning an applicant to an employee is in an audit trail; however this audit trail is not reviewed on a regular basis.	• Perform a periodic review of accounts to ensure that users are currently employed and have the correct access to the system, specifically to sensitive areas. • Require that the person who enters an applicant's data is not the person that hires the applicant or have an independent party at [redacted] monitor Direct Access audit trails on a regular basis for any irregularity.		**X**	**Medium**
CG-IT-06-009	Access authorization requests for [redacted] ids did not indicate the roles or menus necessary for the user to perform job functions; rather access authorizations identified a current user with similar privileges that could be copied to create the privileges for the new [redacted] id. Additionally, requests for new accounts are	• Perform a periodic review of [redacted] accounts to ensure that users are employed by the USCG and have the appropriate access to the system, specifically to sensitive areas. • Utilize the [redacted] access form,		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	accomplished via email, and the system administrator did not routinely retain these emails prior to January 2006.	which indicates the roles and responsibilities required for an individual's job function and a supervisor's approval.			
CG-IT-06-010	• Formal documented procedures are not in place over system software changes, related to , , and ; • A testing baseline for system software changes has not been established and documented; • PSC does not formally document and maintain the following for each system software change: - System software change request and authorization of the request; - Test plan documentation and test results; - Approval for migration of system software changes into production; and • The audit trail of system software changes is not periodically reviewed.	• Document policies and procedures for requesting, authorizing, testing, and approving system software changes, including emergency changes. • Establish a testing detail baseline that defines the standard components that should be documented for software changes, and communicate and enforce this procedure to implement testing as a component of change implementation. • Document and maintain test plans, test results, and approvals for all system modifications. • Review an audit trail of system software changes to identify unauthorized changes.		**X**	**Medium**
CG-IT-06-011	Test plans and test results for application changes were not consistently documented and maintained. Specifically, 28 out of 30 selected application changes did not have test plans or test results documented. In addition, 11 out of 30 changes were not approved by the business sponsor (user acceptance approval) and 4 out of 30	• Document and maintain test plans and test results for application changes, in accordance with the SDLC policy • Obtain and document appropriate approvals prior to the implementation of program	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	changes were not approved by the peer reviewers prior to migration into production, as required by the Systems Development Life Cycle	changes, in accordance with SDLC policy			
CG-IT-06-012	passwords are not in compliance with the DHS password policy. The systems does not enforce the following password rules: • passwords are to be eight characters in length • passwords are to include alphabetic, numeric, and special characters • passwords are not be the same as the previous eight passwords We determined that sessions are not timed out following 20 minutes of inactivity and accounts are not disabled following a period of 90 days of inactivity. During our testing of accounts with special attributes, we determined that two generic accounts have access to and . Additionally, we determined that the and settings were not enabled. Furthermore, four accounts assigned to personnel had both and , two of which were system programmers.	• Strengthen password and account configurations in accordance with DHS 4300A requirements including: - Require passwords to be eight characters in length - Require passwords to include alphabetic, numeric, and special characters - Require that passwords not be the same as the previous eight passwords - Terminate sessions following 20 minutes of inactivity - Delete inactive accounts following 90 days of inactivity • Set security settings to the most restrictive mode. Specifically, the following settings should be changed: - Change to - Enable • Review access to sensitive privileges to ensure that users	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		require the privilege to perform job functions.			
CG-IT-06-013	Outgoing Personnel forms were not documented for two out of nine selected users. These two individuals retained access to the [redacted] system with read only access.	Implement corrective actions to document and implement policies and procedures for use in managing terminations, including use of the Outgoing Personnel form.	**X**		**Medium**
CG-IT-06-014	• Excessive access privileges have been granted within the [redacted] database. • Password configurations for the [redacted] profiles have been configured to permit passwords to be a minimum of six characters in length. Additionally, the password history requirement is the only password requirement that has been configured for the [redacted] profile. • Audit logging has not been enabled within the [redacted] application or database. • Documented access request forms could not be located for nine out of 22 new [redacted] users granted access to the application. Additionally, although the automated access request forms for the other 13 out of 22 new [redacted] users granted access to the application were approved, the level of access/privileges associated with the new user were not documented on the access request form. • Individuals who are no longer employed with	• Review the [redacted] database user listing to determine which users have a business need to retain access to the [redacted]. • Configure the [redacted], [redacted] and [redacted] profiles to be in compliance with [redacted] Password Policy SOP. • Establish detailed procedures for audit trail generation, review and management. • Develop and implement access control procedures for the [redacted] system and database accounts. • Develop and implement access control procedures for the [redacted] system and database accounts. • Develop and implement access control procedures for the [redacted] system and database accounts.	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	were found to have active accounts within . • WINS account reviews have not been performed on a periodic basis.				
CG-IT-06-015	Weaknesses were noted in regard to these personnel entrance and exit procedures for civilian, contractor and military personnel. Specifically, out of fifteen entrance check-in sheets inspected, thirteen were incomplete or did not exist. Additionally, out of fifteen exit check-out sheets inspected, only four were received from our sample selection, and none of which were complete.	• Continue with efforts to improve the implementation of the personnel entrance and exit procedures and a more formalized chain of command for the collection of the check-in and check-out sheets. • Track and monitor the completion of check-in and check-out sheets. • Ensure that personnel indicate which line items on the check-in/check-out sheets are not applicable. • Retain Check-out sheets for up to a year after an employee's departure.	**X**		**Medium**
CG-IT-06-16	• Password configurations for have been not configured to maintain the password history for each account. • Users are not locked out of their accounts after three invalid logon attempts. • Policies and procedures for application and database audit log management have not been documented. • Documented access request forms could not be located for three out of nine new users granted access to the application.	• Configure the application and database to be in compliance with Password Policy SOP. • Configure the application and database to lock users out of their accounts after three failed login attempts. • Establish detailed procedures for audit trail generation, review and management. • Develop and implement access	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• accounts are not immediately disabled upon an employee's termination. Specifically three civilians terminated employment with . • has not been configured to track and deactivate accounts that have not been used in 90 days. • account reviews have not been performed on a periodic basis and results of the reviews are not maintained. • An excessive number of individuals have user administrator capabilities within .	control procedures for the system and database accounts. • Develop and implement access control procedures for the system and database accounts. • Configure the system to track and lock the accounts of individuals who have not logged into the system in 90 days. • Develop and implement access control procedures for the system and database accounts. • Develop a wide segregation of duties policy that provides guidance to personnel regarding incompatible duties.			
CG-IT-06-017	• Password configurations for application and database have been configured to permit passwords to be a minimum of six characters in length. • Users are not locked out of their application accounts after three invalid logon attempts. • Audit logging has not been enabled within the application or database. • Individuals who are no longer employed with were found to have active accounts within . • account reviews have not been performed on a periodic basis.	• Configure the application and database to be in compliance with Password Policy SOP. • Upgrade to ensure that users are locked out of their accounts after three invalid attempts. • Establish detailed procedures for audit trail generation, review and management. • Develop and implement access control procedures for the system and database accounts. • Develop and implement access control procedures for the system and database accounts.	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CG-IT-06-018	• Password configurations for the application and database have been configured to permit passwords to be a minimum of six characters in length • Policies and procedures for application and database audit log management have not been documented. • [redacted] account reviews have not been performed on a periodic basis.	• Configure the [redacted] application and database to be in compliance with [redacted] Password Policy SOP. • Establish detailed procedures for audit trail generation, review and management. • Develop and implement access control procedures for the [redacted] system and database accounts.	**X**		**High**
CG-IT-06-019	• Manager Review of System Administration Monitor Procedures have been developed that guide managers in performing periodic system administration monitoring reviews. However, the procedures do not note the periods of review that are being monitored, who is responsible for performing the reviews and evidence that the manager review was performed could only be obtained for March 2006. Additionally, although the manager reviews were implemented in March 2006, for the first half of the fiscal year, October through March, [redacted] system administration monitoring was not performed by a manager or group outside of the three systems administrators during that time period. • The access request form for one out of four individuals granted access to [redacted] since October 1, 2005, did not contain the supervisor's approval. • The account of a contractor that left [redacted]	• Revise the Manager Review of System Administration Monitor Procedures to note how often managers should perform system administration monitoring reviews. • Continue enforcing [redacted] Instruction 5230.3 – Policy for System Level Access to [redacted] Computer Assets. • Continue enforcing [redacted] Instruction 5230.3 – Policy for System Level Access to [redacted] Computer Assets to ensure that the accounts of terminated civilians/contractors/military personnel are revoked in a timely manner.		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	in October 2005 remained active until May 2006.				
CG-IT-06-020	A [redacted] Security Configuration Management Plan does not exist that clearly delineates the roles and responsibilities between [redacted], and the [redacted]. [redacted] is the organization under contract by Coast Guard to manage the [redacted] and [redacted] software programs. Consequently, the System Security Plans for the [redacted] and [redacted] applications do not include key security control information. Specifically, the plans do not include information on the current security configuration management process, including delineation of responsibilities for all involved parties. The System Security Plans were otherwise compliant with current NIST standards.	Implement corrective actions to implement a [redacted] Security Configuration Management Plan that includes the role and responsibilities of [redacted] and [redacted]. Also, the plan should address both [redacted] and [redacted] and their associated operating systems and databases. Subsequently, the [redacted] and [redacted] System Security Plans should be updated to reflect the approved information in the [redacted] Security Configuration Management Plan.	**X**		**Medium**
CG-IT-06-021	Coast Guard Headquarters is in the process of developing policy that addresses role-based training requirements for individuals with critical IT positions. However, currently this Training and Education Plan is still in draft form and no policies and procedures exist that require critical IT personnel to continue their education through role-based training.	• Finalize the development of centralized headquarter policies and procedures for IT role-based training for civilian personnel with critical IT positions. • Deploy the IT role-based training of civilian personnel with critical IT positions down to the CG component levels for implementation.	**X**		**Medium**
CG-IT-	NOAA forgotten widows, member type 1384,	Implement corrective actions to add the	**X**		**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
06-022	are not designed to be excluded from the actuarial data file created annually to estimate the pension liability for the Coast Guard. Forgotten widows are the survivors of retired personnel who died before any survivor benefit program was enacted. The program is designed to exclude those member types included in the group identified in the , which does not contain member . All member types not in the group are included in the actuarial liability file.	to the group in the to effectively exclude the NOAA Forgotten Widows from the actuarial data file.			
CG-IT-06-024	A security test and evaluation has not been conducted on the General Support System. In addition, the final Certification and Accreditation package has not been created and an Authorization to Operate has not been requested or approved for the General Support System.	Complete the Certification and Accreditation package for the general support system in compliance with NIST Special Publication 800-37 and DHS Sensitive Systems Policy Directive 4300A, including a Security Assessment Report and a signed Authorization to Operate.		**X**	**Medium**
CG-IT-06-025	No documentation exists for the change control process, including the emergency changes process, surrounding the application. Although a development server exists for the application, management indicated that the application version 6.0.13 was the only version implemented for in 2003 and no changes or updates have been made since.	• Develop and implement a change control process for the application. • Develop and implement an emergency change control process for the application.	**X**		**Medium**
CG-IT-	During technical testing patch management	• Implement the corrective actions		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
06-026	weaknesses were identified on hosts supporting the [redacted] and [redacted] applications. Many of these vulnerabilities could allow a remote attacker to gain full control of the affected host and could lead to the compromise of the availability, confidentiality and integrity of [redacted] and [redacted] data.	noted in the finding. • Implement polices and procedures to ensure that the software builds created by the CG software developer are tested to ensure that all software security configurations, such as software patches and non-compliant settings, are up to date. • Continue the process for performing periodic scans of the [redacted] network environment, including the financial processing environment, for the identification of vulnerabilities, in accordance with NIST SP 800-42. • Implement corrective actions to mitigate the risks associated with any vulnerabilities identified during periodic scans.			
CG-IT-06-027	During technical testing configuration management weaknesses were identified on hosts supporting the [redacted] and [redacted] applications. Specifically, servers were identified with excessive access privileges, and password and auditing configuration weaknesses.	• Implement the corrective actions noted in the finding. • Implement polices and procedures to ensure that the software builds created by the CG software developer are tested to ensure that all software security configurations, such as software patches and non-compliant settings, are up to date. • Continue performing periodic scans of the [redacted] network environment, including the financial processing environment, for the		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		identification of vulnerabilities, in accordance with NIST SP 800-42. • Implement corrective actions to mitigate the risks associated with any vulnerabilities identified during periodic scans.			
CG-IT-06-028	• Coast Guard has not completed the process of filing the records that were recovered and recreating of the records that were not found during the migration of records from the Department of Transportation to DHS. • Civilian background investigations and reinvestigations are not being consistently performed. Specifically, three (3) out of seven (7) newly hired civilian employees at [redacted] did not have any record of a background investigation on file. Additionally, for the re-investigation of [redacted] employees, four (4) out of five (5) GS employees selected did not have a current investigation on file. • Position sensitivity level distinctions for civilian personnel with access to DHS information systems at [redacted] are not accurately depicted. Specifically, of the selection of position descriptions received, nine (9) out of ten (10) had non-critical position sensitivities although their job functions were that of IT personnel with advanced access to the DHS system.	• Complete the process of restoring the background investigation records of their military and civilian personnel that were not included during the migration of records from the Department of Transportation to DHS. • Perform the background investigations for civilian employees in accordance with DHS directives. • Reevaluate and assign the correct position sensitivity levels to individuals with access to DHS information systems in accordance with DHS policy.		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CG-IT-06-029	Coast Guard has and continues to operate a separate, informal and largely undocumented change development and implementation process effecting Coast Guard Financial Systems, outside of and conflicting with the formal change control process. This informal script development and implementation process began with the implementation of in June of 2003. reports that the documentation and tracking of the scripts was not developed until June of 2005 but is unable to provide a complete population of implemented scripts, to include the type, purpose and intended effect on financial data. The implemented process is ineffective as the approval, testing and documentation procedures of the script changes are not appropriately designed and the current process is ineffective to control the intended and actual effect on financial data.	• Immediately implement a single, integrated change control process over Coast Guard Financial Systems with appropriate internal controls. • Immediately commence an in depth examination of the Coast Guard Financial Systems with an external independent organization trained in financial information systems, process analysis and with a demonstrated understanding of the federal accounting environment. • In conjunction with item number two above, begin an in depth examination to determine and document, in detail, the effects of the identified root causes and implemented automated and manual adjustments on financial data and affected financial statements for prior reporting periods and make appropriate restatements.	**X**		**High**
CG-IT-06-030	• A copy of the Disaster Recovery Plan has been completed. However, the plan has not been tested. • The DRP for the has been completed. However, testing of the DRP has not taken place. The projected completion date is October 2006. • The DRP for the General Support System has been completed. However, testing of the	• Periodically test the DRPs and Contingency Plans for the , and so that the plans can be adjusted to correct any deficiencies identified in testing. • Obtain a finalized and approved MOU with and CG-61 outlining their responsibilities in getting the DR site up and running in a timely manner.		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	DRP is scheduled to take place by the end of the year. • A copy of the Memorandum of Understanding (MOU) between [redacted] and two other CG components who the [redacted] must rely on for various reasons at the off-site facility was cited in the Disaster Recovery Plan • A finalized contract with the off-site facility was cited in the Disaster Recovery Plan. However, we were unable to obtain the signature page for it during our audit field work.	• Obtain a finalized and approved contract with the [redacted] off-site Disaster Recovery facility.			
CG-IT-06-031	During our FY 2006 follow-up testing, we determined that [redacted] had taken corrective action on several of the previously noted vulnerabilities, however several remained. The remaining vulnerabilities are in the following four areas: • Account management - 2 high-risk vulnerabilities and 4 medium-risk vulnerabilities • Configuration management – 2 medium-risk vulnerabilities • Patch management – 3 high-risk vulnerabilities	• Implement the corrective actions noted in the finding. • Institute a formal process for performing periodic scans of the [redacted] network environment, for the identification of vulnerabilities, in accordance with the *DHS IT Security Program Handbook for MD4300A* and NIST SP 800-42. • Implement corrective actions to mitigate the risks associated with any vulnerabilities identified during periodic scans.		**X**	**High**
CG-IT-06-032	During our FY 2006 testing, we determined that none of the [redacted] prior year vulnerabilities were corrected. As a result, the vulnerabilities present in FY 2006 are in the following four areas:	• Implement the corrective actions noted in the tables above. • Institute a formal process for		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• Audit management – 2 medium risk vulnerabilities • Configuration management – 3 high, 6 medium and 11 low risk vulnerabilities • Password management – 1 high and 5 medium risk vulnerabilities • Patch management- 11 high, 12 medium and 12 low risk vulnerabilities	performing periodic scans of the network environment, for the identification of vulnerabilities, in accordance with *DHS IT Security Program Handbook for MD4300A* and NIST SP 800-42. • Implement corrective actions to mitigate the risks associated with any vulnerabilities identified during periodic scans			
CG-IT-06-033	contracts the maintenance of their information systems software and hardware for the Superdome supercomputer, which houses the four production databases including the production database, to Hewlett Packard (HP) through two separate service agreements. One of the service contracts is valid until 2007 for a segment of their computer software and hardware. However, the second portion of Superdome equipment is covered under a maintenance contract that expired on May 31, 2006. has requested a renewal of this contract however the request is still pending and there is no other contractual agreement to cover the maintenance of their software and hardware during this lapse in service contracts.	• Continue to communicate with Coast Guard Headquarters in order to convey the importance of a timely renewal of the maintenance contract. • Maintain a continuous service contract for the hardware and software with the current vendor by anticipating delays in contract renewal and submitting requests for procurement in a timely manner.	**X**		**Medium**
CG-IT-06-034	• does not perform background investigations or verify that background investigations have been performed for	• Implement policies and procedures to ensure compliance with the new DHS policies for the background		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	contractors working at [redacted] especially those with sensitive IT positions. Specifically, [redacted] employs 150 contractors; however, We were unable to obtain the status of a background investigation on any of them. • No risk levels for contractor personnel with access to DHS information systems at [redacted] exist. Contracting personnel with IT job functions which require advanced access to the DHS system are not categorized at a higher risk level then an individual who uses the system with basic privileges.	investigations of contracting personnel. • Develop risk levels for contractor positions with access to DHS information systems in accordance with DHS policy.			
CG-IT-06-035	The Memorandum of Understanding (MOU) developed between Coast Guard [redacted] and Treasury Financial Management Service addresses the development, management, operation, and security of a connection between systems owned by both parties. The previous agreement expired in April of 2006 and a current MOU between [redacted] and Treasury has not been completed.	Complete planned corrective actions to finalize and obtain all approvals for the MOU and ISA between [redacted] and Treasury-FMS Financial Management Service.	**X**		**Low**
CG-IT-06-036	• Seven developers out of 15 personnel in the Business Services Section had inappropriate access to [redacted] function in the Production and Development environments allowing them to potentially circumvent the change control process at [redacted] from October 1, 2005 through August 10, 2006. • We further note that 5 out of 15 personnel in the Business Services Section had inappropriate access to functions containing	• Remove analyst access to the development environment. • Continue to ensure that developers have limited access (select or read only) to the production environment.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	elevated privileges in the Production and Development environments allowing them to update production and potentially circumvent the change control process at .				
CG-IT-06-037	The following password configuration weaknesses associated with the application: • Passwords were not configured to require password changes every 90 days from October 1, 2005 to February 14, 2006. • Passwords were not configured to require minimum length of six instead of eight. • Passwords were not configured to maintain a history of six passwords. • Passwords were not configured to require a combination of alphabetic, numeric, and special characters. • Passwords were not configured to restrict dictionary words including dictionary words spelled backwards. • Passwords were not configured to restrict simple pattern passwords; such as “qwerty” or “xyz123”. • Passwords were not configured to check that two identical characters in any position exist from the previous password.	• Modify the application password configurations to be compliant with DHS and Coast Guard policy. • Configure the application to terminate idle sessions after a specified period of inactivity as defined in DHS and Coast Guard policy.	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Additionally, we identified that the [redacted] application is configured to terminate idle sessions after 30 minutes of inactivity instead of 20 minutes.				
CG-IT-06-038	The following segregation of duties weaknesses associated with the [redacted] application. Application Audit Trails/Monitoring • The [redacted] application does not have the capacity to maintain audit trails for management review. Incompatible Duties • There is only one individual performing all [redacted] DBA duties. The lone [redacted] DBA actions are not reviewed for appropriateness, including changes to data and/or security profiles. • Users in the "[redacted]" group have privilege to insert data at the database level. • There are 17 accounts associated with the DBA role in Oracle.	• Monitor the [redacted] user and DBA actions as well as develop and implement procedures to periodically perform reviews of [redacted] user actions. • Develop and implement procedures to periodically perform reviews of the [redacted] DBA's actions. • Perform a review of accounts with DBA privileges to determine that access is granted based on the principle of least privilege.	**X**		**High**
CG-IT-06-039	There are no documented policies and procedures on the calculation of the environmental liability reported on the DHS Consolidated balance sheet. The environmental liability is adjusted quarterly based on the data stored in the [redacted] application.	Develop policies and procedures around calculation of the environmental liability using data stored in the [redacted] application.	**X**		**Medium**
CG-IT-06-040	We identified the following account management weaknesses associated with the SAM application. Inactive Accounts	• Develop and implement procedures to periodically perform reviews of inactive [redacted] application accounts. • Develop and implement procedures	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• A planned monthly review of inactive [redacted] application user accounts has not been implemented. • There are 315 active accounts that have not logged into the [redacted] application for 90 days. Access Authorizations • Access authorization documentation was not made available for 17 out of 60 selected new [redacted] application users. Logical/Physical Access Reviews • The [redacted] application accounts are not recertified annually to validate that the accounts belong to appropriate personnel. • Management is not reviewing failed logon attempts to the [redacted] application. Termination Procedures • Five separated civilian personnel had active accounts in the [redacted] application. • Nine separated military personnel had active accounts in the [redacted] application. • Coast Guard does not maintain a centralized listing of separated contractors.	requiring documented authorization for access to the [redacted] application. • Develop and implement procedures to periodically perform reviews of [redacted] application accounts. • Develop and implement procedures to periodically perform reviews of failed logon attempts to the [redacted] application. • Develop and implement centralized process for tracking terminations of all Coast Guard personnel, including military, civilian, and contractor personnel, and implement a process to ensure that access to [redacted] is removed for all terminated personnel in a timely manner.			
CG-IT-06-041	System change request to modify transaction code [redacted] to automatically reestablish the funds as obligated was implemented in March 2006 within the [redacted] 3.2 build. Currently, the automated process appeared to be operating effectively. However, from October 2005 through March 2006, no mitigating controls such as procedures for training of staff and/or	The system change request to automatically reestablish the funds as obligated when transaction code [redacted] is used was implemented in March 2006 and therefore has no further recommendations to provide. For recommendations for all other		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	manual reviews were established to determine whether or not the re-obligation should be established to the associated UDO balance. Additionally, [redacted] management indicated that transaction code [redacted] should not be automatically reestablishing the funds in the system. However, as we could not perform a complete analysis of the [redacted] posting logic in FY 2006 as noted in NFR CG IT-06-029, transaction code [redacted], as well as other codes, may still contain errors as of September 30, 2006.	transaction codes, refer to NFR CG IT-06-029.			
CG-IT-06-042	[redacted] had not developed formal change control procedures documenting the requirements for altering the criteria used in [redacted] to match transactions. Functional changes are required when initially establishing a matching process or when the accounting operations team identifies that transactions that should be matching are not correctly matching in the system.	Complete planned corrective actions to document policies and procedures for requesting, authorizing, testing, and approving functional changes to [redacted].	**X**		**Medium**
CG-IT-06-043	Policies and procedures surrounding the change control process for Coast Guard [redacted] needs improvement. Specifically, no policies and procedures exist for: • the testing/verification the functionality of the change in pre-production before the change is implemented in production • the final approval of the change by [redacted]	• Develop and implement additional change control policies and procedures to include the testing of changes in a pre-production instance and obtain final approvals from [redacted] management on all changes before implementation in production.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	management Additionally, change control test results, as well as approvals, are not consistently documented. Specifically, documentation for the two formula changes requested, did not include evidence of testing in a pre-production instance and the final approvals of the changes when they are implemented in production. Furthermore, of the five remained changes selected, we were unable to obtain documentation of final of final approvals for each of the five sample items approvals for five out of the five items.	• Develop and implement a formalize process for the retention of documentation throughout the change control process.			
CG-IT-06-044	As a result of our audit test work and supported by all the IT NFRs issued during the current year, we determined that Coast Guard is non-compliant with the following laws and regulations: • Federal Information Security Management Act of 2002 (FISMA) • Federal Financial Management Improvement Act (FFMIA) • Office of Management and Budget (OMB) Circular A-130	• Continue to develop, implement and monitor compliance with DHS, Coast Guard and Federal security policies and procedures in the areas of: - Access Controls - Change Controls - System Software - Segregation of Duties - Entity-wide Security Planning - Service Continuity • Develop and implement corrective action plans to remediate the NFRs issued during the FY 2006 audit. These corrective action plans should be developed from the perspective of the identified root		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		cause of the weakness.			

