Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the FY 2010 DHS Financial Statement Audit

(Redacted)

OIG-11-103

August 2011

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 25028

Homeland Security

AUG 18 2011

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 prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report presents the information technology (IT) management letter for the FY 2010 DHS financial statement audit as of September 30, 2010. It contains observations and recommendations related to information technology internal control that were summarized within the *Independent Auditors' Report*, dated November 12, 2010 and represents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit of the DHS' FY 2010 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated April 26, 2011; and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control or conclusion in compliance with laws and regulations.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust 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.

Frank Deffer
Assistant Inspector General
Information Technology Audits

KPMG LLP
2001 M Street, NW
Washington, DC 20036-3389

April 26, 2011

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

We were engaged to audit the balance sheet of the U.S. Department of Homeland Security (DHS or Department) as of September 30, 2010, and the related statement of custodial activity for the year then ended (referred to herein as "financial statements"). We were also engaged to examine the Department's internal control over financial reporting of the balance sheet as of September 30, 2010, and statement of custodial activity for the year then ended. In connection with our audit engagement, we also considered DHS' compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements that could have a direct and material effect on the balance sheet as of September 30, 2010 and the related statement of custodial activity for the year end. We were not engaged to audit the accompanying statements of net cost, changes in net position, and budgetary resources, for the years ended September 30, 2010 (referred to herein as "other fiscal year (FY) 2010 financial statements"), or to examine internal control over financial reporting over the other FY 2010 financial statements. Because of matters discussed in our *Independent Auditors' Report,* dated November 12, 2010, the scope of our work was not sufficient to enable us to express, and we did not express, an opinion on the financial statements.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

During our audit engagement, we noted certain matters in the areas of access controls, configuration management, security management, contingency planning, and segregation of duties with respect to DHS' financial systems Information Technology (IT) general controls which we believe contribute to a DHS-level significant deficiency that is considered a material weakness in IT controls and financial system functionality. We also noted that in some cases, financial system functionality is inhibiting DHS' ability to implement and maintain internal controls, notably IT applications controls supporting financial data processing and reporting. These matters are described in the *IT General Control and Financial System Functionality Findings* section of this letter.

The material weakness described above is presented in our *Independent Auditors' Report*, dated November 12, 2010. This letter represents the separate limited distribution report mentioned in that report.

Although not considered to be a material weakness, we also noted certain other items during our audit engagement which we would like to bring to your attention. These matters are also described in the *IT General Control and Financial System Functionality Findings* section of this letter.

The material weakness and other comments described herein have been discussed with the appropriate members of management, or communicated through a Notice of Finding and Recommendation (NFR), and are intended **For Official Use Only**. We aim to use our knowledge of DHS' organization gained during our audit engagement to make comments and suggestions that we hope will be useful to you. We have not considered internal control since the date of our *Independent Auditors' Report*.

The Table of Contents on the next page identifies each section of the letter. We have provided a description of key DHS financial systems and IT infrastructure within the scope of the FY 2010 DHS financial statement audit engagement in Appendix A; a description of each internal control finding in Appendix B; and the current status of the prior year NFRs in Appendix C. Our comments related to financial management and reporting internal controls have been presented in a separate letter to the Office of Inspector General and the DHS Chief Financial Officer dated February 1, 2011.

DHS's written response to our comments and recommendations has not been subjected to auditing procedures and, accordingly, we express no opinion on it.

This report is intended solely for the information and use of DHS management, DHS Office of Inspector General, U.S. Office of Management and Budget, U.S. Government Accountability Office, and the U.S. Congress, 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

	Page
Objective, Scope and Approach	**1**
Summary of Findings and Recommendations	**2**
IT General Control Findings and Recommendations	**3**
Access Controls	**3**
Configuration Management	**4**
Security Management	**4**
Contingency Planning	**5**
Segregation of Duties	**5**
Financial System Functionality	**5**
Management Comments and OIG Response	**6**

APPENDICES

Appendix	Subject	Page
A	Description of Key DHS Financial Systems and IT Infrastructure within the Scope of the FY 2010 DHS Financial Statement Audit	**7**
B	FY 2010 Notices of IT Findings and Recommendations at DHS	**19**
	• Notice of Findings and Recommendations (NFR)– Definition of Severity Ratings	**20**
C	Status of Prior Year Notices of Findings and Recommendations and Comparison to Current Year Notices of Findings and Recommendations at DHS	**147**
D	Management Comments	**153**
E	Report Distribution	**155**

Department of Homeland Security
Information Technology Management Letter
September 30, 2010

OBJECTIVE, SCOPE AND APPROACH

During our engagement to perform an integrated audit of Department of Homeland Security (DHS), we evaluated 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 (GAO), formed the basis of our audit as it relates to IT general controls assessments at DHS. The scope of the DHS IT general controls assessment is 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 five control functions to be essential to the effective operation of the general IT controls environment.

- *Security Management (SM)* – 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 or detect access to computer resources (data, programs, equipment, and facilities) and protect against unauthorized modification, loss, and disclosure.
- *Configuration Management (CM)* – Controls that help to prevent unauthorized changes to information system resources (software programs and hardware configurations) and provides reasonable assurance that systems are configured and operating securely and as intended.
- *Segregation of duties (SD)* – Controls that constitute policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations.
- *Contingency Planning (CP)* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

To complement our general IT controls audit procedures, we also performed technical security testing for key network and system devices, as well as testing over key financial application controls in the DHS environment. 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 key general support systems.

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 input, processing, and output of financial data and transactions that support the financial systems' internal controls. Application controls are the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, or payroll.

During FY 2010, we also considered the effects of financial system functionality while testing IT general and application controls and other internal controls over financial reporting. Many of the financial systems in use at DHS components were inherited from the legacy agencies and have not been substantially updated since the department's inception. As a result, financial system functionality may be inhibiting DHS' ability to implement and maintain internal controls, notably IT applications controls supporting financial data processing and reporting at some components.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During our FY 2010 assessment of IT general and application controls and financial system functionality, we noted that the DHS made some progress in remediation of IT findings we reported in FY 2009. We have closed approximately 30 percent of our prior year IT findings. In FY 2010 we identified approximately 161 findings, of which approximately 65 percent are repeated from last year. Nearly one-third of our repeat findings were for IT deficiencies that management represented were corrected during FY 2010. Disagreements with management's self assessment occurred almost entirely at the Federal Emergency Management Agency (FEMA).

The most significant weaknesses from a financial statement audit perspective include: 1) excessive unauthorized access to key DHS financial applications; 2) configuration management controls that are not fully defined, followed, or effective; 3) security management deficiencies in the area of the certification and accreditation process and the lack of adhering to or developing policies and procedures , 4) contingency planning that lacked current, tested, contingency plans developed to protect DHS resources and financial applications, and 5) lack of proper segregation of duties for roles and responsibilities within financial systems.

Collectively, the IT control deficiencies limited DHS' ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these deficiencies negatively impacted the internal controls over DHS' financial reporting and its operation and we consider them to collectively represent a material weakness for DHS under standards established by the American Institute of Certified Public Accountants (AICPA) and GAO. The IT findings were combined into one material weakness regarding IT Controls and Financial Systems Functionality for the FY 2010 audit of the DHS consolidated financial statements. As reported last year, both FEMA and Immigration and Customs Enforcement's (ICE) control deficiencies were found to have a more significant impact on the Department. FEMA continues to have a high number of significant IT general controls findings that repeat each fiscal year. These weaknesses affect our ability to fully audit its financial application controls. In addition, ICE has significant weaknesses in its key financial system which has resulted in duplicate payments, and poor configuration and patch management.

IT GENERAL CONTROL FINDINGS AND RECOMMENDATIONS

Conditions: In FY 2010, a number of IT and financial system functionality deficiencies were identified at DHS. Approximately 162 findings were identified of which approximately 65 percent are repeated from last year. The findings identified below are a cross-representation of the nature of IT general control deficiencies identified throughout the department's components which contribute to a material weakness for financial system security as part of the FY 2010 DHS financial statement audit.

Related to IT controls:

1. *Access Controls* - At the following DHS components: United States Coast Guard (USCG), Customs and Border Protection (CBP), Federal Law Enforcement Training Center (FLETC), FEMA, ICE, DHS Headquarters, Transportation Security Administration (TSA), and United States Citizenship and Immigration Services (USCIS) we noted:

   - Deficiencies in management of application and/or database accounts, network, and remote user accounts:
     - System administrator root access to financial applications was not properly restricted, logged, and monitored;
     - Strong password requirements were not enforced;
     - User account lists were not periodically reviewed for appropriateness, inappropriate authorizations and excessive user access privileges were allowed at some DHS components, and users were not disabled or removed promptly upon personnel termination;
     - Emergency and temporary access was not properly authorized, and contractor development personnel were granted conflicting access to implement database changes;
     - Initial and modified access granted to application and/or database, network, and remote users was not properly documented and authorized; and
     - The process for authorizing and managing remote virtual private network (VPN) access to external state emergency management agencies, and component contractors, did not comply with DHS and component requirements.
   - Ineffective safeguards over logical and physical access to sensitive facilities and resources:
     - While performing after-hours physical access testing, we identified the following unsecured items: Government credit cards; financial system user IDs and passwords; computer laptops; and server names and IP addresses; and
     - While performing social engineering testing, we identified instances where DHS employees provided their system user names and passwords to an auditor posing as a help desk employee.
   - Ineffective or insufficient use of available audit logs:
     - Logs of auditable events are not being reviewed to identify potential incidents, or were reviewed by those with conflicting roles;

- Logging of application and/or database events required to be recorded was not enabled;
- Documented procedures for audit log follow-up do not meet DHS requirements; and
- Evidence of audit log reviews was not retained.

2. *Configuration Management:* At the following DHS components: USCG, CBP, FLETC, FEMA, ICE, USCIS, and TSA we noted:
   - Lack of documented policies and procedures:
     - To prevent users from having concurrent access to the development, test, and production environments of the system at four DHS components; and
     - Configuration, vulnerability, and patch management plans have not been established and implemented, or did not comply with DHS policy;
   - Vulnerabilities were identified during periodic internal scans and related corrective actions were not reported and tracked in accordance with DHS policy; and
   - Security patch management and configuration deficiencies were identified during the vulnerability assessment on hosts supporting the key financial applications and general support systems.
3. *Security Management* - At the following DHS components: USCG, CBP, DHS Headquarters, TSA, FLETC, FEMA, USCIS, and ICE we noted:
   - Systems certification and accreditation:
     - Several component financial and associated feeder systems as well as general support systems, were not properly certified and accredited, in compliance with DHS policy;
     - Compliance with the Federal Desktop Core Configuration (FDCC) security configurations is in progress, but has not been completed; and
     - An instance where Interconnection Security agreements were not documented.
   - Roles and responsibilities have not been clearly defined:
     - Instances of security roles and responsibilities are not adequately defined for financial applications and general support systems; and
     - System boundaries have not been adequately and completely defined within the System Security Plan.
   - Lack of policies and procedures:
     - One instance of incomplete or inadequate policies and procedures associated with computer incident response capabilities;
     - Procedures for exit processing of transferred/terminated personnel, including contractors, had not been established; and
     - Lack of component policies and procedures for IT-based specialized security training.
   - Lack of compliance with existing policies:

- Several instances where background investigations of federal employees and contractors employed to operate, manage and provide security over IT systems were not being properly conducted;
- Lack of compliance with DHS computer security awareness training requirements;
- Non-disclosure agreements were not completed at one DHS component; and
- A complete and accurate listing of workstations could not be provided at one DHS component and as a result anti-virus protection is not installed on all workstations.

4. *Contingency Planning* - At the following DHS components: CBP and FEMA, we noted:
   - Instances where incomplete or outdated business continuity plans and systems with incomplete or outdated disaster recovery plans. Some plans did not contain current system information, emergency processing priorities, procedures for backup and storage, or other critical information;
   - Service continuity plans were not consistently and/or adequately tested, and individuals did not receive training on how to respond to emergency situations;
   - An alternate processing site has not been established for high risk systems; and
   - Appropriate authorization to access backup media was not made available.
5. *Segregation of Duties:* At the following DHS components: USCG, CBP, FEMA, ICE, and USCIS we noted:
   - Financial system users had conflicting access rights as the Originator, Funds Certification Official, and the Approving Official;
   - Lack of evidence to show that least privilege and segregation of duties controls exist; and
   - Policy and procedures to define and implement segregation of duties were not properly developed and/or implemented.

These control findings, including other significant deficiencies are described in greater detail in a separate *Limited Official Use* component-specific Information Technology Management letter provided to DHS component management.

FINANCIAL SYSTEM FUNCTIONALITY

We noted that in some cases, financial system functionality is inhibiting DHS' ability to implement and maintain internal controls, notably IT applications controls supporting financial data processing and reporting. Financial system functionality limitations also contributes to other control deficiencies reported in our report dated November 12, 2010, and can make compliance with the Federal Financial Management Improvement Act (FFMIA) and the Office of Management and Budget (OMB) Circular A-127 more difficult. At the following DHS components: USCG, CBP, FLETC, ICE, USCIS, and TSA we noted financial system functionality conditions to include:

- Inability to modify IT system core software, and install controls to prevent duplicate payments. One component identified two instances where duplicate payments were made in FY 2009 and FY 2010, and the funds needed to be recovered;
- System limitations lead to extensive manual and redundant procedures to process transactions, to verify the accuracy of data, and to prepare financial statements;

- The financial systems in one component cannot be configured to:
  - Prevent, detect, and correct excessive refunds;
  - Provide summary information of the total unpaid assessments for duties, taxes, and fees by individual importer; and
  - Report information on outstanding receivables, the age of receivables, or other data necessary for management to fully monitor collection actions; and
- Two inventory tracking systems are not fully integrated with the financial system of record; and
- Several financial systems do not have the necessary functionality to enforce DHS-required system security requirements. For example, one system does not have the functionality to enforce policy requirements related to password complexity, account lockout, and profile changes. In addition, a system does not have the functionality to track new users or user profile changes.

Recommendations: We recommend that the DHS Office of Chief Information Officer (OCIO), in coordination with the Office of Chief Financial Officer (OCFO), the DHS component OCIOs, OCFOs, and other appropriate component management review each individual IT NFR appropriately to ensure that the DHS components enter the recommendations as Plan of Action and Milestones in Trusted Agent FISMA, and work with the respective components to develop corrective action plans to address the root cause and condition of each NFR.