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 Information Technology
Notification of Findings and Recommendations - Detail

- **Federal Emergency Management Agency**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 Information Technology
Notification of Findings and Recommendations - Detail

Federal Emergency Management Agency (FEMA)

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-06-01	During our technical testing, patch management weaknesses were identified on [redacted] servers. Specifically, as a result of missing patches, the [redacted] servers were vulnerable to buffer overflow vulnerabilities.	FEMA should implement the corrective actions listed in the NFR for each technical control weakness identified.		X	High
FEMA-IT-06-02	During our technical testing, configuration management weaknesses were identified on [redacted], and key support servers. Specifically, servers were identified with password and auditing configuration weaknesses, and version weaknesses.	FEMA should implement the corrective actions listed in the NFR for each technical control weakness identified.		X	High
FEMA-IT-06-03	There are no procedures are in place to periodically review [redacted] user access lists to determine if access is still needed, including the development of a master listing of all employees and contractors developed and maintained by FSB.	Develop and implement procedures regarding periodic review of access lists. The policy should require that a master listing of all employees and contractors is collaboratively developed and maintained by FSB in order to periodically determine whether logical user access to [redacted] is valid, consistent with job responsibilities, and according to the least privilege principle.		X	High
FEMA-IT-06-04	The [redacted] production and test servers are located in very close proximity of each other, which is not conducive to effective contingency planning efforts. We note that	FEMA, upon implementation of the [redacted] Data Center's "real-time" back-up facility, create redundant servers at the [redacted] Data Center for the two [redacted] servers located at [redacted].		X	Medium