Financial System Functionality Recommendation: We recommend that the DHS OCIO, in coordination with the OCFO, the DHS component OCIOs, OCFOs, and other appropriate component management address the IT system aspects associated with the financial system functionality issues listed above, or develop compensating/mitigating controls in order to eliminate or reduce the associated risk.

MANAGEMENT COMMENTS AND OIG RESPONSE

The OIG obtained written comments on a draft of this report from the DHS CIO, DHS Acting CFO, and DHS CISO. Generally, DHS management agreed with all of our findings and recommendations. DHS management has developed a remediation plan to address these findings and recommendations. A copy of the comments is included in Appendix D.

OIG Response

We agree with the steps that DHS management is taking to satisfy these recommendations.

Department of Homeland Security
Information Technology Management Letter
September 30, 2010

Appendix A

Description of Key DHS Financial Systems and IT Infrastructure within the Scope of the FY 2010 DHS Financial Statement Audit

Below is a description of significant financial management systems and supporting IT infrastructure included in the scope of the engagement to perform the financial statement audit.

United States Coast Guard (USCG)

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 Finance Center (FINCEN), in Chesapeake, Virginia (VA). The FINCEN is the Coast Guard's primary data center. CAS interfaces with two other systems located at the FINCEN, the Workflow Imaging Network System (WINS) and the Financial and Procurement Desktop (FPD).

- CAS Version 4.1
- CAS Oracle Database 9.2.0.8.0 – 47 GB 16x750mhz RISC Processor; cgofprod.world
- CAS Operating System – HP Unix 11.11; ARGUS Server

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 purchase requests, issue procurement documents, perform system administration responsibilities, and reconcile weekly program element status reports. FPD is interconnected with the CAS system and is located at the FINCEN in Chesapeake, VA.

- FPD Oracle 9.2.0.8.0 Database – 28 GB 12x750mhz RISC Processor; LUFS.world
- FPD Operating System – HP UNIX 11.11; Dart Server

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. WINS is interconnected with the CAS and FPD systems and is located at the FINCEN in Chesapeake, VA.

- WINS Oracle 10.2.0.3 Database - 48 GB 12x750mhz RISC Processor; PROD1.world
- WINS Operating System – HP Unix 11.11; Vigilant Server

Joint Uniform Military Pay System (JUMPS)

JUMPS is a mainframe application used for paying USCG active and reserve payroll. JUMPS is located at the Pay and Personnel Center (PPC) in Topeka, Kansas.

- IBM Mainframe - z890
- JUMPS Operating System z/OS 1.8 Base

Direct Access

Direct Access is the system of record and all functionality, data entry, and processing of payroll events is conducted exclusively in Direct Access. Direct Access is maintained by IBM Application On Demand (IBM AOD) in the iStructure data center facility at Tempe, AZ with a hotsite located in a Qwest data center in Sterling, VA.

- Hardware - 1 Sunfire 4800, 2 Sunfire 880, 1 Sunfire 4500, 1 Sunfire v240, 2 Sunfire V440, 2 F5Big-IP, 1IBM 3650
- Software – PeopleTools v8.4, PeopleSoft HCM v8.0, WebLogic v8, Tuxedo v8, MicroFocus Cobol v4, Oracle DB v9, ImageNow v5.4.1, WebNow v3.4.1

Global Pay (Direct Access II)

Global Pay provides retiree and annuitant support services. Global Pay is maintained by IBM AOD in the iStructure data center facility at Tempe, AZ with a hotsite located in a Qwest data center in Sterling, VA.

- Hardware – 2 Database Servers IBM P550, 1 Web/App Server IBM P520, 1 Web/App Server IBM P550, 1 W2K Server IBM x Series 336, 2 F5 BIGIP Load Balancer, 1 Database/App Server IBM P550, 2 Web Server IBM P520, 1 App Server IBM P550, 1 Proxy Server SunFire v240
- Software – 2 PeopleSoft HRMS v 9.0, 2 PeopleTools v 8.46.05, PeopleSoft Enterprise Portal v 8.0, 2 WebLogic v 8.1 sp3, 2 Tuxedo v 8.1 r3, 2 Oracle RDMS v 10.x, 1McAfee Entercept v 5.1 – IDS, 1 Checkpoint NG with Application Intelligence (R55) 105 – Firewall, 1 Legato v 7.x

Shore Asset Management (SAM)

SAM is hosted at the Coast Guard's Operation System Center (OSC), in Martinsburg, WV. SAM provides core information about the USCG shore facility assets and facility engineering. The application tracks activities and assist in the management of the Civil Engineering (CE) Program and the Facility Engineering (FE) Program. SAM data contributes to the shore facility assets full life cycle Program management, facility engineering full life cycle Program management and rationale to adjust the USCG mission needs through planning, budgeting, and project funding. SAM also provides real property inventory and management of all shore facilities, in addition to the ability to manage and track the facilities engineering equipment and maintenance of that equipment.

- Hardware platform:-Intel MP BladeServer SBXD132, 2x Xeon Dual Core 2.66Ghz, EMT64, 4GB Ram (8GB DB Servers), Mirrored 72GB SAS, 2x 1GB Network Interface
- Operating - Software: Windows 2003 Server Standard 5.2.3790 Service Pack 2 build 3790
- Security Software - McAfee Virus Scan Enterprise 8.0.0
- Database - Oracle 9i, 32 bit

Naval and Electronics Supply Support System (NESSS)

NESSS is one of four automated information systems that comprise the family of Coast Guard logistics systems. NESSS is a fully integrated system linking the functions of provisioning and cataloging, unit configuration, supply and inventory control, procurement, depot-level maintenance and property accountability, and a full financial ledger.

- Hardware platform:-1 HP A7137A, 1 Dell PowerEdge 6450, 2 Dell Power Edge 6650, 2 HP A3639A
- Software - Software: Oracle Application Server Forms and Report Services 10.1.2.02, Xventory Baseline, File Replication Pro, Windows 2003 Server Enterprise Edition, PDF Pagemaster

Aviation Logistics Management Information System (ALMIS)

ALMIS provides Coast Guard Aviation logistics management support in the areas of operations, configuration management, maintenance, supply, procurement, financial, and business intelligence. Additionally, ALMIS covers the following types of information: Financial, Budget, Planning, Aircraft & Crew Status, Training & Readiness, and Logistics & Supply. The Aviation Maintenance Management Information System (AMMIS), a subcomponent of ALMIS, functions as the inventory management/fiscal accounting component of the ALMIS application. The Aircraft Repair & Supply Center (ARSC) Information Systems Division (ISD) in Elizabeth City, North Carolina hosts the ALMIS application.

- Linux AS 4.0 (OS for Oracle Databases)
- HPUX 11i (OS for Ingres Databases)
- Oracle 10g (Database Services)
- Ingress 2.6 (Database Services)
- Windows 2000 Advanced Server (Web Server)

CG Treasury Information Executive Repository (CG Tier)

CG TIER is a financial data warehouse containing summarized and consolidated financial data relating USCG operations. It is one of several supporting applications within CAS Suite designed to support the core financial services provided by FINCEN. CG TIER provides monthly submissions to DHS Consolidated TIER.

- Database- Oracle v 8.1.7.4 (Tiers)
- Operating System- HP-UNIX; v 11.11

Customs and Border Protection (CBP)

SAP Enterprise Central Component (SAP ECC 6.0)

SAP is a client/server-based financial management system and includes the Funds Management, Budget Control System, General Ledger, Real Estate, Property, Internal Orders, Sales and Distribution, Special Purpose Ledger, and Accounts Payable modules. These modules are used by CBP to manage assets (e.g., budget, logistics, procurement, and related policy), revenue (e.g., accounting and commercial operations: trade, tariff, and law enforcement), and to provide information for strategic decision making. The SAP ECC 6.0 financial management system is included in full scope in the FY 2010 financial statement audit. The SAP ECC 6.0 system is located in Newington, VA.

Automated Commercial System (ACS)

ACS is a collection of mainframe-based business process systems used to track, control, and process commercial goods and conveyances entering the United States territory, for the purpose of collecting import duties, fees, and taxes owed the Federal government. ACS collects duties at ports, collaborates with financial institutions to process duty and tax payments, provides automated duty filing for trade clients, and shares information with the Federal Trade Commission on trade violations and illegal imports. The ACS system is included in full scope in the FY 2010 financial statement audit. The ACS system is located in Newington, VA.

Automated Commercial Environment (ACE)

ACE is the commercial trade processing system being developed by CBP to facilitate trade while strengthening border security. It is CBP's plan that the ACE replaced ACS when ACE is fully

implemented. The mission of ACE is to implement a secure, integrated, government-wide system for the electronic collection, use, and dissemination of international trade and transportation data essential to federal agencies. ACE is being deployed in phases, with no set final full deployment date due to funding setbacks. As ACE is partially implemented now and processes a significant amount of revenue for CBP, ACE was included in full scope in the FY 2010 financial statement audit. The ACE system is located in Newington, VA.

Federal Law Enforcement and Training Center (FLETC)

Financial Accounting and Budgeting System (FABS)

Processing Location*:* FLETC Headquarters in Glynco, GA

The FLETC FABS application is an all-in-one financial processing system. It functions as the computerized accounting and budgeting system for FLETC. The FABS system exists to provide all of the financial and budgeting transactions in which FLETC is involved. The FABS environment primarily consists of the latest version of the Momentum version 6.1 COTS software, an Oracle 10g database and its companion Oracle 10.2 Database Management System (DBMS). An application called "Tuxedo," also resides on a separate server. The Tuxedo middleware holds 67 executable files. These files are scripts that process daily information and are not directly accessible by users. The FABS application and servers reside on the FLETC LAN in a Hybrid physical network topology and are accessible from four sites: Glynco, GA, Washington D.C., Artesia, New Mexico, and Cheltenham, MD.

- Hardware: Hewlett Packard ProLiant BL465c Blade Servers (web and application) and Hewlett Packard ProLiant BL685c Blade Servers (database)
- Operating System: Microsoft Windows 2003 Server running on virtual machines on top of VMware Infrastructure 3.5 Enterprise hypervisor on the web and application servers
- Database: Red Hat Enterprise Linux
- Security Software: FABS system does not currently have a firewall scheme and resides on FLETC LAN that has a firewall in place

Interfaces:

- National Finance Center (NFC) Payroll System
- Student Information System (SIS)
- TIER
- US Coast Guard Interface
- Kansas City Financial Center (KFC)

Glynco Administrative Network

Processing Location*:* FLETC Headquarters in Glynco, GA

The purpose of the Glynco Administrative Network (GLYADLAN) is to provide access to IT network applications and services to include voice to authorized FLETC personnel, contractors and partner organizations located at the Glynco, Georgia facility. It provides authorized users access to email, internet services, required applications such as Financial Management Systems (FMS), Procurement systems, Property management systems, Video conference, and other network services and shared resources.

- Hardware: Cisco ACS TACAS Server, Avaya 8700 Media Servers, Dell Poweredge servers 1750, 1850, 1950, 2650, 2850, 2950, and 6650.
- Operating System: Windows XP SP2 (Desktop)
- Database: Redhat Linux 4 Enterprise edition
- Security Software: ASA 5500 series firewall and static IP addresses

Interfaces:

- FMS
- DHS HQ

Federal Emergency Management Agency (FEMA)

Core Integrated Financial Management Information System (IFMIS) (Operational through February 22, 2010

Processing Location*:* Mount Weather Emergency Operations Center in Bluemont, VA

Core IFMIS was the key financial reporting system, and had several feeder subsystems (budget, procurement, accounting, and other administrative processes and reporting). The application was a Commercial Off-The Shelf (COTS) software package developed and maintained by Digital Systems Group (DSG) Incorporated.

- Hardware: Two (2) HP 9000 servers (operational and standby)
- Operating System: HP-UX (Unix) version 11.11
- Database: Oracle 9i Enterprise Edition
    - Security Software: Servers are protected by a CISCO PIX Firewall

Interfaces:

- NEMIS
- Credit Card Transaction Management System (CCTMS)
- Fire Grants
- Mitigation Grants
- eGrants
- ProTrac
- Payroll
- Department of Treasury
- Smartlink
- TIER

Grants and Training (G&T) IFMIS (Operational through February 22, 2010)

Processing Location*:* Mount Weather Emergency Operations Center in Bluemont, VA

In April 2007, the Office of Grants and Training (G&T) that was previously under the Department of Justice was transferred over to FEMA. Due to the short amount of time given to FEMA to take over the financial management role for G&T in FY 2007, a separate instance of IFMIS was inherited from the Department of Justice, resulting in two separate IFMIS instances at FEMA. G&T IFMIS, held all former G&T financial information. The application is a COTS software package developed and maintained by DSG Incorporated.

- Hardware: HP 9000 server

- Operating System: HP-UX (Unix) version 11.11
- Database: Oracle 9i Enterprise Edition
- Security Software: Servers are protected by a CISCO PIX Firewall

Interfaces:

- PARS

IFMIS-Merger (Operational as of February 23, 2010)

Processing Location*:* Mount Weather Emergency Operations Center in Bluemont, VA

IFMIS-Merger is the official accounting system of FEMA and maintains all financial data for internal and external reporting. IFMIS-Merger is comprised of five subsystems: Funding, Cost Posting, Disbursements, Accounts Receivable, and General Ledger. The application is a COTS software package developed and maintained by DSG Incorporated.

- Hardware: Two (2) HP 9000 servers
- Operating System: HP-UX (Unix) version 11.11
- Database: Oracle 9i Enterprise Edition
- Security Software: Servers are protected by a CISCO PIX Firewall

Interfaces:

- Payment and Reporting System (PARS)
- ProTrac
- Smartlink (Department of Health and Human Services)
- TIER (Department of Treasury)
- Secure Payment System (SPS) (Department of Treasury)
- Grants Management System (Department of Justice)
- National Emergency Management Information System (NEMIS)
- US Coast Guard Credit Card System
- CCTMS
- Fire Grants
- eGrants
- Enterprise Data Warehouse (EDW)
- Payroll (National Finance Center)

Payment and Reporting System (PARS)

Processing Location*:* Mount Weather Emergency Operations Center in Bluemont, VA

PARS is a standalone web-based application. The PARS database resides on the IFMIS-Merger UNIX server. Prior to the merger of Core IFMIS and G&T IFMIS, PARS resided on the core IFMIS server. Through its web interface, PARS collects Standard Form 269 information from grantees and stores the information in its Oracle 9i database. Automated chron jobs are run daily to update and interface grant and obligation information between PARS and IFMIS-Merger. All payments to grantees are made through IFMIS-Merger. Prior to the IFMIS-Merger instance in February 2010, the PARS application interfaced with G&T IFMIS.

- Hardware: HP 9000 server
- Operating System: HP-UX (Unix) version 11.11

- Database: Oracle 9i Enterprise Edition
- Security Software: Servers are protected by a CISCO PIX Firewall

Interfaces:

- G&T IFMIS (prior to February 23, 2010)
- IFMIS-Merger (as of February 23, 2010)

National Emergency Management Information System (NEMIS)

Processing Location*:* Mount Weather Emergency Operations Center in Bluemont, VA

NEMIS is a FEMA-wide system of hardware, software, telecommunications, services, and applications. NEMIS consists of many integrated subsystems distributed over hundreds of separate servers accessed by thousands of client workstations.

NEMIS is an integrated system to provide FEMA, the states, and 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.

- Hardware: Numerous HP ProLiant DL series servers
- Operating System: Linux, Microsoft NT and Microsoft 2000
- Database: Replicated Oracle 10g, 9i, and 8i databases
- Security Software: Servers are protected by a PIX Firewall Symantec Anti-Virus corporate edition version 10.1.4.4000

Interfaces:

- IFMIS
- US Coast Guard Credit Card System
- Small Business Administration

Traverse

Processing Location*:* Lanham, MD (until July 31, 2010), Landover, MD (after August 1, 2010).

Traverse is the general ledger application currently used by the Nation Flood Insurance Program (NFIP) Bureau and Statistical Agent to generate the NFIP financial statements. Traverse is a client-server application that runs on the NFIP Local Area Network (LAN) Windows server environment in Landover, MD. The Traverse client is installed on the desktop computers of the NFIP Bureau of Financial Statistical Control group members.

- Hardware: Hewlett Packard ML530, Dual Xeon 2.8 Processors, 2 GB RAM, Redundant Array of Independent Disks (RAID) Storage
- Operating System: Microsoft Windows Server 2003
- Database: Microsoft Structured Query Language (SQL)
- Security Software: CheckPoint firewall

Interfaces:

No known system interfaces

Transaction Recording and Reporting Processing (TRRP)

Processing Location*:* Norwich, CT

The TRRP application acts as a central repository of all data submitted by the Write Your Own (WYO) companies for the NFIP. 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 NFIP mainframe logical partition in Norwich, CT.

- Hardware: IBM 2086-220 Mainframe with two central processing units
- Operating System: IBM z/OS 1.9
- Database: WebFocus

Interfaces:

No known system interfaces

Immigration and Customs Enforcement (ICE)

Federal Financial Management System (FFMS)

The FFMS is a CFO designated financial system and certified software application that conforms to OMB Circular A-127 and implements the use of a Standard General Ledger for the accounting of agency financial transactions. It is used to create and maintain a record of each allocation, commitment, obligation, travel advance and accounts receivable issued. It is the system of record for the agency and supports all internal and external reporting requirements. FFMS is a commercial off-the-shelf financial reporting system and is built on Oracle 9i Relational Database Management System running off an IBM 9672 Mainframe with ZOS 1.4 platform. The FFMS operating system operates off an IBM ZOS, Version 1.4 Mainframe Server and Microsoft Windows 2000 report servers protected by firewalls. It includes the core system used by accountants, FFMS Desktop that is used by average users, and an NFC payroll interface. As of July 2010, the FFMS mainframe component and two network servers are hosted at the DHS DC2 facility located in Clarksville, Virginia. Prior to July, the system was housed at the Department of Commerce in Springfield, VA. FFMS currently interfaces with the following systems:

- Direct Connect for transmission of DHS payments to Treasury
- Fed Travel
- The Biweekly Examination Analysis Reporting (BEAR) and Controlling Accounting Data Inquiry (CADI), for the purpose of processing NFC user account and payroll information.
- The Debt Collection System (DCOS)
- Bond Management Information System (BMIS) Web

ICE Network

The ICE Network, also known as the Active Directory/Exchange (ADEX) E-mail System, is a major application for ICE and other DHS components, such as the USCIS. The ADEX servers and infrastructure for the headquarters and National Capital Area are located on the third floor of the Potomac Center North Tower in Washington, DC. The ICE Network utilizes a hybrid mesh/hub and mesh network design to maximize redundancy throughout the network. ICE operates off of Dell PowerEdge 2950, HP ProLiant DL 385 Server, HP ProLiant BL45p Server Blade, HP BL 25P Blade Server, and EMC Symmetrix DM. ADEX has implemented Microsoft Windows 2003 Enterprise Server operating system to provide directory, domain control, and network services to clients. For security purposes, ADEX has implemented firewalls and a logical Layer-3 encrypted overlay network through the use of Generic Routing Encapsulation (GRE) and IPSec tunneling. ADEX currently interfaces with the following systems:

- Diplomatic Telecommunications Service Program Office (DTSPO) ICENet Infrastructure

Office of Financial Management (OFM)/Consolidated Component

DHS Treasury Information Executive Repository (DHSTIER)

DHSTIER is the system of record for the DHS consolidated financial statements and is used to track, process, and perform validation and edit checks against monthly financial data uploaded from each of the DHS bureaus' core financial management systems. DHSTIER is administered jointly by the OCFO Resource Management Transformation Office (RMTO) and the OCFO Office of Financial Management (OFM) and is hosted on the DHS OneNet at the Stennis Data Center in Mississippi.

- Database: Oracle DB 10g v10.3
- Operating System: Microsoft Windows 2003
- Hardware: HP ProLiant BL460c G1 server

Chief Financial Office VISION (CFO Vision)

CFO Vision is a subsystem of DHSTIER used for the consolidation of the financial data and the preparation of the DHS financial statements. CFO Vision is also administered by RMTO and OFM and is hosted on the DHS OneNet at the Stennis Data Center in Mississippi.

- COTS Software - SAS Financial Management Solutions version 4.3 (FM 4.3) with its own internal SAS database
- Operating System: Microsoft Windows 2003 Hardware: HP ProLiant BL460c G1 server

Transportation Security Administration (TSA)

Core Accounting System (CAS)

CAS is the core accounting system that records financial transactions and generates financial statements for the United States Coast Guard. CAS is hosted at the Coast Guard's FINCEN in Chesapeake, VA and is managed by the United States Coast Guard. The FINCEN is the Coast Guard's primary financial system data center. CAS interfaces with other systems located at the FINCEN, including FPD.

- CAS Version 4.1
- CAS Oracle Database 9.2.0.8.0 – 47 GB 16x750mhz RISC Processor; cgofprod.world
- CAS Operating System – HP Unix 11.11; ARGUS Server

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 purchase requests, issue procurement documents, perform system administration responsibilities, and reconcile weekly program element status reports. FPD is interconnected with the CAS system and is hosted at the FINCEN in Chesapeake, VA and is and managed by the United States Coast Guard.

- FPD Oracle 9.2.0.8.0 Database – 28 GB 12x750mhz RISC Processor; LUFS.world
- FPD Operating System – HP UNIX 11.11; Dart Server

Sunflower

Sunflower is a customized third party COTS product used for TSA and Federal Air Marshals (FAMS) property management. Sunflower interacts directly with the Office of Finance Fixed Assets module in CAS. Additionally, Sunflower is interconnected to the FPD system and is hosted at the FINCEN in Chesapeake, VA and is managed by the United States Coast Guard.

- Sunflower Oracle Database – 10.2.0.3 - 2 x 3.06 GB Xeon Processor – 72 GB
- Sunflower Operating System – Red Hat Linux 4.0AS
- Sunflower Third Party Software – IBMJava 2.-131RC2

MarkView

MarkView is an imaging and workflow software used to manage invoices in CAS. Each invoice is stored electronically and associated to a business transaction so that users are able to see the image of the invoice. MarkView is interconnected with the CAS system and is located at the FINCEN in Chesapeake, VA and is managed by the United States Coast Guard.

- CAS Oracle Database 9.2.0.8.0 – 47 GB 16x750mhz RISC Processor
- CAS Operating System – HP Unix 11.11; ARGUS Server

United States Citizenship and Immigration Services (USCIS)

CLAIMS 3 LAN

CLAIMS 3 LAN provides USCIS with a decentralized, geographically dispersed LAN based mission support case management system, with participation in the centralized CLAIMS 3 Mainframe data repository. CLAIMS 3 LAN 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 the following service centers and district offices: Nebraska, California, Texas, Vermont, Baltimore District Office, and Administrative Appeals Office. CLAIMS 3 executes on Dell 220 S (EMC), RAID Controller, Disk Storage servers protected by firewalls, and Windows 2003, MS Sp2 as the operating system and Pervasive database software and is used to enter and track immigration applications. CLAIMS 3 LAN interfaces with the following systems:

- Citizenship and Immigration Services Centralized Oracle Repository (CISCOR)
- CLAIMS 3 Mainframe
- Integrated Card Production System (ICPS)
- CLAIMS 4
- E-filing
- Benefits Biometric Support System (BBSS)
- Refugee, Asylum, and Parole System (RAPS)
- National File Tracking System (NFTS)
- Integrated Card Production System (ICPS)
- Customer Relationship Interface System (CRIS)
- USCIS Enterprise Service Bus (ESB)

CLAIMS 4

The purpose of CLAIMS 4 is to track and manage naturalization applications. Claims 4 is a client/server application. CLAIMS 4 runs off of Sunfire 890, 490, Solaris 9, and Oracle 9iR2 servers with Oracle 9i, Windows NT, and Windows 2000 Server operating systems and are

protected by firewalls. The central Oracle Database that runs off Oracle Enterprise 9i is located in Washington, DC while application servers and client components are located throughout USCIS service centers and district offices. CLAIMS 4 interfaces with the following systems:

- Central Index System (CIS)
- Reengineered Naturalization Automated Casework System (RNACS)
- CLAIMS 3 LAN and Mainframe
- Refugee, Asylum, and Parole System (RAPS)
- Enterprise Performance Analysis System (ePAS)
- National File Tracking System (NFTS)
- Asylum Pre-Screening System (APSS)
- USCIS Enterprise Service Bus (ESB)
- Biometrics Benefits Support System (BBSS)
- Enterprise Citizenship and Immigration Service Centralized Operational Repository (eCISOR)
- Customer Relationship Interface System (CRIS)
- FD 258 Enterprise Editions and Mainframe
- Site Profile System (SPS)

Department of Homeland Security
Information Technology Management Letter
September 30, 2010

Appendix B
FY 2010 Notices of IT Findings and Recommendations at DHS

Department of Homeland Security
Information Technology Management Letter
September 30, 2010

Notice of Findings and Recommendations (NFR) – Definition of Severity Ratings:

Each NFR listed in Appendix B is assigned a severity rating from 1 to 3 indicating the influence on the DHS Consolidated Independent Auditors Report.

1 – Not substantial

2 – Less significant

3 – More significant

The severity ratings indicate the degree to which the deficiency influenced the determination of severity for consolidated reporting purposes.

These rating are provided only to assist the DHS in prioritizing the development of its corrective action plans for remediation of the deficiency.

Department of Homeland Security
FY 2010 Information Technology - Notice of Findings and Recommendations – Detail

- **United States Coast Guard**

Department of Homeland Security
Information Technology Management Letter
September 30, 2010

Notice of Findings and Recommendations – Detail
Coast Guard

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CG-IT-10-01	In FY 2009, we determined that Coast Guard was finalizing the business process that would be used to remediate the prior year NFR. Once this business process is finalized, a technical implementation could begin, and Coast Guard planned on using the Direct Access Human Resources (HR) system to notify system owners of HR status changes for all individuals within the Coast Guard. During our FY 2010 follow-up test work, we determined that this NFR remediation is still in the planning stages. Requirements still need to be prioritized and cost estimates need to be developed in order to obtain funding. Coast Guard still plans on using Direct Access but will only implement this new process once Direct Access has been upgraded, however, the implementation date has not yet been finalized.	We recommend that Coast Guard Headquarters continue with the following efforts: • Develop a resource plan (RP) with associated supporting business case(s) to address account tracking for terminated, transferred, or retired contractor, military, and civilian personnel; and, • Continue existing planning efforts and develop, document, and implement enterprise-wide processes that will notify all impacted system owners of terminated, transferred, or retired contractor, military, and civilian personnel.		X	2
CG-IT-10-02	In FY 2009, we determined that DHS no longer requires all contracted employees to have a Minimum Background Investigation (MBI) if they have an existing confidential or secret clearance, and the new minimum standard is the National Agency Check and Inquiries (NACI). In addition, Coast Guard Headquarters had in place since 2007 Commandant Instruction (COMDTINST) M5520.12C, which stated that Program Managers are responsible for determining the risk level and position sensitivity designation associated with each Contract	We recommend that Coast Guard Headquarters continue with the following efforts: • Continue to update existing contracts to include the new contractor background check requirements, and perform associated contractor background checks. • Continue to include new contractor background check requirements in new contracts, and perform associated background checks.		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	Line Item Number (CLIN) and/or labor category for procured contractor support. These will be provided to the Contracting Officer who is responsible for including as solicitation and contract requirements. Unfortunately, this instruction did not include specific guidance for the Program Managers on how to set the correct and consistent risk levels and position sensitivity designations. In FY 2010, we determined that Coast Guard Headquarters incorporated Program Manager guidance to the Commandant Instruction, as Enclosure 3, so that the Program Managers could determine the correct risk level and position sensitivity designation. An All Coast Guard (ALCOAST) message was also released in June that stated all contractors must have a favorable fingerprint check and initiated or completed minimum investigation (NACI) in order to obtain a Common Access Card (CAC) card, effective immediately. This has resulted in two activities: 1) new contracts will incorporate these new requirements immediately, and 2) existing contracts will incorporate these new requirements when new task orders are issued, options are exercised, contract modifications are made, etc. Therefore, based upon the renewal/option date of a contract in place prior to the ALCOAST, it could take up to two years before all of the contractors throughout Coast Guard will meet these new requirements. Furthermore, as part of our analysis, we were unable to determine if USCG had the capability to	• Develop a RP with associated supporting business case(s) to address the need for a reporting mechanism for contractor risk level, position sensitivity designation, and associated background check.			