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-06-05	upon the implementation of the [redacted] Data Center's "real-time" back-up facility, both the [redacted] test and production servers will be redundant, alleviating the current condition. However, the Denton back-up facility does not currently have that capability in place. • The [redacted] did not provide adequate documentation of the results to the accrediting authority. The [redacted] included thorough testing of managerial, operational and technical controls and identified 88 vulnerabilities; however, the vulnerabilities listed in the ST&E report were only identified as one POA&M weakness in the [redacted] POA&M • Of the 10 systems deemed critical for which the C&A process was completed, we noted that the following four systems did not include any documentation of their ST&E results in the ATO package: [redacted], [redacted]. • FEMA has completed a majority of the [redacted] migration from Microsoft Windows 2000 Professional to [redacted] except for a few aspects of the migration dealing with Individual Assistance and various regional sites. We noted that these major changes to	• Document the results of the [redacted] by providing a detailed listing for the vulnerabilities and/or corrective action for the vulnerabilities in the ATO as well as documenting them in an individual manner in the POA&M when the system is re-certified and accredited in 2007. • Document the results of the ST&Es performed on [redacted] after performing technical testing, and provide results for the technical testing performed over the baseline security requirements in accordance with NIST 800-37 and IT Security Program Handbook for MD4300A Sensitive Systems. • Re-perform the C&A process for [redacted] due to the major changes the system has undergone using NIST 800-37 and IT Security Program Handbook for MD4300A Sensitive Systems.		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	the system warrant that the [redacted] C&A process be re-performed.				
FEMA-IT-06-06	There is not formal, documented procedures are in place to require updates to the [redacted] system documentation as [redacted] functions are added, deleted, or modified.	Develop and implement procedures to require updates to [redacted] documentation as functions are added, deleted, or modified.		**X**	**Low**
FEMA-IT-06-07	• FEMA did not adequately document testing of the Contingency Plan for [redacted]. Although a table-top test of the Contingency Plan was completed on February 10, 2006, the [redacted] table top test did not adequately test the IT components of the system/processes. • FEMA does not have an accurate Contingency Plan for [redacted]. The most recent version of the [redacted] Contingency Plan is dated July 19, 2004. However, since that time, FEMA has nearly completed its migration of [redacted] from Microsoft Windows 2000 Professional to the [redacted] operating system and is adding a Small Business Administration web interface.	• Perform a full test of the [redacted] Contingency Plan when the [redacted] Data Center is prepared to be the functional alternate site for [redacted]. As part of this contingency plan test, FEMA should include the IT components in order to assess if they will operate as planned. Additionally, testing of the [redacted] Contingency Plan should be performed annually. • Update the [redacted] Contingency Plan and then perform an adequate test of the plan in compliance with DHS 4300A and NIST 800-34, once the [redacted] migration is complete.		**X**	**High**
FEMA-IT-06-08	The FEMA COOP has prioritized each of its 12 critical Information Technology (IT) systems according to criticality of the systems; however, the FEMA COOP has not been updated to take into account the new listing of FEMA critical IT systems. We confirmed with the Office of Cyber	Update the FEMA COOP to clearly state and prioritize the listing of 12 critical IT systems that would be brought back online at various alternate processing sites in the event of a disaster.		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Security (OCS) and ONSC that the updated listing of FEMA mission critical IT systems should be represented in the FEMA COOP.				
FEMA-IT-NFR-06-09	• users are not locked out of the system after three invalid logon attempts. In addition, we determined that upon locking a user account out of the system after three invalid logon attempts at the domain level, the user account becomes unlocked and active again after fifteen (15) minutes of inactivity. • settings on machines running Microsoft Windows 2000 Professional disabled the user's ability to disable the password protected screensaver; however the settings did not disable the user's ability to change the inactivity threshold greater than the FEMA standard of fifteen minutes. This weakness impacts S.	• Complete a review over all settings for Microsoft Windows 2000 users and ensure that all settings are properly applied to those users, including disabling the user's ability to change the inactivity threshold of the password protected screensaver. • Ensure that FEMA users locked out of the system at a domain level must have the system administrator unlock and reset passwords for users, per Department of Homeland Security (DHS) *Information Technology Security Program Publication, 4300A.*		**X**	**Medium**
FEMA-IT-06-10	settings on machines running Microsoft Windows 2000 Professional prevented the user's ability to disable the password protected screensaver; however the settings did not prevent the user's ability to change the inactivity threshold. The implementation of a password protected screensaver as a mitigating control for lacking a second form of authentication is not sufficient if users	Complete a review over all settings for Microsoft Windows 2000 users and ensure that all settings are properly applied to those users, including disabling the user's ability to change the inactivity threshold of the password protected screensaver.		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	have the ability to change the inactivity threshold greater than the FEMA standard of fifteen minutes. This weakness impacts				
FEMA-IT-06-11	• Password configurations for the application have been configured to permit passwords to be a minimum of six characters in length which is not in compliance with Department of Homeland Security (DHS) Information Technology Security Program Publication, 4300A. • Access authorizations for are not consistently documented and maintained on file. We noted that FEMA Form 20-24, User Access Control Form, was not completed for three (3) out of a sample of twenty-five (25) new user access request forms for .	• Configure the application to require a password to be a minimum of eight characters in length to be in compliance with DHS Information Technology Security Program Publication, 4300A Password Policy. • Ensure that user access is only granted upon completion of FEMA Form 20-24, User Access Control Form, and evidence of supervisory authorization. In addition, the access request forms should be retained for at least one year.	**X**		**High**
FEMA-IT-06-12	No policies or procedures exist to periodically review NEMIS access listings to determine if access is still required or if access levels commensurate with users' job responsibilities. We noted that NEMIS user access lists have not been reviewed to determine if access is still required or if access levels commensurate with users' job responsibilities.	Develop and implement procedures regarding periodic review of access lists. The policy should require that a master listing of all users is periodically reviewed to determine whether logical user access to is valid, consistent with job responsibilities, and according to the least privilege principle. Additionally, a review of all user accounts should be performed at least annually.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-06-13	Twenty-nine (29) terminated or separated FEMA employees and contractors maintain active [redacted] user accounts. Additionally, we noted that two (2) terminated or separated FEMA employees maintain active [redacted] user accounts. The implementation of FEMA Instruction 1540.3 as a form of access controls review is not sufficient because FEMA is only performing reviews over current year terminations and separations, and has not performed reviews over legacy users to ensure that all users have valid access.	• Complete a review over all existing FEMA application users' access to ensure that access to each respective application is warranted. • Per FEMA Instruction 1540.3, perform a review of authorized accounts on a semi-annual basis and remove terminated employees' access to all FEMA systems.		**X**	**High**
FEMA-IT-06-14	[redacted] software request forms were not consistently approved by supervisors. We noted that FEMA Software Tracking Form, did not have supervisor approval prior to receiving software for eight (8) out of a sample of fifteen (15) [redacted] software request tickets, which is not in compliance with the FEMA Policy – Procedures for Removal and Return of Storage Media from and to the Library, as well as DHS Information Technology Security Program Publication, 4300A.	Enforce the requirement for written email approval by a supervisor for all [redacted] software requests to comply with FEMA Policy – Procedures for Removal and Return of Storage Media from and to the Library.	**X**		**High**
FEMA-IT-06-15	• Deposits and withdrawals of [redacted] and [redacted] backup tapes are not authorized or logged. • [redacted] and [redacted] backup tapes are not rotated to an offsite location.	• Develop and implement procedures to authorize and log the withdrawal of [redacted] and [redacted] backup tapes. The policy should require that a documented backup inventory for [redacted] and [redacted] is maintained, a log for	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		the deposit and withdrawal of and backup tapes, and documented procedures for the delivery and pickup of and backup tapes. • Upon implementation of the Data Center's "real-time" back-up facility, create redundant servers at the Data Center for the and servers located at .			
FEMA-IT-06-16	FEMA Policy - Sanitization and Release of Electronic Storage Media has not been finalized or implemented and is currently in draft form.	Ensure that FEMA Policy - Sanitization and Release of Electronic Storage Media is finalized, and promulgated to necessary FEMA personnel.	**X**		**Medium**
FEMA-IT-06-17	No formally documented configuration management plan is in place for . FEMA has informal configuration management procedures for ; however they have not been formally documented.	Develop and implement formal policies and procedures over the configuration management process modeled after the informal configuration management process currently in place.	**X**		**High**
FEMA-IT-06-18	• A documented configuration management plan is in place for ; however, it is currently in draft form. We noted that the plan has multiple sections where input from FEMA personnel is requested by the Contractor who created the plan, however, FEMA has not responded back to these requests.	• Finalize the formal policies and procedures over the configuration management process to be in compliance with DHS Information Technology Security Program Publication, 4300A. • Develop and implement formal policies and procedures for restricting access to system software, and promulgate it to all needed personnel, to be in compliance with	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Additionally, the [redacted] configuration management plan was created in 1998 and needs to be updated to reflect the current [redacted] environment. • No documented policies and procedures are in place for restricting access to system software. • No documented [redacted] Patch Management Policy has been documented.	DHS Information Technology Security Program Publication, 4300A. • Develop and implement formal [redacted] patch management policies and procedures in accordance with DHS Information Technology Security Program Publication, 4300A.			
FEMA-IT-06-19	No formally documented policies and procedures are in place for restricting access to [redacted] system software	Develop and implement formal policies and procedures for restricting access to [redacted] system software, and promulgate it to all needed personnel, to be in compliance with DHS Information Technology Security Program Publication, 4300A.	**X**		**Medium**
FEMA-IT-06-20	[redacted] application programmers/configuration management group responsible for maintaining and developing changes for [redacted] are also responsible for migrating application code changes into the production environment. We noted that the Contractor uses the username, [redacted] within the [redacted] Unix environment to deploy application code changes into the [redacted] production environment.	Limit the Contractors access to the [redacted] production environment to "read only" and segregating the responsibility for deploying application code changes into production from the Contractor to an independent control group.	**X**		**High**
FEMA-IT-06-	No formal investigation procedures are in place to review suspicious system	Develop and implement formal policies and procedures to review suspicious system software	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
21	software activities or suspicious access activities for [redacted].	and access activities for [redacted] to be in compliance with DHS Information Technology Security Program Publication, 4300A.			
FEMA-IT-06-22	• No documented policies and procedures exist to monitor sensitive access and system software utilities for [redacted] • No formal investigation procedures are in place to review suspicious system software activities or suspicious access activities for [redacted].	• Develop and implement formal policies and procedures to monitor sensitive access and system software utilities for [redacted] to be in compliance with DHS Information Technology Security Program Publication, 4300A. • Develop and implement formal investigation policies and procedures to review suspicious system software and access activities for [redacted] to be in compliance with DHS Information Technology Security Program Publication, 4300A.	**X**		**Medium**
FEMA-IT-06-23	No documented SDLC has been developed for [redacted]	Develop, implement and establish a documented SDLC methodology for [redacted] as well as incorporating security planning throughout the life cycle. Furthermore, ensure that the SDLC methodology is promulgated to all personnel involved in the design, development, and implementation process on the SDLC methodology.	**X**		**High**
FEMA-IT-06-24	No documented SDLC has been developed for [redacted].	Develop, implement and establish a documented SDLC methodology for [redacted] as well as incorporating security planning throughout the life cycle. Furthermore, ensure that the SDLC methodology is promulgated to all personnel involved in the design, development, and	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		implementation process on the SDLC methodology.			
FEMA-IT-06-25	Emergency exit and re-entry procedures are not effective for the data center housing the production and test servers. The current procedures do not provide detailed information regarding the exact procedures needed to re-enter the data center after leaving the facility for an emergency.	Develop and implement detailed emergency exit and re-entry procedures for the data center housing the production and test servers which accurately portrays the controls around re-entry into the data center. Once these procedures have been developed they must be promulgated to all data center operators as well as displayed throughout the data center.	**X**		**Medium**
FEMA-IT-06-26	Excessive access has been granted to We identified one member of Group 0001 who does not have a real business need to have access to this function. We informed the Financial Services Branch (FSB) of the excessive access and noted that FSB removed the user with excessive access. We noted that corrective action has been taken and completed in the current fiscal year; however, this issue posed a risk for a majority of the fiscal year and therefore will be reported as a weakness for FY 2006.	• Ensure that the system administrator privileges remain restricted to only the minimum number of users necessary to achieve the principle of least privilege. • Develop procedures to perform routine monitoring of the system administrator accounts in .	**X**		**Medium**
FEMA-IT-06-27	Twenty-one (21) users in Group 0002 and eight (8) users in Group 0003 have the ability to gain access to the account mapping functions and make changes to the account tables. Of the 21 users in Group	• Implement a solution to limit the excessive access to the online account mapping functions and the ability to make offline changes to the general ledger account tables. Access rights should be periodically			**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	0002, nine (9) users do not have a real business need to have access to this function. The 9 users that appear to have excessive access consist of developers or others with system administrative access. Additionally, of the 8 users in Group 0003, six (6) users do not have a real business need to have access to this function. Additionally, excessive access is designed to be permitted within I to make offline changes to the general ledger account tables via the . Currently, we identified five (5) users in the group that have the ability to make offline changes to the general ledger account tables. Of the five users, four (4) users do not have a real business need to have access to this function.	reevaluated and limited to people who have a business need. • Develop procedures to perform routine monitoring over access to the online account mapping functions and general ledger account tables.			
FEMA-IT-06-28	user access request forms were not consistently completed prior to granting access to . Specifically, two (2) out of a sample of thirteen (13) did not have a supervisor's approval.	Ensure Enterprise System Access Request forms are only provided to the Department of Treasury for granting access upon completion of the access request form with evidence of supervisory authorization.	**X**		**Low**
FEMA-IT-06-29	• An applicant's homeowner's insurance status is not verified prior to	• Ensure that applicant's homeowner's insurance status is verified by developing and	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	granting disaster housing assistance. • The automated home ownership verification check within [redacted] failed by (a) misidentifying a renter as a homeowner and (b) failing to verify home ownership status for a valid homeowner.	implementing procedures to establish a centralized database to verify applicant's homeowner's insurance status. • In conjunction with a contractor, develop and implement a reliable method of obtaining accurate and up to date home ownership information.			
FEMA-IT-06-30	• Visitor logs are not maintained to the LAN room at [redacted] LAN Data Center in [redacted]. • One separated CSC personnel retained physical access to the Lanham facility; however, this individual did not have access privileges to the LAN room. • Management does not periodically review physical access listings to determine if access is still required or if access levels are commensurate with users' job responsibilities.	• Develops policies and procedures requiring all visitors to sign in and out on the visitors log when entering and leaving the computer/server room. • Maintains visitor logs for the LAN room at [redacted] LAN Data Center in [redacted] • Develops and implements policies to inform the physical security personnel of separated individuals with access to NFIP facilities. • Develops and implements policies to periodically review physical access listings to determine if access is still required or if access levels are commensurate with users' job responsibilities.	**X**		**Low**
FEMA-IT-06-31	• The [redacted] application does not require password authentication separate from an initial Local Area Network (LAN) password authentication to identify and authenticate user access. • No audit trails documenting user	• Implements a separate password authentication for the [redacted] application with password parameters that are in compliance with DHS Information Technology Security Program Publication, 4300A. • Develops and implements policies and	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	actions or actual or attempted access are maintained or reviewed. • The [redacted] application does not timeout after a period of inactivity. • Password protected screensavers are not operating on all NFIP desktops. • Information owners do not periodically review access authorization listings to determine if access is still required or if access levels commensurate with users' job responsibilities. • [redacted] does not disable accounts after a period of inactivity, such as 90 days.	procedures to monitor or review sensitive activity, such as transaction activities, changes to security profiles, and actual or attempted access. • Implements a session termination after the DHS required period of inactivity. • Requires and enforces that all workstations use a password protected screensaver that is activated after the DHS required period of inactivity. • Develops and implements policies and procedures regarding periodic review of [redacted] access lists in order to determine whether logical user access is valid. • Configures the [redacted] application to disable inactive accounts in accordance with DHS 4300A.			
FEMA-IT-06-32	• Information owners do not periodically review access authorization listings to determine if access is still required or if access levels commensurate with users' job responsibilities. • Does not disable accounts after a period of inactivity, such as 90 days. • Does not enforce the DHS password requirements beyond the use of 8 characters. • Does not have a session timeout after the DHS required period of inactivity. • Audit trails are not reviewed in	• Develops and implements policies and procedures regarding periodic review of [redacted] application access lists in order to determine whether logical user access is valid, consistent with job responsibilities, and in accordance with the principle of least privilege. • Configures the [redacted] application to automatically disable inactive accounts in accordance with DHS 4300A. • Configures [redacted] password requirements to meet DHS requirements. • Identifies and implements system capabilities to terminate sessions after a period of	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	accordance with Production Systems Control (PSC) and DHS policy.	inactivity. • Performs reviews of audit trails documenting user actions, including changes to security profiles and actual or attempted unauthorized, unusual, or sensitive access. Documents and maintains reviews and investigations of suspicious activity.			
FEMA-IT-06-33	Segregation of duties controls were not implemented for the [redacted] General Ledger application, such as establishing user roles and groups.	• Identify and document incompatible duties, and system roles and responsibilities within [redacted]. • Develop and implement policies and procedures segregating incompatible duties within [redacted], to be in compliance with DHS Information Technology Security Program Publication, 4300A. • Identify and implement capabilities within [redacted] that enforce segregation of incompatible duties.	**X**		**High**
FEMA-IT-06-34	The current program build of [redacted] Corporate Edition for the NFIP local area network (LAN) program build had Security Advisory [redacted] issued about it on June 6, 2006, indicating that a security flaw had been identified allowing a remote or local attacker to execute code on an affected system.	• Develops and implements policies to monitor, test, and install updates to [redacted] Corporate Edition. • When implementing an update, ensures that patches are successfully installed on all LAN servers and workstations in a timely manner.	**X**		**Medium**
FEMA-IT-06-35	• [redacted] change management procedures are not documented. • Installation of the new version of [redacted] in FY 2006 was not formally	• Develops and implements change management procedures around [redacted] and formally documents approvals to changes prior to installing new versions in the production	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	approved by users. • Installation of the operating system upgrade in FY 2006 was not formally documented or approved.	environment. • Develops and implements change management procedures over system software changes and establishes documented approvals prior to installing or upgrading system software.			
FEMA-IT-06-36	• Five of 15 selected mainframe changes did not have documented requestor's change approval on the Operations Service Request (OSR) forms. • NFIP mainframe baseline configuration document has not been updated to reflect the current environment.	• Documents and implements change management procedures requiring approvals prior to implementing changes in the production environment. • Develops and implements policies and procedures requiring update to the mainframe baseline configuration document when there is a change to the environment.	**X**		**Medium**
FEMA-IT-06-37	Excess access was identified to following Transaction Record Reporting and Processing accounts: • [redacted] • [redacted]	• Implements the recommendations from the table provided in the condition above, in order to mitigate excessive access to sensitive mainframe production members. • Develops and implements procedures to perform a periodic review of access to mainframe production datasets to determine whether access is valid, consistent with job responsibilities, and according to the least privilege principle.	**X**		**Medium**
FEMA-IT-06-38	There are no individual user accounts for LAN administrator access and that the generic "[redacted]" account is shared amongst the three administrators. Furthermore, the LAN has the capability to maintain system activity logs; however,	• Creates additional [redacted] user accounts to allow for accountability while performing [redacted] duties. • Regularly reviews system activity logs over [redacted] accounts in order to	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	system administrators do not regularly review the logs.	detect attempted malicious activity or other security breaches.			
FEMA-IT-06-39	Access to the excel files that calculate the Loss and Loss Adjustment Expense appears excessive. Specifically, we identified that modify and write access permissions to the excel files appear inappropriate for six people of the Bureau of Finance and Statistical Control group.	Restricts access to the Loss and Loss Adjustment Expense ("LAE") Reserves Estimates excel files to the Actuary and Finance Director in order to achieve the principle of least privilege.	**X**		**Medium**
FEMA-IT-06-40	No formal change control procedures are in place to authorize, test, verify, and approve program changes made to the Loss and Loss Adjustment Expense Reserves excel files.	Develop and implement a formal change control procedures around the Loss and Loss Adjustment Expense excel files. Change procedures should at a minimum include procedures to formally authorize, test, and document changes prior to the change being implemented.	**X**		**Medium**
FEMA-IT-06-41	• Visitor logs are not maintained to the [redacted]'s raised floor data center in [redacted]. • Two separated CSC personnel retained physical access to the [redacted] facility.	• Develops and implements policies and procedures requiring all visitors to sign in and out on the visitors log when entering and leaving the computer/server room. Maintain visitor logs for the [redacted]'s raised floor data center in [redacted]. • Develops and implements policies to ensure that physical security personnel are consistently informed of separating individuals, including those terminated through a reduction in force. • Ensures that separated individuals' physical	**X**		**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		access to the facility is being consistently and timely removed.			
FEMA-IT-06-42	• Information owners do not periodically review access authorization listings to determine if access is still required or if access levels are commensurate with users' job responsibilities. • Audit trails are not reviewed in accordance with DHS policy. • Excessive access to the [redacted] on the [redacted] mainframe was provided to 1 security administrator and 31 operations personnel.	• Develops and implements policies and procedures regarding periodic review of [redacted] mainframe access lists in order to determine whether logical user access is valid, consistent with job responsibilities, and in accordance with the principle of least privilege. • Performs reviews of audit trails documenting user actions, including changes to security profiles and actual or attempted unauthorized, unusual, or sensitive access. Documents and maintains reviews and investigations of suspicious activity. • Ensures access to the [redacted] dataset is limited to those personnel that require an elevated level of access in the system.	**X**		**Medium**
FEMA-IT-06-43	One of the eight requested exit checklists used to ensure that all physical and logical access of terminated personnel is removed was not provided.	Perform corrective actions to improve coordination efforts between the [redacted] Data Center and the CSC Human Resources department and to ensure that exit checklists are available for all terminated/separated personnel.	**X**		**Low**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 Information Technology
Notification of Findings and Recommendations – Detail

- **Consolidated**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 Information Technology
Notification of Findings and Recommendations – Detail