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	consistently produce a current and comprehensive list of all Coast Guard contractors to include valid background investigation information tied to the correct risk level and position sensitivity designation. Although Coast Guard has taken corrective actions to remediate the prior year NFR CG-IT-09-10 by updating the Commandant Instruction and begun the process of including the new requirements in contracts, we believe that not having the ability to identify and provide a full population of contractors working for Coast Guard does not fully remediate all of the findings and conditions from FY 2009. Therefore, this prior year NFR will be reissued in FY 2010.				
CG-IT-10-03	In FY 2009, we determined that Coast Guard Headquarters actively monitors all civilians to verify whether they have a valid background investigation on record. Coast Guard stated that it considers Coast Guard government positions that use, develop, operate, or maintain IT systems to be at least low risk based upon OPM guidance. Therefore, Coast Guard continued vetting individuals based on the OPM requirements for low risk positions which require a NACI investigation. This position is not in compliance with the DHS standard that states that all DHS government positions that use, develop, operate, or maintain IT systems are considered at least moderate risk, and per DHS 4300A requirements, a Minimum Background Investigation (MBI) is the minimum standard of investigation.	We recommend that Coast Guard Headquarters continue with the following efforts: • Develop a RP with associated supporting business case(s) to address fixing the organization-wide background investigations report. • Continue existing efforts to update, document, and implement the overall Coast Guard personnel security process for civilian personnel, based upon the JRT report/guidance.		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	In addition, Coast Guard Headquarters did not complete background reinvestigations for all civilian staff due to the fact that this is not a requirement under OPM guidance for low risk positions. This is in non-compliance with DHS policy (MD 11050.2) that states that reinvestigations must be completed every 10 years for moderate risk positions. Further, a Joint Reform Team (JRT) been established by the Office of the Director of National Intelligence (ODNI) and the Office of Management and Budget (OMB) to reform the federal suitability clearance process, and the JRT standards were scheduled for implementation by the end of Calendar Year 2010. The Coast Guard was waiting on the JRT report/guidance to be implemented prior to making a determination on if they would follow the DHS standards in regards to civilian background investigations and reinvestigations. During our FY 2010 follow up, we determined that the Coast Guard will delay issuing any new or updated guidance/instructions until the JRT report/guidance has been issued and will continue to not comply with the DHS standards in regards to civilian background investigation and reinvestigations. Coast Guard will continue to vet civilian individuals based on the OPM requirements and associated methodology both in terms of initial background investigations and re-investigations. In addition, Coast Guard has created an organization-				

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	wide automated report that shows the background investigation status of each civilian Coast Guard employee. However, Coast Guard is currently unable to consistently generate error-free reports. Coast Guard stated that the report could be corrected within two years if additional resources are provided.				
CG-IT-10-04	From the period of October 1, 2009 through the November 29, 2009, there was not adequate guidance in place for Coast Guard to properly assess the financial statement impact of changes to the production environment of the CAS, FPD and WINS. During this time period, two CAS changes were implemented into production without a proper assessment of the financial statement impact of the proposed changes. Upon the effective date of the *Financial Impact Determination for Data Scripts and System Change Requests* Memorandum on November 30, 2009, Coast Guard began and continued to follow adequate guidance to properly assess the financial statement impact of changes to CAS, FPD and WINS.	No recommendation required. Coast Guard took appropriate corrective action during the current fiscal year to remediate the exception that was identified during this fiscal year.	X		1
CG-IT-10-05	We determined that some previously noted weaknesses were remediated (particularly in the second half of FY 2010), while other control deficiencies continued to exist. The remaining control deficiencies that were present throughout FY 2010	We recommend that Coast Guard: • Update the scripting policies and procedures to include additional and more detailed test documentation; • Develop training that addresses all aspects of		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	vary in significance, however three key areas that impact the Coast Guard Script control environment are: 1) Script Testing Requirements; 2) Script Testing Environment; and 3) Script Audit Logging Process. a. Script Testing Requirements: Limited testing requirements exist to guide FINCEN staff in the development of test plans and guidance over the functional testing that should be performed. Additionally, we determined that there are no detailed requirements over the review and testing of functional changes to the data. FINCEN only tracks and documents the number of transactions updated on scripts that have a financial impact and not the detailed dollar amounts associated with the financial impact transactions. b. Script Testing Environment: Not all script changes were tested in the appropriate CAS Suite test environments, as required. FINCEN management informed us that the testing environments, CAS4 and LUFSFQT3, were offline for these exceptions due to a refresh of the databases and that testers used CAS3 and Alpha as alternate testing environments instead. However, FINCEN management informed KPMG that these environments are refreshed on an as needed basis and no further information could be provided over how frequently the CAS3 and Alpha databases were refreshed to verify that the scripts were adequately tested in the appropriate	script testing (including documentation of test documents) and provide training to appropriate CM staff; • Develop a resource plan with associated supporting business case(s) to address the database audit logging requirements; • Develop procedures and perform regular account revalidation for Serena to ensure privileges remain appropriate; and • Conduct an assessment over the Internal Control Over Financial Reporting (ICOFR) process related to identifying and evaluating scripts that have a financial statement impact.			

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	environment. Furthermore, we determined that guidance is not provided over the use of alternate testing environments for the testing of scripts to ensure they are adequately tested. c. Script Audit Logging Process: The CAS, FPD, and Sunflower databases are logging changes to tables as well as successful and unsuccessful logins. However, no reconciliation between the scripts run and the changes made to the database tables is being performed to monitor the script activities and ensure that all scripts run have been approved through Change management Script System or Serena. In addition, we noted that FINCEN has not established a formal process to monitor and review changes made to the Sunflower database including the tables and activities modified by the database administrators. During our test work, we noted weaknesses in the script change management process as it relates to the ICOFR process (e.g., the financial statement impact of the changes to the CAS Suite through the script change management process). While a process exists to identify, and route a script with potential financial statement impact through an assessment process, the review and determination over each script is primarily performed without structured/detailed procedures in place. Furthermore, the rationale documenting the impact of the script, whether deemed as having financial impact or not, is not documented and retained. In addition, within the CAS Suite				

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	environment, there are over 200 scripts run on a weekly basis and we noted that the financial statement impact assessment is essentially performed by a single branch, which has authorized only three people to assess the scripts.				
CG-IT-10-06	To complement our IT audit testing efforts as part of the FY 2010 DHS Financial Statement Audit and Audit of Internal Control over Financial Reporting, we also performed social engineering testing. This testing was conducted at key Coast Guard locations that process, support and house Coast Guard financial data. Social engineering is defined as the act of attempting to manipulate or deceive individuals into taking action that is inconsistent with DHS policies, such as divulging sensitive information or allowing / enabling computer system access. The term typically applies to trickery or deception for the purpose of information gathering, or gaining computer system access. During the course of our social engineering test work, the objective was primarily focused on attempting to obtain user passwords. Posing as DHS technical support employees, attempts were made to obtain this type of account information by contacting randomly selected USCG employees by telephone at two Coast Guard locations, Headquarters (HQ) and the Coast Guard FINCEN. A script was followed which had us ask for assistance from the user in resolving a Coast Guard network issue. As presented in the following table, for each person we attempted to call, we noted whether the individuals were reached and whether we	We recommend that Coast Guard Headquarters update the annual Information Assurance (IA) training to include more robust "phishing" and "social engineering" guidance and instruction and explicitly test individuals during the training on these topic areas.		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	obtained any information from them that should not have been shared with us according to DHS policy. Our selection of individuals was not statistically derived, and, therefore, we are unable to project results to the Coast Guard or the DHS as a whole.				
CG-IT-10-07	During the FY 2010 IT Audit, a selection of newly created users of the JUMPS application was made to inspect whether applicable documentation was recorded and retained to identify authorized users. We determined that documentation was not retained for one of the five users selected. We performed inquiry procedures with management to determine that access was appropriately restricted for this user; however, no JUMPS Access Authorization Form could be located. On July 20, 2010, management remediated the exception by completing a new JUMPS Access Authorization Form for the noted user with a copy of the form being entered into the Coast Guard's ImageNow imagining repository.	As noted in the condition, management remediated the exception upon notification of this IT NFR. No additional actions are required and, therefore, no recommendation will be issued.	X		1
CG-IT-10-08	During our FY 2010 test work, we determined that the Coast Guard TIER System password setting for lockout duration (PASSWORD_LOCK_TIME) is only configured to 0.0005 days (less than one minute). This setting was subsequently remediated on 7/19/201 to a setting of "UNLIMITED" which requires an administrator to unlock the account. We observed and noted that this remediation was taken by Coast Guard.	No recommendation required. Coast Guard took appropriate corrective action during the current fiscal year to remediate the exception that was identified during this fiscal year.	X		1

Department of Homeland Security
Information Technology Management Letter
September 30, 2010

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CG-IT-10-09	To complement our IT audit testing efforts as part of the FY 2010 DHS Financial Statement Audit and Audit of Internal Control over Financial Reporting, we also performed after-hours physical security testing. This testing was conducted at key Coast Guard locations that process, support and house Coast Guard financial data. We performed after-hours physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects include physical access to media and equipment that houses financial data and information residing on a USCG employee's / contractor's desk, which could be used by others to gain unauthorized access to systems housing financial information. The testing was performed at various USCG locations that process and / or maintain financial data. After gaining physical access to the facilities with a USCG employee who was designated to assist with and monitor our test work, we inspected a selection of 45 desks, cubicles, offices, and other work areas for each location. During the testing we were looking for items such as improper protection of user account login information, unsecured portable system hardware, including laptops and external hard drives, and open / active application or network sessions. In addition, we inspected work areas for documentation marked "For Official Use Only" (FOUO), personally identifiable information (PII), Federal Government credits cards, and agency badges. This list does not encompass the total type of items we were searching for during our	We recommend that Coast Guard: • Update the annual IA training to include more robust office "physical security" and "clean desk" guidance and instruction and explicitly test individuals during the training on these topic areas. • Implement enterprise-wide and site-specific processes for verifying the effectiveness of this training via mechanisms such as scheduled and ad hoc desk checks, training follow-ups, and other management controls.	X		2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	testing. As depicted in the following table, for each location visited, we noted the type of unsecured information or property we identified and included the total exceptions noted by location, as well as by type of information or property identified.				
CG-IT-10-10	In FY 2009, we determined that the Role-Based Training for USCG IA Professionals Commandant Instruction had been renamed the Role-Based Industry Standards for USCG IA Professionals Commandant Instruction. However, the renamed Instruction remained in draft form. In addition, we determined that once the Instruction had been finalized, the curriculum had been agreed upon and the training implemented, Coast Guard would utilize the Professional Certifications and Licenses module within the Direct Access system rather than the Training Management Tool (TMT) to monitor and verify training completion. This was not the case as Direct Access was not configured to track contractor information and, therefore will not include training information for contractors. The Instruction continued to reference the use of the TMT and had not been updated to include procedures for utilizing Direct Access. During our FY 2010 follow-up test work, we determined that the *Role-Based Industry Standards for USCG IA Professionals* Commandant Instruction had been renamed *Information Assurance Professional Certifications* and was formally issued on March 23, 2010. The Instruction stated that all military employees assigned to an IA role must obtain a	We recommend Coast Guard Headquarters: X • Continue to implement Commandant Instruction *Information Assurance Professional Certifications*. • Improve and utilize its manual tracking process until such time that the Direct Access implementation is in place.			

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	required certification within 12 months of the Commandant Instruction issue date (*i.e.*, March 23, 2011), and all civilian employees currently in an IA role would be granted a waiver within 12 months of the Commandant Instruction issue date. The Commandant Instruction further stated: 1) both military and civilian employees assigned to an IA role after the issuance date would be required to obtain a certification within 12 months, including transfers, and 2) all certifications must be recorded / tracked in Direct Access. Pertaining to contractors, the Contracting Officer Technical Representative (COTR) must keep records of all IA personnel that require and have received role-based certification preparation or Continuing Professional Education (CPE) credits, and all training and certification requirements are inserted within all future statements of work and awarded contracts. The instruction also states that all IA personnel (military, civilians, and contractors) must receive initial professional certification preparation and annual CPEs thereafter prior to being granted Coast Guard IT systems access specific to those security duties. Although Coast Guard has taken corrective actions to remediate this prior year NFR, we determined that even though the corrective actions are planned for completion by March 2011, they have not yet been completed in FY 2010 (i.e., all IA professionals who are required to obtain / maintain a professional certification within a year of the date of the Instruction have not obtained a certification to date). Our testing				

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	noted that 8 or 3.9% of Coast Guard IA professionals out of the total population of 205 have the required certification for their prescribed level on file. Furthermore, we noted that 59 or 28.7% of Coast Guard IA professionals have not provided evidence of industry-based training. In addition, through our testing, we could not determine the number of IA professionals that had been granted waivers for the certification requirement. In closing, we also noted that 14 Coast Guard System Administrators were not listed as being part of the 205 Coast Guard IA professionals.				
CG-IT-10-11	During the FY 2010 IT Audit, a selection of users added to the CG TIER application for the fiscal year was made to inspect whether proper documentation was recorded and retained for identify authorized users. Our testing determined that documentation was not retained for one of the two CG TIER users selected. Upon further inquiry with management, we were informed that the identified CG TIER user was authorized access by the Financial Branch Chief; however, the email approval had been lost.	We recommend that Coast Guard Finance Center take the follow actions: • For the user identified during testing, complete and retain all appropriate access request documentation; and, • Update the CG TIER account management procedures to effectively track and retain user access documentation.	X		1
CG-IT-10-12	During our FY 2009 test work, we determined that on a quarterly basis, 45-90 Direct Access user accounts are randomly sampled and formally reviewed to determine if access remains appropriate for each selected user account. As part of the quarterly review, Coast Guard's Pay and Personnel Center (PPC) management verifies that no single user has both CGAPPL (ability to enter an applicant) and CGHRSUP (ability to hire an application) roles. PPC management then verifies that no user has both	We recommend Coast Guard headquarters and the PPC: • Develop a RP with associated supporting business case(s) to address the 100% account review requirement. • Continue to coordinate with the DHS CISO's office to determine and formalize the frequency and depth / breadth of effective reviews that address the perceived risk. Based upon the results of these discussions with the		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	CGAPPL and CGHIRE privileges within the Direct Access application. Per PPC management, there are 17,496 individuals with active Direct Access accounts that maintain greater than read-only access. PPC management further advised us that 6,920 (40%) of the Direct Access accounts were revalidated during the period of October 1, 2008 – September 17, 2009, leaving 10,576 (60%) Direct Access accounts not revalidated during FY09. As a result, we determined that 100% of Direct Access user accounts with greater than read-only access are not annually reviewed per the DHS requirement. During our FY 2010 test work, we were informed by the Coast Guard that an annual review of 100% of the Direct Access user accounts with greater than read-only access (and their associated privileges) has not been performed for this fiscal year. Coast Guard also informed us that all Direct Access accounts created and/or modified during the fiscal year have been reviewed as part of the normal transfer and aging processes; however, our testing did not extend to validate this statement. Based upon a risk based decision, the Coast Guard has designed a process to review a subset of users that represent the greatest risk to Direct Access. This annual review would cover approximately 743 Direct Access users. The scope of the review includes users with payment approval, security administrator permissions, all contractors, and users with update/delete permissions.	DHS CISO's office, the Coast Guard will modify procedures and develop, if applicable, required waivers/exceptions to reflect an adequate percentage of Direct Access user accounts to be reviewed. • Continue to use its existing risk-based account review efforts until such time that the procedures are updated in response to the activities associated with the second recommendation.			