Consolidated

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CONS-IT-06-01	Two members of DHS OFM had excessive access within DHS . We informed DHS OFM of the excessive access and noted that DHS OFM removed both users with excessive access. We noted that corrective action has been taken and completed in the current fiscal year; however, this issue posed a risk for a majority of the fiscal year and therefore will be reported as a weakness for FY 2006.	Ensure that the privileges assigned to DHS OFM and Department of Treasury users remain restricted to only the minimum privileges necessary to achieve the principle of least privilege.		**X**	**Low**
CONS-IT-06-02	new user access request forms were not consistently completed prior to granting access to . Specifically, one (1) out of a sample of eleven (11) did not have a supervisor's approval. Additionally, five (5) out of a sample of eleven (11) did not have security manager review.	Ensure that user access is only granted upon completion of the new user access request form with evidence of supervisory authorization and security manager's review. In addition, the access request forms should be retained.		**X**	**High**
CONS-IT-06-03	OFM has not developed procedures to periodically review access lists in order to determine whether user access is valid, consistent with job responsibilities and in accordance with the principle of least privilege	Develop and implement policies and procedures regarding periodic review of access lists in order to determine whether logical user access is valid, consistent with job responsibilities, and in accordance with the principle of least privilege.		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CONS-IT-06-04	During our audit, the following configuration management weaknesses were noted • Segregation of duties violations exists for twelve (12) out of twenty-five (25) system changes made outside of the scheduled Quarterly Releases. • Segregation of duties violations exists for four (4) out of ten (10) emergency system changes made outside of the scheduled Quarterly Releases. • Test documentation is not available for changes implemented outside of the scheduled Quarterly Releases.	• Segregate the duties of the lead developer of emergency and non-emergency software performed outside of the scheduled Quarterly Releases, therefore preventing the developer of a software change from testing their own work. • Ensure that DHS management follows the Department of , ASSC SDLC Workflow and Processes Handbook, and a higher degree of management oversight is utilized for the development and implementation of all changes over DHS • Maintain test plans and test results for all changes implemented outside of the scheduled Quarterly Releases.		**X**	**High**
CONS-IT-06-05	There are no documented procedures in place for DHS components to perform a formal review, by a separate approving individual, to verify the financial data to the general ledger 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, by separate approving official, to the general ledger before moving it into the Repository.		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CONS-IT-06-06	There are no individual user accounts for DBA access and that the generic " account is shared amongst the two DBAs.	Create an additional DBA user account to allow for accountability when migrating approved software changes into the production environment or while performing other DBA duties.	**X**		**High**
CONS-IT-06-07	The DHS Office of Financial Management (OFM) is not requiring users to formally acknowledge and sign the FARS ROB prior to being granted access to . We noted that eighteen (18) out of a sample of (20) users had not formally acknowledged and signed the FARS ROB document.	• Require all Federal and contract DHS users to acknowledge and sign the FARS ROB prior to being granted access to DHS . • Require all existing DHS users to acknowledge and sign the FARS ROB on a yearly basis	**X**		**High**
CONS-IT-06-08	• Password configurations for the application have been configured to permit passwords to be a minimum of six (6) characters in length which is not in compliance with Department of Homeland Security (DHS) Information Technology Security Program Publication, 4300A, which requires passwords to be a minimum of eight (8) characters in length. • application administrators lock out accounts if a user has not accessed the account after 180 days which is not in compliance with Department of Homeland Security (DHS) Information Technology Security Program Publication, 4300A, which requires administrators to lock out accounts if a user has not accessed the account after 90 days.	• Configure the application password parameters to be in compliance with DHS Information Technology Security Program Publication, 4300A. • Configure the application to lock out user accounts that have been inactive for 90 days to be in compliance with DHS Information Technology Security Program Publication, 4300A. • Promulgate DHS Information Technology Security Program Publication, 4300A and other DHS-wide information system security publications to the Department of Treasury Contractors in order to educate them in DHS information	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		system security requirements and to ensure they are implemented onto DHS and DHS .			
CON-IT-06-10	The password configurations for the application have been configured to not enforce passwords to have a combination of alphanumeric characters and special characters which is not in compliance with Department of Homeland Security (DHS) Information Technology Security Program Publication, 4300A, which requires that passwords contain a combination of alphabetic, numeric, and special characters.	Configure the application password parameters to be in compliance with DHS Information Technology Security Program Publication, 4300A.	**X**		**Medium**
CON-IT-06-11	Personnel with physical access to the production server, housed in the Department of Treasury Data Center are not periodically reviewed for appropriateness of access.	Ensure that the Department of Treasury develop and implement documented policies and procedures to periodically review the list of personnel with access to the Department of Treasury Data Center housing the production server to be in compliance with DHS Information Technology Security Program Publication, 4300A.	**X**		**Medium**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CON-IT-06-12	OFM does not maintain a termination/separated employee listing of OFM employees. As a result we were unable to perform a control test to determine if terminated/separated OFM employees have access to	DHS Office of the Chief Financial Officer should work with the DHS HR department in order to obtain a current listing of terminated or separated DHS OFM personnel and use that listing to determine if any terminated or separated DHS OFM personnel continue to have access to on a scheduled basis.	**X**		**High**
CON-IT-06-13	Department of Treasury media sanitization policies and procedures have not been developed for . We noted that media sanitization services are provided by Iron Mountain through Qwest; however, there are no specific media sanitization policies and procedures in place for the Department of Treasury to sanitize media.	The DHS Office of the Chief Financial Officer ensure that the Department of Treasury develop and implement media sanitization policies and procedures for in the event that DHS would like to sanitize media without using the services of Iron Mountain.	**X**		**High**
CON-IT-06-14	Department of Treasury media sanitization policies and procedures have not been finalized or implemented. We noted that the Department of Treasury policy entitled, "Memorandum: Destroying and Sanitizing Media" is currently in draft form.	DHS Office of the Chief Financial Officer ensure that Department of Treasury Policy - Memorandum: Destroying and Sanitizing Media is finalized, and promulgated to necessary personnel.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CON-IT-06-15	Discrepancies exist between the DHS Performance and Accountability Report (PAR) Guidance and the Analytical Report	• Implement the recommendations from the table provided in the condition above, in order to make the analytic report code, equations and PAR guide consistent. • Develop and implement a configuration management process over analytic report changes to ensure that changes to the report are formally documented and discrepancies can be more easily rectified.		**X**	**Low**
CON-IT-06-16	• We determined that normal balance type indicated on the DHS SGL for Account 4132 and Account 7280 differ from the normal balance type indicated on the US SGL. • We determined that 101 DHS SGL accounts were not found in the US SGL and reported a zero balance for period 9. These accounts do not appear to be currently used by DHS and/or do not appear to be related to DHS operations.	• Implement changes to the DHS SGL normal balance types of the accounts listed above in order to be in compliance with the USSGL. • Review the accounts listed in the DHS SGL and remove accounts that are not applicable to DHS operations. • Develop a procedure to verify the abnormal balance report logic after any changes in the DHS SGL or USSGL.		**X**	**Low**
CON-IT-06-17	Access to waive fatal errors using the [redacted] role appears excessive for two employees per OFM policy.	Access to waive fatal errors using the [redacted] role is limited to the Assistant Director of Financial Reporting Branch and the Assistant Director of Financial Management Coordination Branch, per the documented OFM policy.	**X**		**Medium**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CON-IT-06-18	DHS is non-compliant with the Federal Information Security Management Act	The DHS Chief Financial Officer (CFO), in coordination with the DHS Chief Information Officer (CIO) and other DHS functional leaders, continue to ensure that DHS place further emphasis on the monitoring and enforcement of policies and procedures through the performance of periodic security control assessments and audits.		**X**	**High**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 Information Technology
Notification of Findings and Recommendations - Detail

- **Federal Law Enforcement and Training Center**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 Information Technology
Notification of Findings and Recommendations – Detail

Federal Law Enforcement and Training Center

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-06-01	• No documented configuration management plan is in place for [redacted], including the following: - Lack of documented test plan standards and procedures; - Lack of a documented comprehensive set of test transactions; - Test results are not maintained and a documented approval for the test results does not exist; and - Lack of a description for the emergency change process. • We were unable to verify that an independent control group performed the migration of tested and approved [redacted] system software to the production environment. • We were unable to verify that access to [redacted] program libraries is restricted.	• Develop and implement FLETC specific policies and procedures over the [redacted] configuration management process in compliance with DHS Configuration Management policy. • Document a listing of all users with access to the [redacted] production environment. Ensure that access is prohibited to development staff and that an independent group deploys software changes into the production environment. • Document a listing of all users with access to the [redacted] program libraries. Ensure that access is prohibited to development staff.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-06-02	• No documented configuration management plan is in place for [redacted], including the following: - Lack of documented test plan standards and procedures; - Lack of a documented comprehensive set of test transactions; - Test results are not maintained and a documented approval for the test results does not exist; and - Lack of a description for the emergency change process. • We were unable to verify that access to [redacted] program libraries is restricted. We noted that a listing of users with access to the [redacted] production environment was unavailable.	• Develop and implement documented policies and procedures over the [redacted] configuration management process modeled after the informal configuration management process currently in place. • Document a listing of all users with access to the [redacted] program libraries. Ensure that access is prohibited to development staff.	**X**		**Medium**
FLETC-IT-06-03	The installation of [redacted] system software is not logged or reviewed by FLETC management.	Enable audit logging over the installation of [redacted] system software and ensure that logs are maintained and periodically reviewed by management.	**X**		**Medium**
FLETC-IT-06-04	The SDLC for [redacted] is currently in draft form.	• Finalize, and implement a SDLC methodology for [redacted], as well as incorporating security planning throughout the life cycle. • Ensure that the SDLC methodology is promulgated to all personnel involved in the design, development, and implementation process of the SDLC methodology.	**X**		**Medium**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-06-05	• [redacted] backups maintained onsite are not periodically tested. • FLETC does not utilize external labels to indicate the sensitivity of the information on the [redacted] backup compact discs (CDs).	• Periodically test the [redacted] backup compact discs maintained onsite in compliance with DHS Information Technology Security Program Publication 4300A. • Affix external labels to [redacted] backup CDs indicating the distribution limitations and handling caveats of the information in compliance with DHS Information Technology Security Program Publication 4300A.	**X**		**Medium**
FLETC-IT-06-06	The [redacted] contingency plan has not been tested.	Perform an adequate test of the [redacted] Contingency Plan, in compliance with DHS Information Technology Security Program Publication 4300A. Additionally, testing of the [redacted] Contingency Plan should be performed annually.	**X**		**Medium**
FLETC-IT-06-07	FLETC Manual 11041: Safeguarding Sensitive But Unclassified (For Official Use Only) Information is currently in draft form and has not been finalized or implemented.	Ensure that FLETC Manual 11041: Safeguarding Sensitive But Unclassified (For Official Use Only) Information is finalized and promulgated to necessary FLETC personnel.	**X**		**Medium**
FLETC-IT-06-08	We noted that incidents are not tracked from inception to resolution in an incident response management system.	Establish a documented incident response tracking mechanism in compliance with DHS Information Technology Security Program Publication 4300A.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-06-09	We noted that there are five (5) generic/shared accounts shared amongst the two database administrators (DBAs).	• Use unique DBA user accounts to allow for accountability when performing DBA duties on . • Document incompatible duties over and develop and implement policies and procedures that segregate the documented incompatible duties.	**X**		**High**
FLETC-IT-06-10	The following Telecom access control weaknesses were identified: • No policies and procedures are in place to request access to the Telecom Room. • No policies and procedures are in place to periodically review the list of persons with physical access to the Telecom Room. • No emergency policies and procedures are in place for the evacuation and re-entry of the Telecom Room. • No policies and procedures are in place to guide and document the emergency training of Telecom Room personnel.	• Develop policies and procedures regarding gaining access to the FLETC Telecom Room, including the use of a user authorization form. • Perform a semi-annual review of the FLETC Telecom Room access listing in compliance with DHS Information Technology Security Program Publication 4300A. • Develop and implement the emergency procedures that include exit and re-entry procedures into the Telecom Room. • Develop and implement policies and procedures to train Telecom Room staff in emergency procedures pertaining, but not limited to fire, water, and alarm procedures. Additionally, formalize this training by retaining documentation that all staff has completed the training.	**X**		**Medium**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-06-11	• No policies and procedures are in place over access authorizations to [redacted], [redacted] and the general support system hosting these applications. • No policies and procedures are in place to periodically review the list of [redacted] user accounts. • No policies and procedures are in place to immediately notify [redacted] System administrators when users are terminated or transferred. • Password configurations for [redacted] have been configured to permit passwords to be a minimum of six characters in length with no complexity requirements. • [redacted] users are locked out of the system after five (5) invalid logon.	• Ensure that FLETC Manual 4330: User Identification and Authentication Management is finalized, promulgated to all FLETC employees and enforced. • Configure the [redacted] applications to require a password to be a minimum of eight characters in length and contain a combination of alphabetic, numeric, and special characters to be in compliance with DHS Information Technology Security Program Publication, 4300A Password Policy. • Configure the [redacted] to lock out user accounts users after three (3) invalid login attempts to be in compliance with DHS Information Technology Security Program Publication, 4300A.	**X**		**High**
FLETC-IT-06-12	FLETC Directive (FD) 43220: IT System Security Awareness and Training is currently in draft form and has not been finalized or implemented.	Ensure that FLETC Directive (FD) 43220: IT System Security Awareness and Training is finalized, and enforced by having all new and existing FLETC users and contractors complete the training by May 31 of each year.	**X**		**Medium**
FLETC-IT-06-13	There are no established policies and procedures in place for the authorization and use of mobile code technologies. Currently, FLETC uses client side Java Applets in connection with [redacted].	Develop and implement FLETC specific policies and procedures over the authorization and use of mobile code technologies to be in compliance with DHS Information Technology Security Program Publication 4300A.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-06-14	There are no policies and procedures in place to review [redacted] audit logs for actual or attempted unauthorized or unusual access to sensitive data.	Develop and implement policies and procedures to proactively monitor sensitive access to system software utilities for [redacted] to be in compliance with DHS Information Technology Security Program Publication, 4300A.	**X**		**Medium**
FLETC-IT-06-15	There are no documented policies and procedures in place for restricting access to [redacted] system software.	Develop and implement policies and procedures for restricting access to [redacted] system software, and promulgate it to all needed personnel, to be in compliance with DHS Information Technology Security Program Publication, 4300A.	**X**		**Medium**
FLETC-IT-06-16	Incompatible duties and roles identified within the [redacted] application have not been documented and no policies and procedures exist to segregate incompatible duties and roles.	• Identify and document incompatible duties and system roles and responsibilities within the [redacted] application. • Develop and implement policies and procedures segregating incompatible duties within [redacted] to be in compliance with DHS Information Technology Security Program Publication, 4300A.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-06-17	An established sanctions process for personnel failing to comply with established information security policies and procedures does not exist. However, we noted that FLETC Manual 4900, Information Technology System Rules of Behavior (ROB) and Use Agreements, was finalized in August 2006 and establishes disciplinary actions they could be subject to if the ROB are not followed. We noted that the policy is finalized but has yet to be implemented.	• Implement FLETC Manual 4900, Information Technology System ROB and Use Agreements, require all existing Federal and contract employees who use the FLETC LAN to acknowledge and sign the ROB. • Require all new Federal and contract employees who use the FLETC LAN to acknowledge and sign the ROB prior to being granted access to the FLETC LAN.	**X**		**Medium**
FLETC-IT-06-18	There are no FLETC specific established policies and procedures in place for the use and installation of [redacted] We noted that FLETC is currently using the Defense Information Systems Agency (DISA) [redacted] Telephony & [redacted] Guide and the FLETC VoIP Security Checklist for the use and installation of [redacted]. Currently, this technology is used at three FLETC sites and is all interconnected through the FLETC Wide Area Network (WAN), which has a direct connection with [redacted].	• Develop and implement FLETC specific policies and procedures over the authorization and use of [redacted] to be in compliance with DHS Information Technology Security Program Publication, 4300A, and NIST SP 800-58. • Conduct a security inspection of the [redacted] VoIP installations by completing the VoIP Security Checklist for each site.	**X**		**Medium**
FLETC-IT-06-19	We noted that twelve (12) out of a sample of (15) FLETC contractors did not have evidence that a background investigation was initiated or completed.	Perform background checks on all new and existing contractors ensuring that background checks and periodic re-investigations are performed in a timely manner and that supporting documentation be maintained.	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-06-20	We noted that a user of the [redacted] Fixed Assets module has the ability to change the useful life field during the asset entering process.	• Disable the user's ability to manually edit the depreciation useful life field during the asset entering process within the [redacted] Fixed Assets module. • Ensure that changes made after the asset entering process to the depreciation useful life in years undergo a documented change process with evidence of supervisory approval.	**X**		**Medium**
FLETC-IT-06-21	The following [redacted] access control weaknesses were identified: • No policies and procedures are in place to review [redacted] server level system software audit logs for successful or unsuccessful access attempts. • No audit logs are maintained to capture actual or attempted unauthorized, unusual or sensitive access within the [redacted] application level.	• Develop and implement policies and procedures to proactively monitor actual or attempted unauthorized, unusual or sensitive access to system software utilities for [redacted] to be in compliance with DHS Information Technology Security Program Publication, 4300A. • Ensure that management performs manual auditing of the Oracle database tool the [redacted] application resides on.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-06-22	During technical testing, configuration management weaknesses were identified on the databases supporting the [redacted] applications, as well as supporting servers. Specifically, databases and servers were identified with account management, auditing, database configuration and password management weaknesses.	• Implement the corrective actions noted in the findings. • Perform periodic scans of the FLETC network environment, including the financial processing environment, for the identification of vulnerabilities, in accordance with NIST SP 800-42. • Implement corrective actions to mitigate the risks associated with any vulnerabilities identified during periodic scans.	**X**		**High**
FLETC-IT-06-23	During technical testing, patch management weaknesses were identified on hosts and databases supporting the [redacted] applications. The fact that these vendor supplied patches have not been applied in a timely manner could allow a remote attacker to gain unauthorized access on the host or database.	• Implement the corrective actions noted in the findings. • Perform periodic scans of the FLETC network environment, including the financial processing environment, for the identification of vulnerabilities, in accordance with NIST SP 800-42. • Implement corrective actions to mitigate the risks associated with any vulnerabilities identified during periodic scans.	**X**		**High**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 Information Technology
Notification of Findings and Recommendations - Detail

- **Grants and Training (G&T) – Under Preparedness**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 Information Technology
Notification of Findings and Recommendations – Detail