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	However, since this subset review does not cover 100% of the Direct Access user accounts with greater than read-only access (and their associated privileges) as required by DHS, we consider this NFR to be re-issued.				
CG-IT-10-13	During our testing, we determined that all previous year conditions listed in NFRs CG-IT-09-46 were properly remediated by USCG. We consider this prior-year IT NFR as closed. As part of this year's testing, we identified one security configuration management weakness (i.e., outdated operating system software) on hosts supporting CAS, FPD, NESSS, as well as those systems' network infrastructure and associated workstations. Table 1, starting on the next page, lists the conditions as identified by the software tool used, the system (host) impacted, effect statement, IT general control area, software tool used to identify the condition, and if the condition identified was a prior year IT audit issue. The conditions listed in Table 1 are potentially exploitable by an insider without specific knowledge of the operation of the system or the applications hosted on that system.	We recommend that Coast Guard FINCEN: • Develop a RP with associated supporting business case(s) to address the installation of Service Pack 3 on all applicable Windows XP workstations and/or upgrade the operating systems of these workstations to the Coast Guard's Vista-based Standard Image 6.0. • Develop a RP with associated supporting business case(s) to address the server operating system upgrades to include a technical analysis to ensure Windows 2003 server upgrades do not adversely affect system operation. • Based upon the results of Recommendation 1 and Recommendation 2, schedule and perform the upgrades and/or patches of the impacted servers and workstations.	X		1
CG-IT-10-14	During our FY 2010 audit test work, we sampled 25 new user accesses for NESSS that were granted during the fiscal year to determine if an access authorization form had been completed, if the access had been timely approved by the user's supervisor, and that the	We recommend the Coast Guard's Operation Systems Center (OSC) update the NESSS account management Standard Operating Procedure (SOP) to provide clear guidance regarding the use of user access forms and update the access form to include	X		2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	forms were retained. Based upon our testing, we were unable to obtain 9 of the 25 user access forms. In addition, evidence of supervisory approval for 9 of the 25 sampled users was not available.	an approval signature line.			
CG-IT-10-15	During the FY 2010 audit test work, Aviation Logistics Center (ALC) visitor logs for the fiscal year were obtained to determine whether proper documentation was recorded and retained for the verification of individuals visiting the ALC Data Center and Facility. Our testing determined that the ALC Customer Support Desk did not properly complete the visitor logs during the FY 2010 audit period. Specifically, from a total of 190 visitor log entries for the fiscal year, 33 visitor log entries did not have the Date-Out and Time-Out fields completed and 31 visitor log entries did not have the Sponsor field completed. Additionally, the ALC Data Center Access Listing was obtained to determine whether a review of the access listing was conducted and evidence of the review was performed and maintained. Our testing determined that the evidence of reviews of the Data Center Access for the FY 2010 period was not maintained. Therefore, we could not determine that the Data Center Access Listing had been properly reviewed during the year.	We recommend that Coast Guard: • Develop and maintain an SOP to ensure that the ALC Data Center Access Control list is kept current and that its quarterly review is documented and maintained; and • Re-emphasize to all ALC Support Desk personnel (through training), the importance of properly maintaining the visitor log and to ensure it is filled out completely and accurately.	X		1

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CG-IT-10-16	During the FY 2010 IT Audit, the Aviation Maintenance Management Information System (AMMIS) password configuration settings were obtained and tested to determine whether they complied with DHS policy. Our testing determined that the AMMIS subsystem password configuration settings do not comply with all of the required DHS password guidelines. Specifically, AMMIS password configuration settings did not comply with the following DHS password policy: • Contain a combination of alphabetic, numeric, and special characters – the AMMIS password requires a combination of alphabetic, numeric, or special characters; and • Not be the same as the previous 8 passwords. The AMMIS password configuration is set to be the same as the previous 6 passwords. Additionally, our testing determined that the current Aviation Logistics Management Information System (ALMIS) System Security Plan (SSP), which includes the system level requirements of the AMMIS subsystem, states that the implemented password configuration does not comply with the current DHS password policy. Specifically, the ALMIS SSP states that the password cannot be the same as the previous 6 passwords; however, DHS guidance states that passwords cannot be the same as the previous 8 passwords.	We recommend that the Coast Guard configure the AMMIS application to enforce the strong password and password history requirements described in the DHS Management Directive 4300A Policy Directive and to update all impacted Certification & Accreditation and system documentation accordingly.	X		1

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CG-IT-10-17	To complement our IT audit testing efforts as part of the FY 2010 DHS Financial Statement Audit and Audit of Internal Control over Financial Reporting, we also performed social engineering testing. This testing was conducted at key Coast Guard locations that process, support and house Coast Guard financial data. Social engineering is defined as the act of attempting to manipulate or deceive individuals into taking action that is inconsistent with DHS policies, such as divulging sensitive information or allowing / enabling computer system access. The term typically applies to trickery or deception for the purpose of information gathering, or gaining computer system access. This was the second round of social engineering testing conducted as part the FY 2010 DHS Financial Audit and Audit of Internal Control over Financial Reporting. Our initial testing occurred back on June 30th and July 1st. Our initial testing resulted in Coast Guard IT-NFR-10-06 being issued. The testing approach and scope for the second round of testing was the same as the initial round. During the course of our social engineering test work, the objective was primarily focused on attempting to obtain user passwords. Posing as DHS technical support employees, attempts were made to obtain this	It is recommended that Coast Guard implement the recommendations presented in Coast Guard IT-NFR-10-06. No additional actions are required.	X		2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	type of account information by contacting randomly selected USCG employees by telephone at two Coast Guard locations, Headquarters (HQ) and the Coast Guard Finance Center (FINCEN). A script was used to ask for assistance from the user in resolving a network issue at the Coast Guard. As presented in the following table, for each person we attempted to call, we noted whether the individuals were reached and whether we obtained any information from them that should not have been shared with us according to DHS policy. Our selection of individuals was not statistically derived, and, therefore, we are unable to project results to the component or department as a whole.				
CG-IT-10-18	Our testing determined that the evidence of reviews over the AMMIS audit logs for the FY 2010 audit period were not maintained by ALC. Therefore, we could not determine if the AMMIS audit logs had been properly reviewed during the year. Additionally, our testing determined that reviews of all deactivated AMMIS accounts may not have been performed and evidence of the reviews was not maintained by the ALC. Therefore, we could not determine whether deactivated AMMIS accounts had been properly monitored and reviewed during the year. Lastly, we were informed by the ALC that the AMMIS audit logs were not being reviewed by an individual that is considered independent to the process. We noted that an AMMIS system	We recommend that Coast Guard: • Update the AMMIS Standard Operating Procedures to address the audit log review and retention procedures; and • Implement separation of duties for the AMMIS audit log reviews.	X		2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	administrator is responsible for reviewing the AMMIS audit logs.				
CG-IT-10-19	Our testing determined that evidence of a review and recertification of the 11,306 users with "Update" privilege in ALMIS was not maintained by the ALC. Therefore, we could not determine that ALMIS user accounts had been properly reviewed and recertified during the year.	We recommend that Coast Guard: • Develop a RP with associated supporting business case(s) to address the 100% account review requirement; • Continue to coordinate with the DHS CISO's office to determine and formalize the frequency and depth / breadth of effective reviews that address the perceived risk. Based upon the results of these discussions with the DHS CISO's office, the Coast Guard will modify procedures and develop, if applicable, required waivers/exceptions to reflect an adequate percentage of ALMIS user accounts to be reviewed; and • Continue to use its existing risk-based account review efforts until such time that the procedures are updated in response to the activities associated with the second recommendation.	X		2
CG-IT-10-20	Our testing determined that the AMMIS Software Change Request Forms were not appropriately authorized. Specifically, for the four (4) AMMIS software changes made during the fiscal year, two (2) of the software change request forms were not signed by the Division Chief.	We recommend that Coast Guard establish and follow a management review process to ensure that any new AMMIS SCRs processed will be reviewed by the PC team for the proper / required signatures.	X		1

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CG-IT-10-21	During our FY 2010 audit test work over the NESSS recertification process, we noted that 32 users were assigned the role FLS_USR_ADM_GRP within the NESSS application. This role grants the ability to add, modify, and delete user accounts. In addition, two (2) of these users were system administrators. This number of users with this elevated role was considered excessive based upon the ratio of this role to the NESSS user population. On October 7, 2010, OSC management remediated the condition by reducing the number of users with the FLS_USR_ADM_GRP role down to six.	Coast Guard took appropriate corrective action to remediate the exception that was identified and no additional corrective actions are required.	X		2
CG-IT-10-22	We determined that Operations System Center (OSC) had updated the policies and procedures for System Administrators (SAs) and Database Administrators (DBAs) to include more detail and instructions on entering sufficient evidence regarding the weekly non-independent audit log reviews documented and tracked in the ClearQuest Ticketing system. We also noted that the monthly SAM audit log reviews were being conducted by an independent team. Although OSC has taken steps to remediate the prior year conditions by updating the policies and completing the monthly independent reviews, we determined that the 3 sampled months of SA and DBA audit log reviews did not have sufficient detail on the ClearQuest tickets. Specifically, we identified the following:	We recommend that Coast Guard: • Update the SAM and NESSS audit log review procedures within the Standard Operating Procedures to include more detail in the ClearQuest Tickets including recording the results of the review of the audit logs; • Implement similar separation of duties for the NESSS audit log reviews as have been implemented for the SAM audit log reviews; and; • Continue with ongoing efforts for identifying, designing, and implementing automated tools to assist in audit log collection, storage, analysis, and reporting which will further improve consistency, timeliness, and accuracy of the reviews when compared with labor and time intensive manual processes.		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	• 1 of the 3 SA monthly reviews did not have a searchable title • 2 of the 3 SA monthly reviews did not include results of the audit log review (i.e., audit logs had no exceptions.) • 3 of the 3 DBA monthly reviews did not list the logs that were included in the review • 3 of the 3 DBA monthly reviews did not have results of the audit log reviews As a result of limitations of the underlying operating system of the Shore Asset Management System AM system: • The servers do not automatically alert in the event of an incident. • The server operating systems do not inherently provide audit reduction and report generation capability. Furthermore, the OSC has not implemented a centralized log solution for audit log reduction and reporting, and automated alert notifications. <u>NESSS Audit Logs:</u> During our FY 2010 test work for the NESSS, we noted that daily and weekly audit log reviews are performed by the NESSS System Administrator. The weekly audit log reviews are documented in the ClearQuest system with a running ticket for the calendar year. Each week's review is added to the				

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	ClearQuest ticket. However, we determined that there is not sufficient detail in the ClearQuest ticket in recording the results of the review of the audit logs. Furthermore, as similar to SAM audit log review process listed above, OSC has not implemented a centralized log solution for audit log reduction and reporting, and automated alert notifications. In addition, the weekly reviews are performed by the NESSS System Administrator, who is not considered an independent party as required by DHS MD 4300A.				
CG-IT-10-23	During the FY 2010 audit test work, the OSC data center access listing was obtained in order to determine whether a review of the access listing was conducted and evidence of the review was maintained. OSC informed us that they perform a review of the data center access on a quarterly basis. However, our testing determined that the evidence of reviews concerning OSC data center access for the FY 2010 period was not maintained. Therefore, we could not determine whether the OSC data center access listing had been properly reviewed during the year.	We recommend that Coast Guard develop detailed procedures for: • Quarterly data center access reviews to include validating that users have a physical need to access the data floor; and • Methods for maintaining the review documentation.	X		1
CG-IT-10-24	During prior financial statement audits dating back to FY 2003, we noted that the implementation and oversight of the Coast Guard's information security controls needed various improvements. In FY 2010, continued improvements have been made in the areas of access controls, entity-level controls, and configuration management. Improvements in the IT control environment were identified at each of the Coast Guard financial processing locations where IT	We recommend Coast Guard to: • Continue to implement and improve upon the monitoring of compliance with DHS, Coast Guard, and Federal security policies and procedures in the areas of script configuration management controls to include the use of the automated tools deployed at the FINCEN; and • Develop and implement corrective action		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	audit was previously conducted. However, significant improvements are still warranted in the area of script configuration management controls for the key financial systems located at the FINCEN. Script configuration management control is the subject of the significant control deficiencies identified and recommendations that were developed during the audit. Other weaknesses continued to exist, to a lesser extent, in the areas of access controls and entity-wide security at each of the Coast Guard financial processing locations. These continued weaknesses require Coast Guard to continue with the implementation of their corrective actions plans and monitoring efforts. 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 Federal Financial Management Improvement Act (FFMIA).	plans to address and remediate the NFRs issued during the FY 2010 audit.			
CG-IT-10-25	During our FY 2010 year-end IT roll-forward audit testing procedures, we determined that one (1) of the five (5) Financial Procurement Desktop (FPD), Production Implementation Request (PIR) forms tested was not signed off on by the analyst/submitter/implementer as required per the FINCEN PIR form.	The process for obtaining written sign-off on PIR forms has recently been replaced with an automated workflow process that eliminates the need for written approvals; therefore no additional corrective actions are required.	X		1

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CG-IT-10-26	During the FY 2010 audit test work, we determined that ALC policies and procedures for the following control areas are not adequately detailed to provide clear and complete control descriptions for each of the following processes: • Physical Access to the data center and systems in the data center; • Access to Program Libraries; • Segregation of Duties in support of the AMMIS application; • AMMIS Audit Log Review and Retention; • Backups and Data Restoration; and, • Offsite Storage of Backup media.	We recommend that Coast Guard develop, document, communicate, train, test, and continuously maintain policies and procedures for the cited control and process areas.	X		2
CG-IT-10-27	The NESSS' Oracle *verify_function* in the SYS schema is incorrectly configured and does not include verification of special characters for passwords.	We recommend that Coast Guard review and update the Oracle *verify function* in the SYS schema to include the verification of special characters for passwords.	X		1
CG-IT-10-28	During our FY 2010 audit test work, we followed up with Coast Guard management and were notified that this Direct Access audit logging weakness, noted in FY 2009, cannot be resolved until Direct Access is updated to PeopleSoft version 9. There is no current timeline for the upgrade to take place. The following conditions were noted last year and are still open in FY 2010. Not all Direct Access failed logon attempts are logged or reviewed; and account management audit logs for the Direct Access application are not reviewed on a	We recommend Coast Guard continue with the PeopleSoft 9.0 upgrade and PeopleSoft Portal implementation.		X	1

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	monthly basis, which is a requirement set forth within DHS Policy.				