Grants and Training (G&T) – Under Preparedness

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
G&T 06-01	The Plan of Action and Milestones (POA&M) report for G&T does not identify the scheduled completion date, and/or the status of corrective action taken for each IT weakness listed on the POA&M report.	• Follow OMB policy in regards to reporting and tracking all security weaknesses identified during any reviews done by, for, or on behalf of the agency, in the G&T POA&M reports. • Do not remove any POA&M weakness until the corrective action taken by G&T to mitigate the identified POA&M weakness has been verified. Additionally, if the POA&M weakness was identified by the OIG during an audit, then the POA&M weakness cannot be removed until the OIG has verified and validated that the corrective action has mitigated the weakness.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
G&T 06-02	G&T does not have a signed waiver in place as part of their Interagency Agreement (i.e. MOU) to mitigate the issue of their lack of compliance with NIST Special Publication (SP) 800-53 "Recommended Security Controls for Federal Information Systems" security controls.	Revise the Interagency Agreement (i.e. MOU) to include the following: • Any updates made to federal laws/regulations the service level provider (i.e. OJP) should ensure all General Support Systems (GSS) and Major Applications (MA) are in compliance. If not, then a waiver should be documented by G&T to mitigate the issue of non-compliance with DHS laws/regulations. The revised Interagency Agreement (i.e. MOU) should be agreed upon and communicated between appropriate G&T and the Department of Justice (DOJ), Office of Justice Personnel (OJP) personnel.	**X**		**High**
G&T 06-03	We identified that all 45 G&T users (17 , 11 Integrated and 17) recertification forms contained one of the following weaknesses; original access level/privileges assigned were not documented on the form, and the user privileges were notated as deleted on the form but still active on the access listing. In addition, the recertification process was not performed on a semi-annual basis as stipulated by the OJP's recertification process.	Perform a review of all user accounts and associated access levels within the and applications on an appropriate, periodic basis.	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
G&T 06-04	We identified 14 out of 15 remote users, did not have an authorized remote access form on file. Specifically, we noted that the forms were missing signatures from the employee and his/her supervisor.	Ensure procedural improvements have been made for ensuring supervisor and employee signatures are obtained for all remote access requests.	**X**		**High**
G&T 06-05	We identified 1 out of 6 terminated employees who had a missing requestor signature on their SF-52 form. In addition, we identified 6 out of 6 terminated employees who did not sign their DHS 400-2 exit clearance form upon departure.	Ensure procedural improvements have been made for ensuring supervisor and employee signatures are obtained for exit clearance forms.	**X**		**Medium**
G&T 06-06	The following weaknesses were identified as a part of the FY 2006 Department of Justice, Office of Justice Programs (OJP) Financial Statement Audit and impact the reliance G&T has on OJP's IT control environment: Access Controls: • Procedures for Generic User Accounts Not Documented. • Periodic Recertification of OJP Application and System Accounts Not Consistently Performed. • OJP does maintain log of changes to security profiles. Application Change Controls: • Application and System Change Controls Procedures and Processes Need Improvement.	Revise the Interagency Agreement (i.e. MOU) to include the minimum-security related responsibilities. The agreement should be revised to include the description and related responsibility for the following components: • Description of Services • Description of Processing Services • Security Services • Software Development and Maintenance Support • List of applications to be processed • Help desk support • Service Level Objectives • Communications support (LAN, WAN) • Continuity of Operations/Disaster Recovery The MOU should be agreed upon and communicated to the appropriate G&T personnel. In addition, G&T should continue to		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Service Continuity: • Tape Backup Polices and Procedures and Documentation Storage Requirements Need Enhancement. System Software: • General Support System Configurations Need Enhancement.	work with OJP to ensure all weaknesses that impact G&T reliance on the OJP IT control environment are mitigated and corrected.			
G&T 06-07	1 out of 6 G&T terminated employees access was not removed from the [redacted] application within a timely manner (i.e. two business days).	Pursue methods for improving the process to notify the G&T Security Administrator that an employee or contractor has been transferred or has terminated employment with DHS G&T and no longer requires system access to [redacted]			**High**
G&T 06-12	Three users who have been assigned privileges that allow them to enter, modify, and approve journal vouchers. According to their job functions and responsibilities, these users should only have the ability to enter journal vouchers. In addition, two users who have been assigned privileges (e.g. [redacted]) that allow them to modify vendor tables, and allow them to open and close fiscal years.	Adjust/modify or remove the access levels for the individuals identified in the condition.		**X**	**High**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 Information Technology
Notification of Findings and Recommendations – Detail

- **Transportation Security Administration**

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Department of Homeland Security
FY2006 Information Technology
Notification of Findings and Recommendations – Detail

Transportation Security Administration

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA 06-01	The [redacted] Business Contingency and Disaster Recovery Plan (collectively referred to as the DRBC) is approximately 70% completed, with full completion expected by September 30, 2006. Because the plan is in draft form it has not yet been tested, and a tabletop exercise has been planned upon completion of the DRBC.	• Finalize and implement the DRBC and ensure that it reflects changes in hardware and software and addresses disaster recovery procedures for [redacted]'s key financial systems. • Identify an alternate processing site and document associated restoration procedures. • Periodically test the DRBC and evaluate the results of the testwork so that the DRBC can be adjusted to correct any deficiencies identified in testing.		**X**	**High**
TSA 06-02	A comprehensive incident capability that includes designated response team members and procedures for incident handling to help ensure that the incident is properly handled has not been documented and implemented. [redacted] management has acknowledged this issue and is currently developing a draft incident response capability.	• Develop an incident response capability that includes: - Designation of response team members; - Training for team members; and - Procedures for incident handling, including preparation, containment, eradication, recovery and follow-up activities. • Approve and implement the incident response capability at the [redacted].	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA 06-03	• emergency procedures are in place for the evacuation of and its Data Center. However, no emergency re-entry procedures exist within this directive. • No policies and procedures are in place to guide and document the emergency training of Data Center personnel. • Weaknesses exist in the implementation of least privilege regarding granting access to the Data Center personnel. Specifically, two out of the fifteen personnel forms selected, granted twenty-four hour access to individuals on the janitorial staff.	• Finalize and implement the emergency procedures that include re-entry procedures into the Data Center. • Develop and implement policies and procedures to train Data Center staff in emergency procedures pertaining, but not limited to fire, water, and alarm procedures. Additionally, formalize this training by retaining documentation that all staff has completed the training. • Continue to limit entry to the Data Center, especially after normal business hours, to critical personnel only.	**X**		**Medium**
TSA 06-04	Although backup tapes for the Coast Guard General Support System (GSS) are created on a regular basis, testing procedures have not been documented in accordance with Instruction. Additionally, although CAS backup tapes are rotated offsite to the GSS backups have not been included in the tape rotation process to the . Although a tape rotation schedule and tape rotation procedures have been documented, the tape transfer logs are not being completed in their entirety to note the tape numbers and the number of tapes being rotated offsite.	• Develop and document comprehensive backup procedures, which include testing the GSS backup tapes on a regular basis, at least annually. • Enforce the tape rotation procedures to ensure that tape transfer logs are completed and perform a weekly review to ensure that the logs are completed in their entirety before the tapes are sent to the • Include the GSS backup tapes in the weekly offsite tape rotation to the . Update the tape transfer log to include the GSS backup tapes that will be included in the rotation.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA 06-05	Configuration weaknesses over [redacted] workstations allowed users to modify sensitive workstation system and security settings. During our test work, using a [redacted] network user account provided with ordinary privileges, we were able to successfully: • Disable the desktop's anti-virus; • Change the screen saver setting to remove the password-locking feature; and • Increase the time period for the screen saver activation significantly. Upon notification, [redacted] management took immediate action to correct the configuration settings.	• Develop and implement a configuration checklist for the anti-virus server. • Perform periodic audits of the anti-virus and workstation security settings to ensure appropriate configurations are maintained.	**X**		**High**
TSA 06-06	Weaknesses were noted in regard to [redacted] personnel entrance and exit procedures for civilian, contractor and military personnel. Specifically, out of fifteen entrance check-in sheets inspected, thirteen were incomplete or did not exist. Additionally, out of fifteen exit check-out sheets inspected, only four were received from our sample selection, and none of which were complete.	• Continue with efforts to improve the implementation of the personnel entrance and exit procedures and a more formalized chain of command for the collection of the check-in and check-out sheets. • Track and monitor the completion of check-in and check-out sheets. • Ensure that personnel indicate which line items on the check-in/check-out sheets are not applicable. • Retain Check-out sheets for up to a year after an employee's departure.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA 06-07	A [redacted] Security Configuration Management Plan does not exist that clearly delineates the roles and responsibilities between [redacted], and the [redacted]. GCE is the organization under contract by Coast Guard to manage the [redacted] software programs. Consequently, the System Security Plans for the [redacted] applications do not include key security control information. Specifically, the plans do not include information on the current security configuration management process, including delineation of responsibilities for all involved parties.	Implement corrective actions to implement a [redacted] Security Configuration Management Plan that includes the role and responsibilities of [redacted]. Also, the plan should address both [redacted] and their associated operating systems and databases. Subsequently, the [redacted] System Security Plans should be updated to reflect the approved information in the [redacted] Security Configuration Management Plan.	**X**		**High**
TSA 06-08	During technical testing patch management weaknesses were identified on hosts supporting the [redacted] applications. Many of these vulnerabilities could allow a remote attacker to gain full control of the affected host and could lead to the compromise of the availability, confidentiality and integrity of [redacted] data.	• Implement the corrective actions noted in the tables above. • Implement polices and procedures to ensure that the software builds created by the software developer are tested to ensure that all software security configurations, such as software patches and non-compliant settings, are up to date. • Continue the process for performing periodic scans of the [redacted] network environment, including the financial processing environment, for the identification of vulnerabilities, in accordance with NIST SP 800-42. • Implement corrective actions to mitigate the risks associated with any vulnerabilities identified during periodic scans.		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA 06-09	During technical testing configuration management weaknesses were identified on hosts supporting the [redacted] applications. Specifically, servers were identified with excessive access privileges, and password and auditing configuration weaknesses.	We recommend that TSA ensure and verify that Coast Guard's [redacted] complete the following corrective actions: • Implement the corrective actions noted in the tables above. • Implement polices and procedures to ensure that the software builds created by the software developer are tested to ensure that all software security configurations, such as software patches and non-compliant settings, are up to date. • Continue the process for performing periodic scans of the [redacted] network environment, including the financial processing environment, for the identification of vulnerabilities, in accordance with NIST SP 800-42. • Implement corrective actions to mitigate the risks associated with any vulnerabilities identified during periodic scans.		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA 06-11	The [redacted] & Treasury MOU addresses the development, management, operation, and security of a connection between systems owned by both parties. The previous agreement expired in April of 2006 and a current MOU between [redacted] and Treasury has not been completed, although finalization is in the process. With the renewal of the MOU, [redacted] is also creating an ISA which will further define the technical details of the systems interconnection.	Ensure and verify that Coast Guard's [redacted] complete planned corrective actions to finalize and obtain all approvals for the MOU and ISA between [redacted] and Treasury-FMS Financial Management Service.	**X**		**Low**
TSA 06-12	[redacted] contracts the maintenance of their information systems software and hardware for the Superdome Supercomputer, which houses the four production databases including the [redacted] production database, to Hewlett Packard (HP) through two separate service agreements. One of the service contracts is valid until 2007 for a segment of their computer software and hardware. However, the second portion of [redacted] 's Superdome equipment is covered under a maintenance contract that expired on May 31, 2006.	• Continue to communicate with Coast Guard Headquarters in order to convey the importance of a timely renewal of the maintenance contract. • Maintain a continuous service contract for the hardware and software with the current vendor by anticipating delays in contract renewal and submitting requests for procurement in a timely manner.	**X**		**Low**
TSA 06-13	• Manager Review of System Administration Monitor Procedures have been developed that guide managers in performing periodic system administration monitoring reviews. However, the procedures do not note the periods of review that are being monitored, who is responsible for performing the reviews and evidence that the manager review was performed could only be	• Revise the Manager Review of System Administration Monitor Procedures to note how often managers should perform system administration monitoring reviews. Additionally, the procedures should note the titles/positions of the individuals who are authorized and responsible for performing the reviews and what type of documentation should be retained as a		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	obtained for March 2006. Additionally, although the manager reviews were implemented in March 2006, for the first half of the fiscal year, October through March, [redacted] system administration monitoring was not performed by a manager or group outside of the three systems administrators during that time period. • The access request form for one out of four individuals granted access to [redacted] since October 1, 2005, did not contain the supervisor's approval. • The account of a contractor that left [redacted] in October 2005 remained active until May 2006.	result of the review. • Continue enforcing [redacted] Instruction 5230.3 – Policy for System Level Access to [redacted] Computer Assets. Additionally, review the access request forms before the request is implemented to ensure that the request contains a supervisor approval and notes the level of access/privileges that the individual should be granted. • Continue enforcing [redacted] Instruction 5230.3 – Policy for System Level Access to [redacted] Computer Assets to ensure that the accounts of terminated civilians/contractors/military personnel are revoked in a timely manner.			
TSA 06-14	During our audit, the following [redacted] access control weaknesses were noted: • Password configurations for application and database were configured to permit passwords to be a minimum of six characters in length which is not in compliance with the [redacted] Password Policy Standard Operating Procedure (SOP). • Users are not locked out of their [redacted] application accounts after three invalid logon attempts. • Audit logging has not been enabled with in the [redacted] application or database. • Individuals who are no longer employed	• Continue with efforts to correct the implementation of the lockout policies and procedures to ensure that users are locked out of their accounts after three invalid attempts. • Establish detailed procedures for audit trail generation, review and management. The procedures should discuss the conditions under which the audit trails should be generated, reviewed, the frequency of the reviews, and the basis for determining when suspicious activity should be investigated. • Develop and implement access control procedures for the [redacted] system and database accounts. These procedures	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	with [redacted] were found to have active accounts with in [redacted]. Although their application accounts have been disabled, one civilian and one contractor retained open and active database accounts after their departure from [redacted]. • [redacted] account reviews have not been performed on a periodic basis for [redacted] personnel.	should include, at a minimum, steps for removing the accounts of terminated individuals. Additionally, the procedures should include information regarding the notification of both internal and remote user terminations. • Develop and implement access control procedures for the [redacted] system and database accounts. These procedures should include, at a minimum, steps for reviewing the system and database user listings to ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked and that privileges associated with each individual are still authorized and necessary. Additionally the procedures should note the parties that should be involved in the review process and supporting documentation that should be maintained as a result of the review.			
TSA 06-15	During our audit, the following [redacted] access control weaknesses were noted: • Password configurations for application and database have not been configured to maintain the password history for each account which is required by the [redacted] Password Policy Standard Operating Procedure (SOP), as well as DHS Information Technology Security Program	• Configure the [redacted] application and database to maintain the password history for each account. • Configure the [redacted] application and database to lock users out of their accounts after three failed login attempts. • Establish detailed procedures for audit trail generation, review and management. The procedures should discuss the conditions under which the audit trails should be	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Publication, 4300A. • Users are not locked out of their [redacted] accounts after three invalid logon attempts. • Policies and procedures for application and database audit log management have not been documented. Additionally, although audit logs are generated that document who is logging in and out of the [redacted] database administrator account, the logs are being generated and reviewed by the database administrators and not by an external party. • [redacted] has not been configured to track and deactivate accounts that have not been used in 90 days.	generated, reviewed, the frequency of the reviews, and the basis for determining when suspicious activity should be investigated. In addition, sufficient resources should be allocated to ensure the proper implementation and monitoring of these procedures. • Configure the system to track and lock the accounts of individuals who have not logged into the system in 90 days.			
TSA 06-16	In FY 2006, we performed access control test work around the Sunflower application and database. During our review, the following Sunflower access control weaknesses were noted: • Password configurations for application and database were configured to permit passwords to be a minimum of six characters in length which is not in compliance with the [redacted] Password Policy Standard Operating Procedure (SOP), or the DHS policy, during the time period of October 2005 through June 2006. After June 2006, the password length was changed to eight characters. • Users are not locked out of their Sunflower	We recommend that TSA ensure and verify that Coast Guard's [redacted] complete the following corrective actions: • Continue with efforts to correct the implementation of the lockout policies and procedures to ensure that users are locked out of their accounts after three invalid attempts. • Establish detailed procedures for audit trail generation, review and management. The procedures should discuss the conditions under which the audit trails should be generated, reviewed, the frequency of the reviews, and the basis for determining when suspicious activity should be investigated. In addition, sufficient	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	application accounts after three invalid logon attempts. • Audit logging has not been enabled with in the Sunflower application or database. Specifically, unusual or sensitive access (database and system administrator activity) is not monitored and suspicious activity is not investigated. Additionally, audit trails of appropriate user actions, including changes to security profiles are not generated and maintained.	resources should be allocated to ensure the proper implementation and monitoring of these procedures.			

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA 06-17	During our audit, the following access control weaknesses were noted: • accounts are not immediately disabled upon an employee's termination. Specifically, one out of the two separated employees who had access to the system was not disabled until six months after separating. Additionally, the employee's TSA LAN account was also active during this time. • No policies and procedures exist for the periodic review of TSA personnel with access to	• Develop and implement access control policies and procedures for the periodic review of the application accounts for TSA users. These procedures should include, at a minimum, steps for reviewing the application user listings to ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked and that privileges associated with each individual are still authorized and necessary. Additionally, the procedures should note the parties that should be involved in the review process (i.e. – supervisors, database administrators and system administrators) • Retain supporting documentation indicating the results of each review. • Notify and coordinate with CG- to implement the corrective actions that must result from the review, such as removing separated users from the system or modifying account privileges.	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA 06-18	During our audit the following [redacted] access control weaknesses were noted: • [redacted] accounts are not immediately disabled upon an employee's termination. Specifically: - Three separated TSA employees had active accounts on [redacted] and the remote connection, [redacted]. These three user accounts for [redacted] were not end dated until October 16, 2006. Additionally, one out of the three have an open TSA Local Access Network (LAN) Account. - As of September 2006, eight separated TSA employee's [redacted] accounts were still active on the application after they had separated from TSA over seven months previously. Additionally, seven of those eight individuals had open [redacted] accounts during that time period as well and at least four individuals had active TSA LAN accounts as well. • No formalized policies and procedures for the periodic reviews for the [redacted] accounts exist. • No access request forms could be obtained for the selection of four TSA users who were granted access to the [redacted] application this fiscal year.	• Immediately disable [redacted] application, [redacted] and LAN access for all separated employee accounts. • Formalize and implement access control policies and procedures for the periodic review of the [redacted] application, [redacted] and LAN accounts for TSA users. These procedures should include, at a minimum, steps for reviewing the application user listings to ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked and that privileges associated with each individual are still authorized and necessary. Additionally, the procedures should note the parties that should be involved in the review process (i.e. – supervisors, database administrators and system administrators) • Retain supporting documentation indicating the results of each review. • Develop and implement formalized access control policies and procedures for granting access to the [redacted] application and database accounts. These procedures should include, at a minimum, steps for granting and approving access. Additionally, the procedures should require the supervisors to document the level of access each new user should be granted within the system and database before the request is submitted to the system administrator and database administrator for implementation. This documentation should be retained for each user.	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA 06-19	In FY 2006, we performed access control test work around the Sunflower application, database and the TSA Local Area Network (LAN). During our review, the following Sunflower access control weaknesses were noted: • Sunflower accounts are not immediately disabled upon an employee's termination. Specifically, six terminated TSA personnel have active accounts on the Sunflower application. Additionally, three of the six individuals still retain active LAN accounts. Furthermore, one Sunflower account, for a separated individual, was active for over six months on the Sunflower system and the TSA LAN before being disabled. • Policies and procedures requiring the periodic reviews of Sunflower accounts have not been documented.	• Develop and implement access control policies and procedures for the periodic review of the Sunflower application accounts and LAN accounts for TSA users. These procedures should include, at a minimum, steps for reviewing the application user listings to ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked and that privileges associated with each individual are still authorized and necessary. Additionally, the procedures should note the parties that should be involved in the review process (i.e. – supervisors, database administrators and system administrators) • Retain supporting documentation indicating the results of each review. • Notify and coordinate with CG- to implement the corrective actions that must result from the Sunflower review, such as removing separated users from the system or modifying account privileges.	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA 06-20	The TSA Form 1402, IT off-boarding form for Non-Screeners and Contractors, is not consistently completed for terminated personnel. Specifically, we noted that the form was unavailable for thirty-eight (38) of sixty (60) terminated employees selected for testing. Additionally, eight (8) out of the twenty-two (22) forms received were incomplete.	• Send out a TSA broadcast message reminding all TSA Non-Screeners and Contractors to completely fill out the TSA Form 1402 as they are initiating their own termination process. • Assess implementing a process whereby the terminated individual's supervisor would initiate the completion of TSA Form 1402, instead of the terminated individuals themselves.	**X**		**Medium**
TSA 06-21	During our audit, the following weaknesses were identified: • Initial and/or annual refresher training for security awareness was not completed for 9,821 out of 52,106, approximately 19% of the TSA personnel and contractors with access to TSA information systems. • Computer Access Agreements were not complete for 9,627 out of 55,335, approximately 17%, of TSA federal employees and contractors, with access to TSA information systems. Additionally, 30,835 out of 55,335 personnel, approximately 56% had agreements on file that were over a year old.	Enforce the completion of security awareness training and the computer access agreement for all TSA employees and contractors each fiscal year.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA 06-22	Although the Interagency agreement between United States Coast Guard (CG-) and TSA states that CG- is responsible for configuration management on both the technical and operational sides of the product suite, TSA however, has not formalized a tracking process of their own for requests that they submit nor do they retain records of the change control process. TSA has no policies and procedures surrounding the change control process for the product suite. Specifically, TSA should be responsible for approving the functional resolution documents provided for their specific changes, retain evidence that testing was done by CG- on their behalf, and approving the final change before it is moved into production. Additionally, TSA has not retained any documentation of initial approvals, testing and final approvals for TSA specific changes made Sunflower in the 2006 FY. Specifically, no documentation for the initial approvals, testing or final approvals could be obtained for a selection 14 changes, 16 Changes and 4 Sunflower changes emergency changes.	• Formally document and better define the different roles and responsibilities that TSA, CG- and GCE have in the change control process for the product suite. • Develop and implement policies and procedures to document TSA's role and responsibilities in the change control process. Be sure to specifically address initial approvals, testing and final approval of all changes to the system. • Develop and implement a formalize process for the retention of documentation throughout the change control process.	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA 06-23	During our audit, the following weaknesses were identified: • [redacted] does not perform background investigations or verify that outside background investigations have been performed for contractors working at [redacted], especially those with sensitive IT positions. Specifically, [redacted] employs 150 contractors; however, we were unable to obtain the status of a background investigation on any of them. • No risk levels for contractor personnel with access to DHS information systems at [redacted] exist. Contracting personnel with IT job functions which require advanced access to the DHS system are not categorized at a higher risk level then an individual who uses the system with basic privileges.	• Implement policies and procedures to ensure compliance with the new DHS policies for the background investigations of contracting personnel. • Develop risk levels for contractor positions with access to DHS information systems in accordance with DHS policy.	**X**		**High**
TSA 06-24	Excessive access has been granted within [redacted]. Specifically, of the 27 individuals that have been granted Authorized Certifying Officer (ACO) privileges to approve invoices of any dollar value, four were not justified in having such privileged access.	• Develop and implement access control procedures for the periodic access review of the [redacted] system. These procedures should include, at a minimum, steps for reviewing the system user listings to ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked and that privileges associated with each individual are still authorized and necessary. The procedures also should note the parties that should be	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		involved in the review process (ie – supervisors, database administrators and system administrators) and supporting documentation that should be maintained as a result of the review. After the results of the review are obtained TSA is responsible for communicating the results to [redacted] for the appropriate actions to be completed. Additionally, TSA should follow-up with [redacted] to ensure that corrective actions are taken if necessary. • Ensure that [redacted] removes the access privileges of the four individuals that do not have appropriate access to the system.			

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

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, 2006

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
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.	**X**	
USCIS	05-03	The C&A package for the Texas Service Center (TSC) GSS-LAN is outdated and has expired.	**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 .		**06-04**
USCIS	05-05	A Novell NetWare server at USCIS' Texas Service Center (TSC) was identified as not having the correct vendor supplied patches installed.	**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.	**X**	
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.	**X**	
CBP	05-01	Numerous user IDs were identified as having segregation of duties issues	**X**	
CBP	05-02	The Top Secret mainframe account administration on the had several weaknesses over unauthorized access to accounts with high-level authority, and inactive accounts.	**X**	
CBP	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.	**X**	
CBP	05-04	The National Benefits Center (NBC) has not defined or documented the appropriate user permissions for the various roles granted to Local Area Network (LAN).		**06-01**
CBP	05-05	CBP management has not developed formal procedures for granting access to sensitive SAP Technical Team member roles.	**X**	
CBP	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 .	**X**	
CBP	05-08	The documentation of completed initial security awareness training is not properly maintained. We selected security awareness training documentation for 45 users. Per inspection of documentation, and noted that 13 of 45 did not have security awareness training certificates documented.		**06-29**
CBP	05-09	Improvements still needed in CBP's technical security controls. Related to issues reported in FY02, FY03 and FY04 findings		**06-17**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		regarding host and network based security system access deficiencies, we noted the following: • CBP has confirmed that they will not be implementing the [redacted] to enforce strong passwords or the Windows NT password protection feature enhancement upgrade referred to as NT LANMAN v2 (LM v2). • CBP has not made the configuration changes to the Windows NT [redacted] Domain Controller that was compromised in our FY03 intrusion tests. • Discovered key systems' domains in targeting for potential unauthorized access attempts where we were able to identify major CBP network domains. • Exploited a system vulnerability that had not been corrected. • We confirmed that the number of Domain Administrators on selected Domains has increased since 2005. • ESM identified weak passwords, expired passwords, misconfigurations, and missing patches. • Identified vulnerabilities on an Oracle database which had critical patches missing, week passwords and auditing is not enabled.		
CBP	05-10	[redacted] security audit log reviews not evidenced for the majority of FY 2005.	**X**	
CBP	05-11	• CBP management has not established ISAs for legacy connections with [redacted]. • Additionally, the majority of financial institutions connecting with [redacted] do not have ISAs.		**06-02**
CBP	05-12	CBP alternate processing site agreement not finalized. Priority of service provision not in place.	**X**	
CBP	05-13	Field offices are not consistently reporting the completion of [redacted] re-certifications at their ports to the OFO headquarters. Email confirmation of completion of [redacted] re-certifications were not available for Boston, Baltimore, New Orleans, Miami, and Calgary (Canada) field offices, and the Los Angeles field office only provided an email stating that re-certification process exists, but did not confirm that [redacted] re-certifications had been completed. The six field offices listed above represent 10 of 44 ports selected for testing.		**06-08**
CBP	05-14	• CBP management has not performed a formal review of individuals with physical access to the data center. • Additionally, CBP management has not established formal procedures for revoking physical access to [redacted] buildings.		**06-05**
CBP	05-15	Eighteen (18) [redacted] developers were found with access to the production environment.	**X**	
CBP	05-16	Improvements are still needed in CBP's Incident Handling and Response Capability which may potentially limit CBP's ability to		**06-10**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		respond to incidents in an appropriate manner. Specifically, we noted the following issues: • [redacted] Health Endpoint will not be installed on all workstations for the majority of the fiscal year. • 3 of 8 selected system flaw notifications did not have an associated Service Center ticket.		
CBP	05-17	CBP has not configured their version of [redacted] to include a company code setting of "productive."	**X**	
CBP	05-18	We could not obtain the requested evidence of [redacted] recertifications from CBP for any of the 44 selected field level ports to determine whether [redacted] accounts with sensitive and high-risk combination of functions are reviewed for appropriateness.		**06-09**
CBP	05-19	Separated employees with active [redacted] accounts.	**X**	
CBP	05-20	CBP does not document changes to the [redacted] system including test plans, test cases, impact analysis, and test results.	**X**	
CBP	05-21	CBP management has not activated logging for critical tables within [redacted]	**X**	
CBP	05-22	CBP management has not performed a formal certification and accreditation on the NDC LAN as a whole. Specifically, a formal security control assessment and a formal risk assessment have not been performed for components of the NDC LAN.		**06-03**
CBP	05-23	CBP has not performed a separate certification and accreditation for the applications remaining in the seven business process areas defined in the Administrative Applications C&A. These seven business process areas include the following: • Disclosure Administrative Support Systems • Financial Administrative Support Systems • Field Operations Support Systems • Investigation Support Systems • OIT Administrative Support Systems • Personnel Administrative Support Systems • Training Support Systems		**06-06**
CBP	05-24	CBP does not maintain a centralized listing of separated contract personnel. The only method CBP employs to track terminated contractors is the use of a report of users that had their mainframe account deleted. We cannot acknowledge this list as representative of all terminated contractors. This is because terminated contract personnel might not have mainframe access or their access was not removed after their termination.		**06-04**
CBP	05-25	[redacted] idle session lock inconsistent with CBP policy.	**X**	