Department of Homeland Security
FY 2010 Information Technology - Notice of Findings and Recommendations – Detail

- **Customs and Border Protection (CBP)**

Department of Homeland Security
Information Technology Management Letter
September 30, 2010

Notice of Findings and Recommendations – Detail
Customs and Border Protection

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-10-01	This is a system-level finding. KPMG noted that CBP portal accounts for separated employees are removed on a bi-weekly basis and are not removed on the day of the individual's separation as required by CBP and DHS policy. KPMG did note that CBP is aware of the issue and is looking into an automated solution for compliance with CBP and DHS policy. Upon further testing of terminated employees, KPMG did not find any users that had accessed the system after their separation date from CBP.	CBP should implement procedures to reinforce adherence to guidance requiring timely notification of separations by employees or contractors with access to ACE. Those responsible for ACE access control need to be notified of a separation no later than the day of separation.		X	2
CBP-IT-10-02	This is a system level finding. KPMG noted that ACE is not currently configured to prevent incompatible roles from being assigned to a user, as required by CBP and DHS policies. While, initial steps have been taken to address formal segregation of duties within the system, no additional actions have taken place.	CBP Office of Information and Technology will continue to work with the Office of International Trade, Office of Administration and Office of Field Operations to identify incompatible roles and develop procedures as part of the access control process to ensure that these role combinations are not granted to ACE users, except when a waiver is granted in writing.		X	2
CBP-IT-10-03	This is a system-level finding. KPMG noted that evidence of completed ACE system log (Syslog) reviews did not include an appropriate level of detail. Specifically, during the majority of FY 2010, there was no formal method of documenting who performed the audit log reviews, when they were reviewed, what issues (if any) were identified, and the actions taken (if applicable). KPMG noted that procedures regarding the review of ACE audit logs have been established prior to FY 2010, and that management is currently implementing a formal method of documenting the requisite system log review information.	We recommend that CBP maintain evidence that regular reviews of audit logs are occurring. Specifically, we recommend that CBP continue with plans initiated in July of 2010 to institutionalize a more formal method of documenting who performed reviews of audit logs, when these reviews occurred, and what issues (if any) were identified. We also recommend that CBP perform a cost/benefit analysis to determine whether an ACE custom-developed solution or a purchased COTS product should be implemented for full automation of audit log reviews.		X	2
CBP-	Social engineering is defined as the act of attempting to	We recommend that CBP implement multiple types of	X		2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
IT-10-05	manipulate or deceive people into taking action that is inconsistent with policies, such as divulging sensitive information or allowing / enabling computer system access. The term typically applies to trickery or deception for the purpose of information gathering, or computer system access. The objective of our social engineering test work primarily focused on attempting to identify user passwords. Posing as DHS technical support employees, attempts were made to obtain this type of account information by contacting randomly selected employees by telephone. A script was used to ask for assistance from the user in resolving a network issue in the component. For each person we attempted to call, we noted in the table below whether the individual answered and whether we obtained any information from them that should not have been shared with us according to DHS policy. Our selection of individuals was not statistically derived, and therefore we are unable to project results to the component or department as a whole. Of 25 individuals called, 16 answered. Of the 16 that answered, 2 divulged their network password.	security awareness reminders and opportunities to educate users of the importance of protecting CBP information systems and data. Specifically, we recommend that social engineering evaluations be incorporated into routine site inspections to test employee's security awareness and to educate users on how to respond to information security attacks.			
CBP-IT-10-06	This is a system-level finding. KPMG requested access authorization documentation for 25 individuals who were granted ACE access during FY 2010. Initial access requests and approvals for 9 of these individuals were not provided. Although a process for creating and maintaining user access forms and requests has been in place since before the beginning of FY 2010, access approvals prior to the creation of ACE accounts were not consistently maintained in accordance with CBP policy and procedures.	We recommend that the Office of Information and Technology (OIT) issue a memorandum and distribute the procedures to the respective CBP Offices to implement. We also recommend that monitoring procedures be established to ensure compliance with the procedures and that OIT coordinate a meeting with the other CBP Offices to determine if centralized access control measures are necessary.		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-10-07	We performed after-hours physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects include physical access to equipment that houses financial data and information residing on CBP personnel desks, which could be used by others to inappropriately access financial information. The testing was performed at various CBP locations that process and/or maintain financial data. A CBP employee was designated to assist with and monitor our test work. After gaining access to CBP facilities, we inspected a selection of desks and/or offices, looking for items such as improper protection of system passwords, unsecured information system hardware, documentation marked FOUO, and unlocked network sessions. Our selection of desks and offices was not statistically derived, and therefore we are unable to project results to the component or department as a whole. For each location visited, we note the type of unsecured information or property we identified and included the total exceptions noted by location, as well as by type of information or property identified. A total of 102 instances were identified across the six locations where physical assets or sensitive information was not secured in accordance with DHS and/or CBP policies.	CBP should continue its annual security awareness training. In addition, it should seek to add other means of increasing security awareness.		X	2
CBP-IT-10-08	This is a component-level finding. KPMG noted that separation procedures for contract employees (Customs Directive 51715-006) are out of date and include incomplete and inaccurate references. Specifically, the procedures have not been updated since September 2001. The procedures reference Treasury facilities and	We recommend that CBP review the current Customs Directive and update it to reflect the current operating environment. Additionally, we recommend that CBP require the consistent and accurate completion of the SF 242 for all separating contractors with access to CBP facilities, information systems and/or sensitive information.		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Treasury policies as source documentation. KPMG notes that a new directive, CBP Directive 1210-007, entitled 'Contractor Tracking System,' was issued requiring the use of the Contractor Tracking System; however, the new directive still refers to out of date Customs Directive 51715-006 for separation procedures for contractor employees. Additionally, KPMG noted that SF 242 contractor separation forms are not completed consistently for separating CBP contractors. Specifically, KPMG noted that of 45 separated contractors with access to CBP facilities, information systems, and/or sensitive information who were selected for testing, 9 forms were not completed, were not provided, or were not completed in a timely manner.				
CBP-IT-10-09	This is a component level finding. KPMG selected 45 government employees that had separated in FY 2010 and noted that 19 of these individuals did not have a completed CBP Form 241 on file.	We recommend that CBP review the validity of the CBP Form 241 Employee Separation process and determine an alternate mechanism to hold managers accountable for timely notification of employee separations and for confirming the termination of access to information systems, and the return of property and equipment.		X	2
CBP-IT-10-10	This is a component level finding. While KPMG notes that progress has been made in implementing procedures requiring the signing of NDAs, KPMG noted that NDAs are still not consistently completed by contractors at CBP. Specifically, KPMG noted that out of a selection of 45 contractors, one NDA was signed more than four months after the hire date. In addition, one NDA was not provided for a contractor in a medium or high risk position. Further, KPMG noted that the NDAs for 27 contractors in medium or high risk positions did not have a date of signature.	We recommend that CBP implement a more consistent method of ensuring that each contractor employee in moderate and high-risk positions sign and date a NDA.		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-10-11	This is a component-level finding. KPMG has noted that CBP has not been able to provide evidence that workstations not on [redacted] are receiving anti-virus and other security patch updates on a timely basis. KPMG noted that while progress has been made in accounting for all CBP workstations, a complete and up-to-date listing of all CBP workstations has not been maintained for the majority of FY 2010. As a result, CBP does not have an accurate inventory of which workstations have not received anti-virus and other security patch updates.	We recommend that CBP continue installing [redacted] and develop, implement, and monitor policies and procedures to move all workstations to [redacted] or to obtain waivers and compensating controls for those workstations that cannot be moved to [redacted].		X	2
CBP-IT-10-12	CBP's RBST Program does not meet the DHS requirements for "annual specialized training" that is "commensurate with the individual's duties and responsibilities." Specifically, the CBP RBST program requires IT personnel to complete only one hour of Incident Response training, and one hour of Classified Information training (if applicable to the individual's responsibilities) annually. Furthermore, out of the sampled 45 CBP personnel with significant IT security responsibilities, 5 completed the training after CBP's internal June 30, 2010 deadline. In addition, another eight have yet to complete the training.	We recommend that CBP re-examine its role-based training program and consider implementing the DHS Role-Based Security Training Program once it has been implemented at the department level.	X		2
CBP-IT-10-13	This is a component-level finding. We noted the following weaknesses related to access to the raised floor area: • We reviewed access request authorizations to the raised floor area of [redacted] and noted that of the 45 individuals selected, 1 authorized access form was not provided. • We reviewed evidence of the recertification of	We recommend that management develop tools and procedures for facilitating and documenting the approval/recertification and review of individual access to the raised floor area.	X		2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	individuals with access to the raised floor area and noted that of the 15 selected individuals, 2 had not yet been recertified.				
CBP-IT-10-14	This is a system level finding. KPMG noted that although changes to a user's ACS access profile are logged, the logs of these events are not regularly reviewed by personnel independent from those individuals that made the changes.	We recommend that CBP formalize a detailed procedure for the review of ACS security profile change logs. The procedure should include implementing a periodic review of the logs by an independent reviewer.		X	2
CBP-IT-10-15	During our technical testing, patch and configuration management exceptions were identified on the [redacted]	[redacted]	X		2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	[redacted]				
CBP-IT-10-16	This is a system-level finding and a prior year issue from FY 2008 and FY 2009. KPMG determined that evidence of ISAs for 6 of the 17 PGAs identified in the System Security Plan could not be provided. Of the six that were provided, two expired during FY2010 and had not been renewed.	We recommend that CBP devote sufficient resources in order to implement and maintain formal ISAs with the PGAs that interconnect with ACS. We recommend that CBP document ISAs for all ACS PGA connections identified in the ACS SSP.		X	2
CBP-IT-10-17	This is a system-level finding. We requested access authorization evidence for 45 ACS users to determine whether ACS access was appropriately authorized. OIT was unable to provide evidence of the access request authorizations for any of the 45 selected ACS users. As a result, we are not able to determine whether ACS access initiations or modifications were appropriately approved and whether ACS access controls are in place and operating as required by DHS and CBP policies.	We recommend that CBP implement procedures to consistently document the access requests and approvals for any and all access creations and changes to ACS user profiles.		X	2
CBP-IT-10-18	This is a component level finding. We noted that access request forms, or evidence of recertification of access, to the offsite media could not be provided for 5 of the 15 selected employees.	We recommend that CBP update the access authorization process to indicate that the access list will undergo a 100% recertification annually. The artifact should be an official report from the Contracting Officer Technical Representative for offsite media storage clearly stating the results along with backup paperwork for all add, deletes, and changes to the access list.	X		1
CBP-IT-10-19	This is a system level finding. We were informed that ACS Security Audit Logs are not being reviewed. Additionally, we noted that the following weaknesses related to the ACS Security Audit Logs procedures continue to exist: • Procedures do not define how often the ACS	We recommend that CBP develop and implement procedures that document the review process for ACS profile change logs. The process should include the documented evidence of review, how often audit logs are reviewed, and the review sampling methodology.		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	security profile change audit logs are reviewed. • Procedures do not describe how the documented evidence of the review process is created by the ACS Information System Security Officer (ISSO)/Independent Reviewer. • Procedures do not define the sampling methodology that is used to select ACS profile change security logs for review				
CBP-IT-10-20	This is a system-level finding. We noted the following weaknesses related to the [redacted]e configuration settings: • KPMG noted that users were allowed an [redacted] number of failed attempts to access datasets to which they were not authorized. KPMG determined that the control option in the security software, which results in immediate suspension of any user who exceeds the specified number of violations, had not been configured properly. KPMG noted that this setting was corrected on February 24, 2010. • KPMG noted that users were allowed [redacted] failed logon attempts before their accounts were locked. At the end of the fiscal year the setting was updated to three failed login attempts, and KPMG observed the setting in the system and noted that it was corrected on September 24, 2010.	As the conditions were closed during testing, no recommendation is required.		X	2
CBP-IT-10-21	This is a component level finding. We noted the following weaknesses related to the CBP Background Investigation process: • Of the 45 individuals selected, we noted that 1 contractor did not have a completed background investigation as required by the CBP Information System Security Policies and Procedures	We recommend that CBP: • Complete via e-QIP the "initiation" of all remaining employee reinvestigations by December 30, 2010. • Complete the reinvestigations for all such employees by December 30, 2011. • Develop/deploy a tracking mechanism (Contractor Tracking System) by which to identify those contractors		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Handbook. We noted that this contract has access to the Automated Commercial Environment (ACE) system. • Of the 45 individuals selected, we noted that 5 employees and 25 contractors did not have their background reinvestigations initiated within the five year timeframe as required by CBP Memorandum Regarding Reinvestigations, dated August 18, 2008.	requiring reinvestigation. • Develop and implement a strategy to ensure that reinvestigations for all contractors are initiated as required.			
CBP-IT-10-22	This is a system-level finding. ACS developers may gain emergency/temporary access to the production environment through the portal request process. While the emergency/temporary account activities are logged, CBP does not review these activity logs to identify inappropriate activities.	KPMG recommends that CBP reports on the TSS audit of emergency access should be run as needed at management's (e.g., emergency approver's) request.	X		2
CBP-IT-10-23	This is a system-level finding. Access approvals prior to the creation of NDC-LAN accounts were not consistently maintained in accordance with CBP policy and procedures. KPMG requested access authorization documentation for 25 individuals who were granted NDC-LAN access during FY 2010. Although a process for creating and maintaining user access forms and requests has been in place since before the beginning of FY 2010, initial access requests and approvals for 10 of these individuals were not provided.	We recommend that CBP fully transition their process for requesting NDC-LAN Network access from the paper-based user access request form to an electronic user access request form. Once the electronic form is fully implemented, the documented process will be updated to reflect that all NDC-LAN user access requests must go to the Technology Service Desk (TSD) for action. TSD will generate a trouble ticket and attach the electronic access request form to the initial user request ticket for NDC-LAN access. The ticket will be issued in the name of the user gaining the access so it is easily searchable. TSD is currently in the development phase for a new user account request portal which will provide a secure online environment for managing this process. This new tool will allow requestors the ability to complete and submit LAN and eMail account requests via online web form. Once the request is reviewed and approved by the CBP supervisor, a	X		2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		ticket will be automatically generated (bypassing the need of saving/attaching and emailing the TSD) and routed to the appropriate group for processing. A log will be captured and saved in the new system for each approved/denied request for future reference.			
CBP-IT-10-24	CBP has not corrected functionality issues currently noted in ACS, and routine maintenance is increasingly difficult and expensive. Currently, only two vendors support ACS, which limits CBP's ability to obtain maintenance services at a reasonable cost. During FY 2010, CBP spent nearly $12.1 million just to maintain ACS at its current level of functionality. In addition, CBP is currently re-visiting the amount of funding necessary to complete the implementation of the ACE financial modules and will complete this analysis in FY 2011. Due to these conditions regarding the functionality of ACS and delayed implementation of ACE, CBP has not resolved the following known ACS functionality issues: • ACS lacks the controls necessary to prevent, or detect and correct excessive drawback claims. The programming logic in ACS does not link drawback claims to imports at a detailed, line item level. In addition, ACS does not have the capability to compare, verify, and track essential information on drawback claims to the related underlying consumption entries and export documentation upon which the drawback claim is based. Export information is not linked to the Drawback module and therefore electronic comparisons of export data cannot be performed within ACS. See NFR CBP-10-20 for further details.	To address this finding, CBP recommends that it continue to: • Modernize its business processes though the development and deployment of functionality in the Automated Commercial Environment as it has done since 2001. • Work with [redacted] stakeholders, including CBP personnel, the trade, participating government agencies, the Department of Homeland Security and the Congress to prioritize, develop, and deploy functionality that allows CBP to fulfill its mission and meet the needs of its stakeholders. • Seek funds through the budget process that will allow CBP to continue to develop and deploy functionality in [redacted] that will support CBP's mission and meet the needs of its stakeholders.	X		2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• Certain monitoring reports used to monitor (review) importer compliance with the in-bond process have not been developed and therefore importer compliance is not being tracked. In addition, in-bonds are not automatically linked to the relevant entry or export filings in ACS, which leads to extensive manual work to close open in-bonds. Finally, ACS does not provide the ability to run oversight reports to determine if ports have completed all required in-bond post audits and exams. See NFR CBP-10-14 for further details. • ACS does not properly account for bond sufficiency of claims that involve a continuous bond and therefore a claimant can potentially claim and receive an accelerated payment that exceeds the bond amount on file. As a result, CBP will not have sufficient surety against a drawback over claiming. See NFR CBP-10-05 for further details. • ACS does not provide summary information of the total unpaid assessments for duties, taxes, and fees by individual importer (i.e., a sub-ledger) and cannot provide reporting information on outstanding receivables, the age of receivables, or other data necessary for management to effectively monitor collection actions. See NFR CBP-10-04 for further details. • The drawback selectivity function of ACS is not programmed to select a statistically valid sample of prior drawback claims against a selected import entry. See NFR CBP-10-03 for further details. • ACS is programmed to automatically indicate that a Port Director certified a refund or drawback payment even if the Port Director does not certify a given payment. See NFR CBP-10-19 for further details.				