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
CBP	05-26	does not have an automated mechanism to detect and deactivate users that have not logged on for 90 days per DHS policy.		**06-07**
CBP	05-27	We noted that 24 out of 45 selected individuals did not have formally documented VPN access authorization forms. Additionally, CBP has not implemented formal procedures for VPN recertification for the majority of FY 2006.		**06-12**
CBP	05-28	Access to the related dataset and CSD definition file is excessive.	**X**	
CBP	05-29	CBP management did not provide information as to whether vendor and bank tables are appropriately segregated.	**X**	
CBP	05-30	The number of users with access to Audit, Recovery, and Backup datasets is excessive.	**X**	
CBP	05-31	Weaknesses in the C&A process at field sites including several missing site assessments.	**X**	
CG	05-001	The has not completed a Business Recovery Plan (BRP).	**X**	
CG	05-002	has not completed a testing baseline and users were able to change their privileges to gain access to production.	**X**	
CG	05-003	Access authorization requests for ids did not indicate the roles or menus necessary for the user to perform job functions; rather access authorizations identified a current user with similar privileges that could be copied to create the privileges for the new id. Additionally, requests for new accounts are accomplished via email, and the system administrator did not routinely retain these emails prior to January 2006.		**06-009**
CG	05-004	A periodic review of Direct Access access lists was not conducted to ensure that users had the correct access privileges. Additionally, we determined that an applicant could be entered and hired by the same individual. The process of transitioning an applicant to an employee is in an audit trail; however this audit trail is not reviewed on a regular basis.		**06-008**
CG	05-005	A security test and evaluation has not been conducted on the General Support System. In addition, the final Certification and Accreditation package has not been created and an Authorization to Operate has not been requested or approved for the General Support System.		**06-024**
CG	05-006	• Coast Guard has not completed the process of filing the records that were recovered and recreating of the records that were not found during the migration of records from the Department of Transportation to DHS.		**06-028**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		• Civilian background investigations and reinvestigations are not being consistently performed. Specifically, three (3) out of seven (7) newly hired civilian employees at [redacted] did not have any record of a background investigation on file. Additionally, for the re-investigation of [redacted] employees, four (4) out of five (5) GS employees selected did not have a current investigation on file. • Position sensitivity level distinctions for civilian personnel with access to DHS information systems at [redacted] are not accurately depicted. Specifically, of the selection of position descriptions received, nine (9) out of ten (10) had non-critical position sensitivities although their job functions were that of IT personnel with advanced access to the DHS system.		
CG	05-006	• [redacted] does not perform background investigations or verify that background investigations have been performed for contractors working at [redacted], especially those with sensitive IT positions. Specifically, [redacted] employs 150 contractors; however, we were unable to obtain the status of a background investigation on any of them. • No risk levels for contractor personnel with access to DHS information systems at [redacted] exist. Contracting personnel with IT job functions which require advanced access to the DHS system are not categorized at a higher risk level then an individual who uses the system with basic privileges.		**06-034**
CG	05-008	The passwords for [redacted] are not required by the system to be 8 characters in length or contain a combination of alphabetic, numeric and/or special characters. Due to lack of vendor support, there is uncertainty to the feasibility of implementing stronger password controls.		**06-007**
CG	05-009	The [redacted] Business Contingency and Disaster Recovery Plan is still in draft form and has not yet been tested.		**06-001**
CG	05-010	FINCEN Unix change control process supporting [redacted] 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.	X	
CG	05-011	[redacted] does not have documented procedures for controlling the processes associated with the granting, monitoring, and termination of user accounts within [redacted] have not been documented.	**X**	
CG	05-012	• Manager Review of System Administration Monitor Procedures have been developed that guide managers in performing periodic system administration monitoring reviews. However, the		**06-019**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		procedures do not note the periods of review that are being monitored, who is responsible for performing the reviews and evidence that the manager review was performed could only be obtained for March 2006. Additionally, although the manager reviews were implemented in March 2006, for the first half of the fiscal year, October through March, [redacted] system administration monitoring was not performed by a manager or group outside of the three systems administrators during that time period. • The access request form for one out of four individuals granted access to [redacted] since October 1, 2005, did not contain the supervisor's approval. • The account of a contractor that left [redacted] in October 2005 remained active until May 2006.		
CG	05-013	[redacted] 's Certification and Accreditations (C&A) for [redacted], and [redacted] were not complete. Specifically, security testing and evaluations (ST&E) were incomplete and security plans had not been updated.	**X**	
CG	05-014	Results of reviews over [redacted] user access were not available and documentation of periodic reviews was not on file at [redacted].	**X**	
CG	05-015	[redacted] has not implemented formal procedures for the periodic management review and monitoring activities of [redacted] database administrators and system administrators, or the [redacted] accounts.	**X**	
CG	05-016	During technical testing patch management weaknesses were identified on hosts supporting the [redacted] applications. Many of these vulnerabilities could allow a remote attacker to gain full control of the affected host and could lead to the compromise of the availability, confidentiality and integrity of [redacted] data.		**06-026**
CG	05-016	During technical testing configuration management weaknesses were identified on hosts supporting the [redacted] applications. Specifically, servers were identified with excessive access privileges, and password and auditing configuration weaknesses.		**06-027**
CG	05-017	The Enterprise Security Management (ESM) tool identified configuration and account management weaknesses on [redacted].	**X**	
CG	05-018	Internet Security Systems Internet Scanner identified three hosts that were missing patches.	**X**	
CG	05-019	Formal procedures regarding access to the [redacted] data center have not been established and implemented.	**X**	
CG	05-021	System change request to modify transaction code 136-2 to automatically reestablish the funds as obligated was implemented in March 2006 within the [redacted] 3.2 build. Currently, the automated process appeared to be operating effectively. However, from October 2005 through March 2006, no mitigating controls such as procedures for training of staff and/or manual reviews were established to determine whether or not the re-obligation should be established to		**06-41**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		the associated UDO balance. Additionally, [redacted] management indicated that transaction code [redacted] should not be automatically reestablishing the funds in the system. However, as we could not perform a complete analysis of the [redacted] posting logic in FY 2006 as noted in NFR CG IT-06-029, transaction code [redacted], as well as other codes, may still contain errors as of September 30, 2006.		
CG	05-022	• A copy of the [redacted] Disaster Recovery Plan has been completed. However, the plan has not been tested. • The DRP for the [redacted] has been completed. However, testing of the [redacted] DRP has not taken place. The projected completion date is October 2006. • The DRP for the General Support System has been completed. However, testing of the GSS DRP is scheduled to take place by the end of the year. • A copy of the Memorandum of Understanding (MOU) between [redacted] and two other CG components who the OSC must rely on for various reasons at the off-site facility was cited in the Disaster Recovery Plan • A finalized contract with the off-site facility was cited in the Disaster Recovery Plan. However, we were unable to obtain the signature page for it during our audit field work.		**06-30**
CG	05-023	[redacted] has not completed a security plan for CMPlus 5.	**X**	
CG	05-024	During our FY 2006 follow-up testing, we determined that [redacted] had taken corrective action on several of the previously noted vulnerabilities, however several remained. The remaining vulnerabilities are in the following four areas: • Account management - 2 high-risk vulnerabilities and 4 medium-risk vulnerabilities • Configuration management – 2 medium-risk vulnerabilities • Patch management – 3 high-risk vulnerabilities		**06-031**
CG	05-025	During our FY 2006 testing, we determined that none of the [redacted] prior year vulnerabilities were corrected. As a result, the vulnerabilities present in FY 2006 are in the following four areas: • Audit management – 2 medium risk vulnerabilities • Configuration management – 3 high, 6 medium and 11 low risk vulnerabilities		**06-032**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		• Password management – 1 high and 5 medium risk vulnerabilities • Patch management- 11 high, 12 medium and 12 low risk vulnerabilities		
CG	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.	**X**	
CG	05-027	As a result of our audit test work and supported by all the IT NFRs issued during the current year, we determined that Coast Guard is non-compliant with the following laws and regulations: • Federal Information Security Management Act of 2002 (FISMA) • Federal Financial Management Improvement Act (FFMIA) • Office of Management and Budget (OMB) Circular A-130		**06-044**
CON	05-01	Two members of DHS OFM had excessive access within DHS We informed DHS OFM of the excessive access and noted that DHS OFM removed both users with excessive access. We noted that corrective action has been taken and completed in the current fiscal year; however, this issue posed a risk for a majority of the fiscal year and therefore will be reported as a weakness for FY 2006.		**06-01**
CON	05-02	new user access request forms were not consistently completed prior to granting access to Specifically, one (1) out of a sample of eleven (11) did not have a supervisor's approval. Additionally, five (5) out of a sample of eleven (11) did not have security manager review.		**06-02**
CON	05-03	OFM has not developed procedures to periodically review access lists in order to determine whether user access is valid, consistent with job responsibilities and in accordance with the principle of least privilege		**06-03**
CON	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.	**X**	
CON	05-05	• During our audit, the following configuration management weaknesses were noted • Segregation of duties violations exists for twelve (12) out of twenty-five (25) system changes made outside of the scheduled Quarterly Releases. • Segregation of duties violations exists for four (4) out of ten (10) emergency system changes made outside of the scheduled Quarterly Releases.		**06-04**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		• Test documentation is not available for changes implemented outside of the scheduled [redacted] Quarterly Releases.		
CON	05-06	Discrepancies exist between the DHS Performance and Accountability Report (PAR) Guidance and the Analytical Report		**06-15**
CON	05-07	• We determined that normal balance type indicated on the DHS SGL for Account 4132 and Account 7280 differ from the normal balance type indicated on the US SGL. • We determined that 101 DHS SGL accounts were not found in the US SGL and reported a zero balance for period 9. These accounts do not appear to be currently used by DHS and/or do not appear to be related to DHS operations.		**06-16**
CON	05-08	There are no documented procedures in place for DHS components to perform a formal review, by a separate approving individual, to verify the [redacted] financial data to the general ledger before moving the [redacted] file from the Holding Area into the [redacted] Repository.		**06-05**
CON	05-09	DHS is non-compliant with the Federal Information Security Management Act		**06-18**
FEMA	05-01	There are no procedures are in place to periodically review [redacted] user access lists to determine if access is still needed, including the development of a master listing of all employees and contractors developed and maintained by FSB.		**06-03**
FEMA	05-02	• [redacted] users are not locked out of the system after three invalid logon attempts. In addition, we determined that upon locking a user account out of the system after three invalid logon attempts at the domain level, the user account becomes unlocked and active again after fifteen (15) minutes of inactivity. • [redacted] settings on machines running Microsoft Windows 2000 Professional disabled the user's ability to disable the password protected screensaver; however the [redacted] settings did not disable the user's ability to change the inactivity threshold greater than the FEMA standard of fifteen minutes. This weakness impacts [redacted].		**06-09**
FEMA	05-03	The [redacted] production and test servers are located in very close proximity of each other, which is not conducive to effective contingency planning efforts. We note that upon the implementation of the [redacted] Data Center's "real-time" back-up facility, both the [redacted] test and production servers will be redundant, alleviating the current condition. However, the [redacted] back-up facility does not currently have that capability in place.		**06-04**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
FEMA	05-04	Twenty-nine (29) terminated or separated FEMA employees and contractors maintain active [redacted] user accounts. Additionally, we noted that two (2) terminated or separated FEMA employees maintain active [redacted] user accounts. The implementation of FEMA Instruction 1540.3 as a form of access controls review is not sufficient because FEMA is only performing reviews over current year terminations and separations, and has not performed reviews over legacy users to ensure that all users have valid access.		**06-13**
FEMA	05-05	• The [redacted] ST&E did not provide adequate documentation of the results to the accrediting authority. The [redacted] ST&E included thorough testing of managerial, operational and technical controls and identified 88 vulnerabilities; however, the vulnerabilities listed in the ST&E report were only identified as one POA&M weakness in the [redacted] POA&M • Of the 10 systems deemed critical for which the C&A process was completed, we noted that the following four systems did not include any documentation of their ST&E results in the ATO package: [redacted]. • FEMA has completed a majority of the [redacted] migration from Microsoft Windows 2000 Professional to Linux except for a few aspects of the migration dealing with Individual Assistance and various regional sites. We noted that these major changes to the system warrant that the [redacted] C&A process be re-performed.		**06-05**
FEMA	05-06	[redacted] settings on machines running Microsoft Windows 2000 Professional prevented the user's ability to disable the password protected screensaver; however the [redacted] settings did not prevent the user's ability to change the inactivity threshold. The implementation of a password protected screensaver as a mitigating control for lacking a second form of authentication is not sufficient if users have the ability to change the inactivity threshold greater than the FEMA standard of fifteen minutes. This weakness impacts [redacted]		**06-10**
FEMA	05-07	There is not formal, documented procedures are in place to require updates to the [redacted] system documentation as [redacted] functions are added, deleted, or modified.		**06-06**
FEMA	05-08	• FEMA did not adequately document testing of the Contingency Plan for [redacted]. Although a table-top test of the [redacted] Contingency Plan was completed on February 10, 2006, the [redacted] table top test did not adequately test the IT components of the system/processes. • FEMA does not have an accurate Contingency Plan for [redacted]. The most recent version of the [redacted] Contingency Plan is dated July 19, 2004. However, since that time, FEMA has nearly		**06-07**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		completed its migration of [redacted] from Microsoft Windows 2000 Professional to the [redacted] operating system and is adding a Small Business Administration web interface.		
FEMA	05-09	The FEMA COOP has prioritized each of its 12 critical Information Technology (IT) systems according to criticality of the systems; however, the FEMA COOP has not been updated to take into account the new listing of FEMA critical IT systems. We confirmed with the Office of Cyber Security (OCS) and ONSC that the updated listing of FEMA mission critical IT systems should be represented in the FEMA COOP.		**06-08**
FEMA	05-10	During our technical testing, configuration management weaknesses were identified on [redacted], and key support servers. Specifically, servers were identified with password and auditing configuration weaknesses, and version weaknesses.		**06-02**
FEMA	05-11	During our technical testing, configuration management weaknesses were identified on [redacted] and key support servers. Specifically, servers were identified with password and auditing configuration weaknesses, and version weaknesses.		**06-02**
FEMA	05-12	During our technical testing, configuration management weaknesses were identified on [redacted], and key support servers. Specifically, servers were identified with password and auditing configuration weaknesses, and version weaknesses.		**06-02**
FEMA	05-13	During our technical testing, patch management weaknesses were identified on [redacted] servers. Specifically, as a result of missing patches, the [redacted] servers were vulnerable to buffer overflow vulnerabilities.		**06-01**
FEMA	05-14	Twenty-one (21) users in [redacted] and eight (8) users in [redacted] have the ability to gain access to the account mapping functions and make changes to the account tables. Of the 21 users in [redacted], nine (9) users do not have a real business need to have access to this function. The 9 users that appear to have excessive access consist of [redacted] developers or others with system administrative access. Additionally, of the 8 users in [redacted], six (6) users do not have a real business need to have access to this function. Additionally, excessive access is designed to be permitted within [redacted] to make offline changes to the general ledger account tables via the [redacted] Group. Currently, we identified five (5) users in the [redacted] group that have the ability to make offline changes to the general ledger account tables. Of the five users, four (4) users do not have a real business need to have access to this function.		**06-27**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
G&T	05-04	Three users who have been assigned privileges that allow them to enter, modify, and approve journal vouchers. According to their job functions and responsibilities, these users should only have the ability to enter journal vouchers. In addition, two users who have been assigned privileges (e.g.) that allow them to modify vendor tables, and allow them to open and close fiscal years.		**06-12**
G&T	05-06	The following weaknesses were identified as a part of the FY 2006 Department of Justice, Office of Justice Programs (OJP) Financial Statement Audit and impact the reliance G&T has on OJP's IT control environment: Access Controls: • Procedures for Generic User Accounts Not Documented. • Periodic Recertification of OJP Application and System Accounts Not Consistently Performed. • OJP does maintain log of changes to security profiles. Application Change Controls: • Application and System Change Controls Procedures and Processes Need Improvement. Service Continuity: • Tape Backup Polices and Procedures and Documentation Storage Requirements Need Enhancement. System Software: • General Support System Configurations Need Enhancement.		**06-06**
G&T	05-12	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	**X**	
G&T	05-13	1 out of 6 G&T terminated employees access was not removed from the Web 269 application within a timely manner (i.e. two business days).		**06-07**
TSA	05-01	Formal procedures regarding access to the Coast Guard (data center have not been established and implemented.	**X**	
TSA	05-03	change control process supporting 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	**X**	

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		and test results are not documented.		
TSA	05-04	The [redacted] Business Contingency and Disaster Recovery Plan (collectively referred to as the DRBC) is approximately 70% completed, with full completion expected by September 30, 2006. Because the plan is in draft form it has not yet been tested, and a tabletop exercise has been planned upon completion of the DRBC.		**06-01**
TSA	05-05	No documented procedures exist for controlling the processes associated with the granting, monitoring, and termination of user accounts within [redacted] have not been documented.	**X**	
TSA	05-06	• Manager Review of System Administration Monitor Procedures have been developed that guide managers in performing periodic system administration monitoring reviews. However, the procedures do not note the periods of review that are being monitored, who is responsible for performing the reviews and evidence that the manager review was performed could only be obtained for March 2006. Additionally, although the manager reviews were implemented in March 2006, for the first half of the fiscal year, October through March, [redacted] system administration monitoring was not performed by a manager or group outside of the three systems administrators during that time period. • The access request form for one out of four individuals granted access to [redacted] since October 1, 2005, did not contain the supervisor's approval. • The account of a contractor that left [redacted] in October 2005 remained active until May 2006. Once the system administrators were notified of the active account, it was deleted.		**06-13**
TSA	05-07	Certification and Accreditations (C&A) for the [redacted] were not complete. Specifically, security testing and evaluations (ST&Es) were incomplete and security plans had not been updated.	**X**	
TSA	05-08	[redacted] has not implemented formal procedures for the periodic management review and monitoring of activities of [redacted] database administrators and system administrators or the [redacted] accounts.	**X**	
TSA	05-09	The Enterprise Security Management tool identified world writeable directories without a sticky bit set, and account management weaknesses over DART.	**X**	
TSA	05-10	During technical testing patch management weaknesses were identified on hosts supporting the [redacted] applications. Many of these vulnerabilities could allow a remote attacker to gain full control of the affected host and could lead to the compromise of the availability, confidentiality and integrity of [redacted] data. During technical testing configuration management weaknesses were		**06-08 & 06-09**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		identified on hosts supporting the [redacted] applications. Specifically, servers were identified with excessive access privileges, and password and auditing configuration weaknesses.		
TSA	05-11	Internet Security Systems Internet Scanner identified three hosts that were missing patches.	**X**	
TSA	05-12	Inaccuracies exist within TSA personnel records which addresses both separated employee issue and other erroneous personnel records.	**X**	

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

Homeland Security

MAY 31 2007

MEMORANDUM FOR: Richard L. Skinner
Inspector General

VIA: Scott Charbo
Chief Information Officer

David Norquist
Chief Financial Officer

FROM: Robert West
Chief Information Security Officer

SUBJECT: Draft Audit Report - *Information Technology Management Letter for the FY 2006 DHS Financial Statement Audit,* January 31, 2007

The Office of Information Security (OIS) has reviewed the Draft *Information Technology Management Letter for the FY 2006 DHS Financial Statement Audit.*

A remediation summary description is provided in Attachment A. A detailed response to the *IT Management Letter FY 2006 Financial Statement Audit* recommendations is provided in Attachment B.

Attachments:
A. OIS Financial System Security FY06 Remediation Summary
B. OIG-07-XX OIS Response, *Draft IT Management Letter for the FY 2006 DHS Financial Statement Audit*, May 2007. [Sensitive Financial Information (FOUO)]

Letter Distribution Request:
Secretary
Deputy Secretary
General Counsel
Chief of Staff
Deputy Chief of Staff
Executive Secretariat
Under Secretary, Management
DHS Chief Financial Officer
DHS GAO OIG Audit Liaison
CIO Audit Liaison

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

Attachment A. OIS Financial System Security FY06 Remediation Summary

Introduction

OIS will address the FY06 Financial System Security Material Weakness by providing corrective actions in four areas:

1. Policy
2. Procedures
3. Tests of Effectiveness
4. Compliance Tracking & Monitoring

Please refer to Figure 1 for an illustration of the following DHS activities.

1. Policy

DHS has completed an update to DHS 4300A, which added governance to support compliance for IT General Controls based on:

- Federal Financial Management Improvement Act of 1996 (FFMIA), P.L. 104-208
- Federal Managers' Financial Integrity Act of 1982 (FMFIA), P.L. 97-255
- OMB Circular A-123, Management's Responsibility for Internal Control, Revised, 12/21/2004
- OMB Circular A-127, Financial Management Systems, Revised 12/1/2004
- OMB Memorandum 06-03, Audit Requirements for Federal Financial Statements 08/23/2006

Based on these laws and regulations, requirements for "CFO designated Financial Systems" have been identified in DHS 4300A Version 5.1, Section 3.15, which was released in March 2007.

The CISO is also working with the CFO on a Memorandum of Understanding (MOU) to further clarify roles and responsibilities for system security controls. Signatures on the joint MOU are targeted for the end of May 2007. As illustrated in Figure 1, an additional 4300A Appendix to further clarify Financial System Requirements is targeted for release by the end of July 2007.

2. Procedures

The Department implements its entity-wide information security program through procedural IA compliance tools:

- DHS TAF provides enterprise procedures for tracking Component System security performance measures, including FIPS199, Risk Assessments, Security Plans, Test Plans and Results, ATO's and Plans of Action and Milestones (POA&Ms).
- DHS RMS provides the enterprise procedures for Certification and Accreditation (C&A) of IT systems based on DHS policies.
- DHS Security Operations Center (SOC) implements enterprise procedures for incident response, patch management, as well as managed services to support vulnerability assessments, etc.