Department of Homeland Security
Information Technology Management Letter
September 30, 2010

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating

Department of Homeland Security
FY 2010 Information Technology - Notice of Findings and Recommendations – Detail

Federal Emergency Management Agency

Department of Homeland Security
Information Technology Management Letter
September 30, 2010

Notice of Findings and Recommendations – Detail
Federal Emergency Management Agency

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-10-01	During FY 2010, FEMA finalized and documented requirements, and initiated automated technical processes and controls related to the NEMIS Access Control System (NACS) Position Re-Approval Project (NPRP). Specifically, Enterprise Operations Branch personnel have begun systematically expiring position assignments and requiring supervisor reauthorization of a subset of NACS accounts and related positions progressively over a 180 day period. Due to the volume of active positions, FEMA management stated that the recertification process will recertify all NACS positions after the 180 days and is anticipated to be completed in FY 2011. Thus, while we noted that improvements were made by developing and implementing an automated process for recertifying all NACS accounts and related positions, including those related to NEMIS access, initial recertification to review and revalidate all NACS accounts and positions has still not been completed.	• Complete the initial recertification of all existing NACS accounts and related positions initiated in April 2010 to ensure that all active NEMIS accounts and their associated privileges are appropriately authorized; and • Ensure that all NACS accounts and related positions are recertified by the user's appropriate supervisor no less than annually, in accordance with DHS policy.		X	3
FEMA-IT-10-02	FEMA has not established an alternate processing site for NEMIS. Additionally, an exception to DHS policy for the lack of an established alternate processing site as required systems such as NEMIS that are categorized as "high impact" for availability has not been requested by FEMA.	• Continue and complete efforts required to establish and implement an alternate processing site for NEMIS according to DHS 4300A. • Until an alternate processing site is established, develop and submit an exception for approval in accordance with DHS policy, and ensure that compensating controls over the alternate processing site have been implemented and are effective, and documentation of their effectiveness is maintained as auditable records.		X	3
FEMA-IT-10-03	The FEMA domain security policy is configured to enforce activation of a password-protected screensaver on end-user workstations after 15 minutes of inactivity,	• Configure the FEMA LAN domain security policy to automatically activate a password-protected		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	rather than the five minute inactivity threshold required by DHS policy.	screensaver on end-user workstations after five minutes of inactivity, consistent with DHS policy. • Implement appropriate management controls to ensure timely communication and implementation of existing and future DHS information security policy requirements pertaining to the configuration of FEMA end user workstations, and to periodically assess system controls to determine compliance.			
FEMA-IT-10-04	As noted during our FY 2009 audit procedures, weaknesses exist in processes related to logging, monitoring, and retaining audit logs on system software and operating systems supporting NEMIS. Specifically, policies and procedures related to the monitoring of activity on system software and operating systems supporting NEMIS have not been revised to include all identified operating systems and IT components that comprise the system boundary for the NEMIS application. Additionally, controls have not been configured and appropriately implemented to log, monitor, or retain sufficiently detailed audit logs for activity on NEMIS operating systems and servers.	• Revise the SOP, *Monitoring Sensitive Access to NEMIS*, to ensure that it states that the scope of the procedures includes operating systems on all servers within system boundaries as defined in up-to-date NEMIS system documentation. • Acquire and deploy appropriate tools on operating systems and servers supporting NEMIS to generate audit trails and records in accordance with FEMA and DHS policy. • Implement the SOP, *Monitoring Sensitive Access to NEMIS*, by reviewing and retaining audit trails and records in accordance with FEMA and DHS policy.		X	3
FEMA-IT-10-05	As identified during the FY 2009 audit, PARS database security controls are not appropriately established as noted below: • PARS database accounts are not reviewed to identify accounts that have been inactive for 45 days or more, as required by DHS policy for high impact systems. • Strong passwords and authenticator controls are not implemented for PARS database accounts in accordance with FEMA and DHS policy.	• Document and implement a formal process to implement appropriate controls to ensure that inactive PARS database accounts are disabled in accordance with DHS policy. • Configure PARS database accounts in accordance with DHS and FEMA requirements for passwords and authenticator controls, including expiration, reuse, and complexity. • Document and implement system-specific processes for generating and performing reviews of PARS database audit logs and retaining auditable		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Specifically: - A minimum password length is not set; - Password complexity is not enforced to require passwords that include a combination of upper/lowercase letters, numbers, and special characters or to restrict the use of dictionary words as passwords; - Reuse of previous passwords is not prohibited; - Passwords are not configured to expire or be changed after a pre-determined length of time; and - Accounts are not configured to disable after a pre-determined number of consecutive invalid login attempts. • System-specific policies and procedures have not been developed for the PARS Oracle database, and existing policies and procedures inherited from the IFMIS application operating environment do not adequately describe implementation of FEMA policies for the generation, review, and retention of all required auditable events. • Database audit logs are not configured to capture auditable events, including failed login attempts and administrator-level actions, as required by FEMA and DHS policy. • Although a periodic recertification of PARS database access accounts is performed to ensure that access is still necessary and appropriate for each individual, policies and procedures over the management of accounts on the PARS Oracle database do not specify requirements for performing a periodic recertification of database	evidence of review in accordance with FEMA and DHS policy. Additionally, ensure that all DHS requirements are met through this process, including appropriate supervisory review and segregation of duties principles. • Configure PARS database audit logs to capture and retain auditable events in accordance with FEMA and DHS policy. • Further define and establish a formal process for granting initial access and recertifying access specifically to the PARS database that includes appropriate approval from FEMA management and requirements for temporary and emergency access, in accordance with DHS guidance. Please see NFR FEMA-IT-10-48 for recommendations related to the periodic review and assessment of security controls in place to ensure that corrective actions are appropriately implemented over identified security weaknesses.			

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	accounts to validate the continued appropriateness of access. Additionally, the FY 2010 recertification of PARS Oracle database user accounts was not completed consistently and in accordance with FEMA requirements. Specifically, of a selection of recertification forms for five PARS database user accounts requested, four forms recertified access for contractors without documented COTR approval. • Authorization of initial access for the PARS database is not consistently completed in accordance with FEMA and DHS policy. Specifically, of a selection of three PARS database access forms requested: - Two user accounts were granted to contractors without the required COTR signature. - One account was identified by Financial Systems Section (FSS) personnel as an IFMIS system account. However, no documentation justifying or authorizing the use of this system account was provided.				
FEMA-IT-10-06	During the FY 2010 financial statement audit, we noted that FEMA has made improvements over the management of NEMIS Oracle database password controls for IT Operations database administrator accounts, specifically by configuring a 104-day password lifetime. However, the following weaknesses noted in FY 2009 continue to exist in FY 2010 for the four databases selected for testing: • A password complexity verification function is not configured to require a combination of upper/lowercase letters, numbers, and special	We recommend that FEMA configure all NEMIS Oracle databases to ensure compliance with effective DHS and FEMA policy requirements for passwords and authenticator control requirements, including expiration, reuse, and length and complexity.		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	characters. • Reuse of previous passwords is not prohibited. • No minimum password length is enforced.				
FEMA-IT-10-07	FEMA has made improvements over the management of IFMIS-Merged Oracle database passwords by configuring the system to retain a history of the previous ten passwords. However, upon inspection of additional database password parameters, we determined that the password history for the ten previous passwords is only retained for 30 days. Therefore, after the 30 day timeframe, the password history is erased, allowing the user to potentially use one of the previous ten passwords.	We recommend that FEMA configure the IFMIS-Merged Oracle database to ensure compliance with effective DHS and FEMA policy requirements regarding the reuse of user passwords.		X	3
FEMA-IT-10-08	During the FY 2010 financial statement audit, we selected four NEMIS Oracle databases for testing and noted that each is configured to lock accounts after three consecutive failed login attempts and to remain locked for 415 seconds (7.5 minutes) before being unlocked.	Configure all NEMIS Oracle databases to ensure compliance with effective DHS and FEMA policy requirements for account lockouts due to failed login attempts.	X		3
FEMA-IT-10-09	As noted during the FY 2009 audit, the following weaknesses over audit logging controls for the NEMIS Oracle databases continue to exist in FY 2010: • The FEMA IT Operations Branch *Standard Operating Procedure (SOP) for Handling of Oracle Audit Logs* has not been updated. Specifically: - The scope section of the SOP does not list all Oracle databases identified that comprise the NEMIS data processing environment. - The SOP has not been updated to address all DHS policy requirements surrounding audit	• Revise the *SOP for Handling of Oracle Audit Logs* to ensure that procedures over requirements for logging and monitoring auditable activities on all NEMIS databases are documented in accordance with DHS and FEMA guidance and the process for audit log review is appropriately implemented for all databases within the NEMIS system boundary. • Implement database configurations on all NEMIS databases in accordance with DHS and FEMA policy and procedures over required auditable events and activities. • Dedicate the appropriate resources and implement the appropriate automated tools or establish manual processes to collect, review, and retain		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	trails and activity monitoring. Specifically, successful logins, access modifications, highly privileged user account activity, and changes to user profiles are not required to be logged and reviewed. - The SOP specifies that database administrators will review Oracle audit records, which is a violation of segregation of duties principles that require an independent review of system activity. • On the four NEMIS databases selected for testing, configurations are not fully enabled so that a review of audit trails and activity defined by DHS policy requirements can be completed. Specifically, only failed login attempts are recorded in the audit trails of all database user accounts.	auditable activities on all NEMIS databases, to ensure compliance with DHS and FEMA policy.			
FEMA-IT-10-10	As noted during the FY 2009 audit, we determined that weaknesses over the tracking of FEMA contractors continue to exist in FY 2010. Specifically: • FEMA does not have a formal process for centrally and adequately tracking FEMA contractors throughout the on-boarding, termination, and transfer processes. As a result, FEMA could not provide a complete listing of all contractors working for FEMA. • The process established for notifying FEMA Office of Chief Information Officer (OCIO) management, including IT system administrators, of changes in contractor's status, so that accounts can be disabled/removed or account profiles can be appropriately modified in the required timeframe,	• Develop, document, fully implement, and communicate formal policies and procedures, according to DHS guidelines and requirements, for centrally tracking all contractors throughout the on-boarding, termination, and transfer processes. Ensure policies and procedures include: • The assignment of roles and responsibilities to appropriate FEMA management and stakeholders. • Procedures to ensure that COTRs notify the FEMA OCIO of changes in contractors' status, including separation or transfer, so that accounts can be disabled/removed or account profiles can be appropriately modified in the required timeframe. • Establishment of controls for periodically		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	is not effective or comprehensive. Specifically, no formal requirements exist for Contracting Officer's Technical Representatives (COTRs) to notify the OCIO of separating contractors.	monitoring the effectiveness of the process to ensure compliance with policy. • Regularly distribute a listing of terminated contractor personnel to information system administrators so they can remove user access timely.			
FEMA-IT-10-11	While FEMA has made improvements over the review of IFMIS-Merger application activity by documenting responsibilities for performing periodic reviews of super user account activities, the following weaknesses noted in FY 2009 continue to exist in FY 2010: • Existing policies and procedures, including FEMA Interim CFO Directive 2600-21, *IFMIS User Access and Termination*, and FEMA SOP 2000-002, *Monitoring of IFMIS Database Audit Log*, do not require the generation, review, or retention of audit logs for all activities required by FEMA and DHS policy. • Failed database (Oracle) and application (UNIX) login attempts and activity performed by application users with the "super user" role remain the only forms of activity logged and monitored for IFMIS-Merger. Other types of activity required by FEMA and DHS policy, including successful logins, access modifications, and changes to user profiles, are not logged or monitored. • While we noted that logging of users accessing or attempting to access the IFMIS-Merger application is enabled and distributed to appropriate independent reviewers, evidence of review of application login attempts is not documented. Additionally, we noted the following weaknesses related to reviews of activity of super users within the	• Revise and implement policies and procedures that document requirements for configuring, retaining, and reviewing audit trails for the IFMIS-Merger application and database, including defined roles and responsibilities, in accordance with DHS and FEMA policy. • Implement configurations on the IFMIS-Merger application and database to ensure that audit logs record required auditable events and activities, in accordance with DHS and FEMA policy. • Implement appropriate management controls to ensure timely communication and implementation of existing and future DHS information security policy requirements pertaining to the configuration of audit logs on the IFMIS-Merger application and database, and to periodically assess system controls to determine compliance.		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	IFMIS-Merger application: • Activity of users with elevated privileges is logged and reviewed on a weekly basis. However, FEMA policy requires that audit records be captured and reviewed at least every three days. • Review of super user activity is performed by an individual with super user privileges within the application, in conflict with segregation of duties principles.				