As illustrated in Figure 1, the procedures identified in these tools will be updated to include changes required to support CFO designated financial systems. Training on new financial system roles and responsibilities as well as the new DHS 4300 procedures will be introduced to Components at the DHS Annual Security Conference in August 2007.

Attachment A. OIS Financial System Security FY06 Remediation Summary

3. Tests of Effectiveness

In each FISCAM control domains, a set of key A-123 control requirements will be identified by DHS and minimum mandatory control testing procedures will be developed for:

- Entity-wide Security Program Planning & Management
- Access Control
- Application Software Development and Change Control
- System Software
- Service Continuity
- Segregation of Duties

Additional test of effectiveness processes for key controls will be mapped into RMS requirements Traceability Matrix (RTM) based on the security controls outlined in NIST SP 800-53 and additional security performance measures will be mapped into TAF procedures by the end of November 2007. If a key control weakness is identified for a CFO designated financial system and is not scheduled for remediation within 12 months, a waiver from the CISO and CFO will be required.

4. Compliance Tracking and Monitoring

OIS will then implement Compliance Tracking and Monitoring of CFO Designated Financial Systems. Initially C&A reviews will be manually tracked, and then financial compliance A-123 scorecards will be developed. Independent compliance monitoring of key controls for financial systems is targeted for support at the Component level.

Attachment A. OIS Financial System Security FY06 Remediation Summary

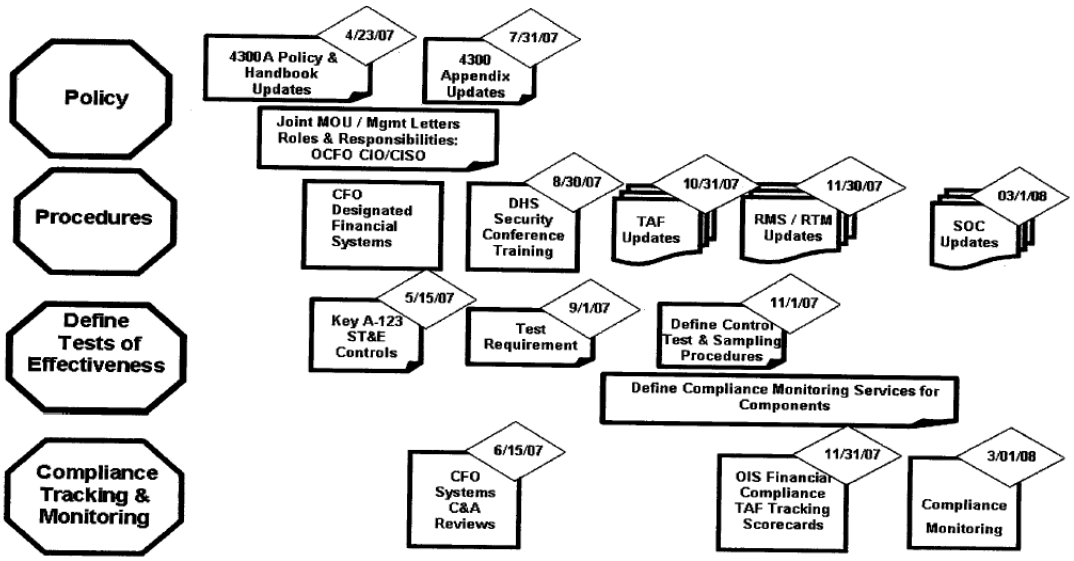

Figure 1. OIS FY06 Remediation Summary

A-3

Department of Homeland Security
Information Technology Management Letter
September 30, 2006

OFFICE OF INFORMATION SECURITY

IT MANAGEMENT LETTER
For the FY2006 DHS Financial Statement Audit, January 31, 2007.

Status
May 2, 2007

This memorandum is covered by Federal Regulations governing Security Sensitive information and may contain confidential and legally privileged information.

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of the Office of Information Security or CISO.

TAF System ID	System Name	Financial Non-Financial System	Number of NFRs	Program Owners
Office of Information Security (OIS) Program	**Department-wide Controls**	**N/A**	**1**	**Robert West, CISO** Don Hagerling, Policy Director Wayne Bavry, Compliance Director Lawrence Henson, Program Director

1

Attachment B. OIG-07-xx OIS Response, *Draft IT Management Letter for FY 2006 DHS Financial Statement Audit*, May 2007.

Risk Rating: HIGH **Finding Title / Auditor Recommendations**	**OIS Remediation Activities**	**Scheduled Completion Dates**
1. For entity-wide security program planning and management:		
No. 1.a: Enforce through the DHS C&A program across all DHS components, a testing process which goes beyond an assessment of in-place policies and procedures, to include tests of password strength, access lists, and software patches, of an application, as an example;	1) The CFO will approve designated FY07 Financial Systems by May 15, 2007. 2) Procedures for testing and sampling key A-123 control effectiveness will be developed and published in RMS / RTM by November 30, 2007. 3) Components will perform monitoring of key controls, including password strength (See *No. 2.a)*, access lists *(No. 2.b)* and software patches *(No. 2.c)*. POA&M Weakness Number: **75**	March 15, 2008
No. 1.b: Enforce the consistent implementation of security programs, policies, and procedures, including incident response capability and IT security awareness and training.	1) DHS 4300 Policies updates will be completed by August 2007. [Appendix] 2) DHS will update general IA Compliance Tool procedures for RMS and TAF by December 2007. 3) OIS has completed a Joint CIO and CFO Management Memo to require explicit SOC incidence reporting (**AC 4.3 Suspicious access activity is investigated and appropriate action taken and SS 2.2 Inappropriate or unusual activity is investigated and appropriate actions taken**) for CFO designated financial systems. SOC procedures will require the Component CFO to be notified of any inappropriate activity. 4) OIS is researching additional methods for IA Awareness Compliance Tracking with Account Management. 5) CFO workshops or meetings with Components will support training on Roles and Responsibilities after the joint CIO/CFO MOU is signed. [4300 Appendix] 6) The DHS Security Conference will include ISSO training on Financial Systems control testing by September 2007. POA&M Weakness Number: 77	December 15, 2007

2

Attachment B. OIG-07-xx OIS Response, *Draft IT Management Letter for FY 2006 DHS Financial Statement Audit*, May 2007.

No. 1.c: Enforce DHS policy to ensure that all contractors go through appropriate background/suitability check.	1) The CFO will be required to identify any requirements above the minimum background/suitability requirements based on DHS 4300A Section 4.1.1.1 Citizenship, Personnel Screening, and Position Categorization, by August 2007. [4300 Appendix] 2) The A-123 Key Control (**SP4.1: Hiring, transfer, termination, and performance policies address security**) test and sampling procedures will be defined and published by November 2007. [RMS / RTM] 3) Systems will require annual testing of SP 4.1 to ensure no IT Accounts are established on CFO Designated Systems without completing the CFO required BI requirements to confirm suitability during the 1st Quarter of the FY. [TAF] 4) Compliance monitoring will be required to be performed by the Component or the SOC during the 3rd quarter of the FY. 5) Key controls will be reviewed by OIS for tracking in a A-123 Compliance Monitoring Scorecards POA&M Weakness Number: **78**	March 15, 2008

2. For access control, ensure that		
No. 2.a: Password controls meet DHS password requirements and are enforced on all systems.	1) The A-123 Key Control (**AC 3.2A: Passwords, Tokens, or other devices are used to identify and authenticate users**) test and sampling procedures will be defined and published by November 2007. [RMS / RTM] 2) Systems will require annual testing of AC 3.2A to ensure compliance with DHS 4300A during the 1st Quarter of the FY. [TAF] 3) Compliance monitoring will be required to be performed by the Component during the 3rd quarter of the FY. 4) Key controls will be reviewed by OIS for tracking in an A-123 Compliance Monitoring Scorecard. POA&M Weakness Number: **55**	March 15, 2008.

Attachment B. OIG-07-xx OIS Response, *Draft IT Management Letter for FY 2006 DHS Financial Statement Audit*, May 2007.

No. 2.b: A password account management process is implemented within the components to ensure the periodic reviews of user accounts.	1) The Password account management process in DHS 4300A will be updated by August 2007. [4300 Appendix] 2) The A-123 Key Control for Account Management (**AC 2.1: Resource owners have identified authorized users and their access is authorized.**) test and sampling procedures will be defined and published by November 2007. [RMS / RTM] 3) Systems will require annual testing of AC 2.1 to ensure compliance with DHS 4300A during the 1st Quarter of the FY. [TAF] 4) Compliance monitoring will be required to be provided by the Component or the SOC during the 3rd quarter of the FY. 5) Key controls will be reviewed by OIS for tracking in an A-123 Compliance Monitoring Scorecard. POA&M Weakness Number: **9**	March 15, 2008
No. 2.c: A DHS-wide patch and security configuration process is implemented and periodically tested by individual DHS components and the DHS-CIO;	1) A DHS-wide patch and security configuration process is defined in SOC CONOPS, Version 1.3. Dated March 2007. 2) DHS security configuration policies for major operating systems are up-to-date and published on DHSOnLine on the CISO web page. 3) The A-123 Key Control (**SS 3.1 System Software changes are authorized, tested and approved before implementation and SS 3.2 Installation of system software is documented and reviewed.**) test and sampling procedures will be defined and published by November 2007. [RMS / RTM] 4) Systems will require annual testing of patch processes (SS 3.1) and security configurations (SS 3.2) to ensure currency during the 1st quarter of the FY. [TAF] 5) Compliance monitoring will be required to be provided by the Component during the 3rd quarter of the FY. 6) Key controls will be reviewed by OIS for tracking in an A-123 Compliance Monitoring Scorecard. POA&M Weakness Number: **64**	March 15, 2008
No. 2.d: Testing of a system's technical security controls take place, including periodic vulnerability assessments, whereby systems are periodically reviewed for access control not in compliance with DHS and Federal guidance.	1) The A-123 Key Control (**AC 3.1: Physical and AC 3.2: Logical**) and test and sampling procedures will be defined and published by November 2007. [RMS / RTM] 2) Systems will be required to complete annual testing of AC 3. 1and AC 3.2 to ensure controls are compliant during the 1st quarter of the FY. [TAF] 3) Compliance monitoring will be required to be provided by the Component during the 3rd quarter of the FY. 4) Key controls will be reviewed by OIS for tracking in an A-123 Compliance Monitoring Scorecard. POA&M Weakness Number: **51**	March 15, 2008

Attachment B. OIG-07-xx OIS Response, *Draft IT Management Letter for FY 2006 DHS Financial Statement Audit*, May 2007.

3. For application software development and change control, ensure that:		
No. 3.a: Policies and procedures regarding configuration management controls are developed and implemented to ensure segregation of duties for change control duties	1) An analysis of the policy and procedures in DHS 4300A compared to OMB A-123 controls will be completed for system segregation of duties objectives. [4300 Appendix] 2) A-123 Key Control (**CC 2.1 Changes are controlled as programs progress through testing to final approval and SD 1.1: Incompatible duties have been identified and policies implemented to segregate these duties**) test and sampling procedures will be defined and published by November 2007. [RMS / RTM] 3) Systems will be required to complete annual testing of CC 2.1 and SD 1.1 to ensure controls are compliant during the 1st quarter of the fiscal year. [TAF] 4) Compliance monitoring will be required to be provided by the Component during the 3rd Quarter of the FY. 5) Key controls will be reviewed by OIS for tracking in an A-123 Compliance Monitoring Scorecard. POA&M Weakness Number: **16**	March 15, 2008
No. 3.b: Changes to the configuration of the system are approved and documented and audit logs are activated and reviewed on a periodic basis.	1) An analysis of the policy and procedures in DHS 4300A compared to OMB A-123 controls will be completed for configuration control and audit logs. ISSO's will be required to review security audit logs at a minimum every month. [4300 Appendix] 2) A-123 Key Controls (**SS 3.1 System Software changes are authorized, tested, and approved before implementation, AC 4.1 Audit Trails are maintained AC4.3 Suspicious access activity is investigated and appropriate actions taken**) test and sampling procedures will be defined and published by November 2007. [RMS / RTM] 3) Systems will be required to complete annual testing of these three key controls to ensure compliance during the 1st quarter of the fiscal year. [TAF] 4) Compliance monitoring will be required to be provided by the Component during the 3rd Quarter of the FY. 5) Key controls will be reviewed by OIS for tracking in an A-123 Compliance Monitoring Scorecard. POA&M Weakness Number: **67**	March 15, 2008

5

Attachment B. OIG-07-xx OIS Response, *Draft IT Management Letter for FY 2006 DHS Financial Statement Audit*, May 2007.

4. For system software, ensure that:		
4. For system software, ensure that Component personnel comply with the established DHS and Federal guidance for monitoring, use and changes related to operating systems and as well as other sensitive utility software and hardware.	1) An analysis of the DHS 4300A compared to OMB A-123 controls will be completed for system software objectives. [4300 Appendix]. 2) A-123 Key Controls (**CC 1.2 OS Patching, SS 1.1 Access authorizations are appropriately limited, SS 3.1 System Software changes are authorized, tested, and approved before implementation, and SS 3.2 Installation of system software is documented and reviewed.**) test and sampling procedures will be defined and published by November 2007. [RMS / RTM] 3) Systems will be required to complete annual testing of key system software controls to ensure compliance during the 1st quarter of the fiscal year. [TAF] 4) Compliance monitoring will be required to be provided by the Component during the 3rd Quarter of the FY. 5) Key controls will be reviewed by OIS for tracking in an A-123 Compliance Monitoring Scorecard. POA&M Weakness Number: **80**	March 15, 2008

5. For Segregation of duties, ensure that:		
No. 5.a: Responsibilities are documented so that incompatible duties are consistently separated. If this is not feasible given the smaller size of certain functions, then sufficient compensating controls, such as periodic peer reviews, should be implemented; and	1) An analysis of the policy and procedures in DHS 4300A compared to OMB A-123 controls will be completed for system segregation of duties objectives. DHS guidance for compensating controls will also be documented. [4300 Appendix] 2) A-123 Key Control (**SD 1.1: Incompatible duties have been identified and policies implemented to segregate these duties.**) test and sampling procedures will be defined and published by November 2007. [RMS / RTM] 3) Systems will be required to complete annual testing of SD 1.1 to ensure compliance during the 1st quarter of the fiscal year. [TAF] 4) Compliance monitoring will be required to be provided by the Component or SOC during the 3rd quarter of the FY. 5) Key controls will be reviewed by OIS for tracking in an A-123 Compliance Monitoring Scorecard. POA&M Weakness Number: **82**	March 15, 2008

Attachment B. OIG-07-xx OIS Response, *Draft IT Management Letter for FY 200o DHS Financial Statement Audit*, May 2007.

No. 5.b: Policies and procedures are developed and documented to assign key security positions and maintain current position descriptions.	1) All CFO Designated Financial Systems will require a dedicated ISSO. Appointment letters, System Security Plans and TAF will be updated to reflect current assignments. [Joint Management Memo][TAF] 2) The ISSO roles and responsibilities for CFO Designated Financial Systems will be clarified [4300 Appendix] and reviewed at the DHS FY07 Security Conference. POA&M Weakness Number: **74**	September 1, 2007

6. For service continuity, ensure that:		
No. 6.a: Components develop and implement complete business continuity plans and system disaster recovery plans; and.	1) An analysis of the policy and procedures in DHS 4300A compared to OMB A-123 controls will be completed for service contingency and disaster recovery plans. [4300 Appendix] 2) An updated CP / DR test plan template for A-123 Key Controls **(SC 3.2 Arrangements have been made for alternate data processing and telecommunication facilities.)** [RMS] 3) Systems will be required to annually update disaster recovery plans SC2.1 during the 1st quarter of the FY. [TAF] 4) Systems will be required to annually test disaster recovery during the 2nd quarter of the FY. . [TAF] 5) Key controls will be reviewed by OIS for tracking in an A-123 Compliance Scorecard. POA&M Weakness Number: **40**	March 15, 2008
No. 6.b: Component-specific and DHS-wide testing of key service continuity capabilities are performed.	1) A-123 Key Control **(SC 4.1: The plan is periodically tested.)** test and sampling procedures will be defined and published by November 2007. [RMS / RTM] 2) Systems will be required to annually update contingency test plans SC 4.1 during the 1st quarter of the FY. [TAF] 3) Systems will be required to annually test contingency during the 2nd quarter of the FY. [TAF] 4) Compliance monitoring will be required to be provided by the Component during the 3rd Quarter of the FY. 5) Key controls will be reviewed by OIS for tracking in an A-123 Compliance Scorecard. POA&M Weakness Number: **68**	March 15, 2008

Report Distribution

Department of Homeland Security

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

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) 254-4199, fax your request to (202) 254-4305, 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 our Hotline at 1-800-323-8603;**
- **Fax the complaint directly to us at (202) 254-4292;**
- **Email us at DHSOIGHOTLINE@dhs.gov; or**
- **Write to us at:**
  DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations - Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.