FEMA-IT-10-12	The following weaknesses noted in FY 2009 continued to exist in FY 2010:
	• G&T IFMIS application user accounts were not consistently approved or authorized prior to initial account creation or modification of account privileges. Of the 25 active application users selected for testing, FEMA was unable to provide adequate documented evidence that creation of, or modifications to, account privileges for 22 accounts were properly authorized. Specifically:
	  • Documentation for 10 accounts did not evidence that access was authorized by the Office of the Chief Financial Officer (OCFO).
	  • Documentation for 11 accounts indicated that access was authorized by the OCFO after the modifications to the account privileges were performed.
	  • Documentation for one account was not available.
	• G&T IFMIS Oracle database user accounts were not consistently approved or authorized prior to initial account creation. Specifically, of the eight
		There is no recommended corrective action specific to this finding because of the decommissioning of G&T IFMIS in June 2010. Any G&T IFMIS accounts which now exist on the IFMIS – Merged instance will need to be included in recertification efforts that will be performed by FEMA as corrective action to remediate NFR FEMA-IT-10-14, which cites a lack of consistent recertification of Core/Merged IFMIS accounts, to ensure that all migrated G&T IFMIS accounts are appropriately authorized.		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	active database user accounts selected for testing, FEMA was unable to provide documented evidence that the initial account creation of two accounts in FY 2010 was authorized. While KPMG noted that the planned merger of the G&T IFMIS and Core IFMIS instances occurred in February 2010, and the existing G&T IFMIS Oracle database and application server was decommissioned in June 2010, the weaknesses over the financial data existed for the majority of the fiscal year.				
FEMA-IT-10-13	As noted during the FY 2009 audit, weaknesses in G&T IFMIS Oracle database audit logging controls continued to exist in FY 2010. Specifically, Oracle database audit trails were not configured to capture any activity, including failed login attempts or administrator-level actions as required by FEMA and DHS guidance. While we noted that the planned merger of the G&T IFMIS and Core IFMIS instances occurred in February 2010 and the existing G&T IFMIS Oracle database was decommissioned in June 2010, the weaknesses over the financial data existed for the majority of the fiscal year.	There is no recommended corrective action specific to this finding because of the decommissioning of G&T IFMIS in June 2010.		X	3
FEMA-IT-10-14	During the FY 2010 audit procedures, we noted that weaknesses which existed in FY 2009 related to the recertification of IFMIS application accounts continue to exist. Specifically, although the Core IFMIS application user accounts were recertified in January 2010 prior to the merge of the G&T and Core IFMIS applications, we determined that the recertification of the Core IFMIS accounts was not properly completed. Of the 25 active application accounts selected, FEMA was unable to provide documented evidence that three of the accounts were recertified by the system owner to	• Dedicate resources to fully implement FEMA and DHS requirements for a recertification of all IFMIS-Merger application accounts at least annually, including revoking access for any accounts not currently in compliance with the annual recertification. • Identify and implement appropriate monitoring controls to ensure continued compliance with recertification requirements for the IFMIS-Merger application.		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	validate the continued appropriateness of the account, as required by FEMA and DHS policy. Furthermore, these accounts then remained on the IFMIS-Merger application after the merger of the applications occurred.				
FEMA-IT-10-15	During the FY 2010 audit, we noted that the weaknesses over the recertification of G&T IFMIS application and Oracle database users noted in FY 2009 continued to exist. Specifically, a management review to validate the appropriateness of G&T IFMIS application and Oracle database user accounts was not formally implemented or performed by the Office of the Chief Financial Officer/Financial System Section (OCFO-FSS) this fiscal year. We noted that the planned merger of the G&T IFMIS and Core IFMIS instances occurred in February 2010, and the existing G&T IFMIS Oracle database and application server was decommissioned in June 2010. However, prior to the migration of G&T accounts to the IFMIS – Merged instance in February 2010, a recertification of G&T IFMIS application users did not occur. Therefore, the weaknesses over the recertification of users with access to G&T IFMIS financial data existed for the first two quarters of the fiscal year.	There is no recommended corrective action specific to this finding because of the decommissioning of G&T IFMIS in June 2010. Any G&T IFMIS accounts which now exist on the IFMIS – Merged instance will be included in recertification efforts that need to be performed by FEMA as corrective action to remediate NFR FEMA-IT-10-14, which cites a lack of consistent recertification of Core/Merged IFMIS accounts.		X	3
FEMA-IT-10-16	The merger of Core IFMIS and G&T IFMIS was performed in February 2010, and the G&T IFMIS application and database server were formally decommissioned in June 2010. While an ATO was granted for the IFMIS-Merger system by the FEMA Chief Information Officer on June 4, 2010, prior to the completion of the merged instance, a C&A had not been performed over the G&T IFMIS instance. Consequently, as noted during the prior year FY 2009 audit, G&T IFMIS operated without an ATO prior to its decommissioning. In addition, we determined that during the time the system was operational, neither an	There is no recommended corrective action specific to this finding because of the decommissioning of G&T IFMIS in June 2010.		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Information System Security Officer (ISSO) nor a Designated Authorizing Authority (DAA) had been formally designated by FEMA management for G&T IFMIS.				
FEMA-IT-10-17	During the FY 2010 integrated audit, we noted the following weaknesses regarding specialized training for FEMA employees and contractors with significant information security responsibilities: • FEMA has not formally documented or implemented policies and procedures to meet the requirements over specialized training for FEMA employees and contractors with significant information security responsibilities in accordance with DHS policy. • With the exception of ISSOs, FEMA has not formally identified all individuals or positions with significant information security responsibilities subject to specialized training requirements. • FEMA does not track or monitor completion of specialized training for FEMA personnel with critical IT roles.	• Develop and implement policies and procedures requiring initial and periodic specialized training for individuals with significant information security responsibilities. • Formally identify specific roles and positions possessing significant information security responsibilities that are subject to specialized training requirements. • Develop and implement a mechanism for tracking and monitoring compliance with specialized training requirements for individuals with significant information security responsibilities.	X		2
FEMA-IT-10-18	In FY 2010, we noted that the NEMIS SSP was updated in November 2009. However, we determined that the following weaknesses continue to exist: • NEMIS system boundaries, including identification of all hardware and software elements that comprise the NEMIS general support system and subsystems, have not been fully defined. • FEMA has not documented the assignment of FEMA personnel with security responsibilities for the modules and major applications that are	• Fully identify all hardware and software components of the NEMIS platform and update appropriate NEMIS system documentation, including the SSP, to reflect the current operating environment as required by DHS policy and NIST guidance. • Establish and implement a formal process for periodically reviewing and assessing system documentation to ensure that system boundaries and hardware and software components are accurately reflected.		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	classified as NEMIS subsystems within the current NEMIS SSP.	• Formally assign and document security responsibilities of FEMA personnel for all components of NEMIS, including all identified modules and major applications.			
FEMA-IT-10-19	During the FY 2010 integrated audit, we noted the following weaknesses regarding configuration management over network devices such as firewalls, routers, and switches that support in-scope financial systems: • Comprehensive configuration baselines identifying all relevant configuration items (CIs) within the scope of IFMIS and NEMIS have not been documented. • FEMA configuration management (CM) policies and procedures require the implementation of Configuration Status Accounting (CSA), which includes recording approved configuration documentation, performing Configuration Audit (CA), and documenting physical configuration audits to assess conformance with established baselines. However, requirements for the frequency, documentation, and retention of results of these activities have not been defined in existing FEMA policies or procedures. Additionally, the required CSA reports and CAs have not been performed for IFMIS or NEMIS.	• Formally establish roles and responsibilities related to oversight and implementation of configuration management policies and procedures for network devices, including firewalls and routers, supporting financial applications in accordance with DHS and FEMA requirements. • Revise and implement configuration management policies and procedures over documenting and maintaining current baseline configurations for network devices supporting financial applications, including IFMIS and NEMIS, to ensure DHS and FEMA requirements are adequately addressed and configuration baselines are comprehensively documented by FEMA. Additionally, policies and procedures should include guidance over requirements such as documentation of baselines, periodic review and auditing, and approval of baseline changes for network devices. • Perform required configuration management activities, including periodic Configuration Status Accounting and Configuration Audit activities, for network devices supporting financial applications, including IFMIS and NEMIS, and retain auditable evidence of these activities as required by FEMA policy.	X		3
FEMA-IT-10-20	Conditions noted in FY 2009 related to weaknesses over the documentation and testing of the NEMIS contingency plan continue to exist in FY 2010, as follows:	• Update the NEMIS IT Contingency Plan in accordance with DHS and NIST requirements for systems categorized at the high impact availability objective. Additionally, ensure that the Contingency Plan comprehensively addresses the		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating

	• The NEMIS IT Contingency Plan does not adequately and comprehensively include information required by DHS policy for systems with high impact availability. For example, we noted the following weaknesses:
	  • Detailed information over NEMIS system architecture, such as the database and server names, as well as information over the various modules of NEMIS, has not been appropriately documented to reflect the current operating environment.
	  • The plan does not sufficiently include details necessary to fully restore NEMIS and dependent subsystems in the event of an emergency.
	  • The contingency plan does not specify critical roles, system resources, or system/application recovery priorities in sufficient detail to distinguish between the various modules within NEMIS.
	  • The Business Impact Analysis (BIA) included in the Contingency Plan was completed in 2004 and is not adequately documented.
	• Testing of the NEMIS IT contingency plan has not been performed in the past 12 months in accordance with DHS policy.
		numerous sub-systems within NEMIS so that detailed information exists over the current system architecture, critical processing priorities, detailed recovery procedures and other required components in accordance with DHS guidance.
		• Conduct and document annual tests of the NEMIS Contingency Plan that address all critical phases of the plan, and update the Contingency Plan with lessons learned, as necessary and in accordance with DHS and NIST requirements.			

FEMA-IT-10-21	We performed a comparison of active IFMIS-Merger, G&T IFMIS, and NEMIS Access Control System (NACS) accounts, as well as individuals with Virtual Private Network (VPN) remote access privileges, against a list of FEMA employees that had separated from employment since October 1, 2009 to determine	• Identify the root cause(s) associated with separated employees remaining on FEMA information systems. As appropriate, revise existing procedures or develop additional procedures over removal of separated user access to IT systems to address weaknesses that contribute to untimely		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	if any separated employees retained active accounts on the applications or remote access to the FEMA network. The following weaknesses were identified: • 11 IFMIS-Merger user accounts remained active and unlocked after the account holder's separation from FEMA. • 3 G&T IFMIS user accounts remained active and unlocked after the account holder's separation from FEMA. • 164 NACS accounts with NEMIS positions assigned at the time of our test work remained active and unlocked after the account holder's separation from FEMA. • 33 individuals retained the ability to access the FEMA network remotely due to active VPN remote access privileges after the account holder's separation from FEMA. All 33 individuals additionally retained an active NACS account as described above, thus allowing them to potentially access NEMIS as well.	removal of separated individuals from the systems. • Ensure that procedures are implemented consistently to remove system and application accounts for all separated users immediately upon notification of separation, in accordance with FEMA, DHS and NIST guidance. No corrective action specific to the portion of this finding related to G&T IFMIS will be provided because of the decommissioning of that system in June 2010.			

FEMA-IT-10-22	In FY 2010, we noted that the following conditions identified in FY 2009 related to FEMA LAN accounts continue to exist:
	• The FEMA LAN domain security policy does not enforce password requirements in accordance with DHS policy. Specifically:
	  • The FEMA LAN does not enforce a password history or prevent reuse of passwords.
	  • The FEMA LAN does not enforce complexity requirements, including password length or the use of mixed-case alphanumeric and special
		Configure the FEMA LAN to ensure compliance with DHS and FEMA policy requirements for passwords and authenticator control requirements, including expiration, reuse, and length and complexity.
		Identify and implement appropriate monitoring controls to ensure that all accounts on the FEMA LAN are in compliance with DHS requirements for authorization. Additionally, ensure that where appropriate policies and procedures are further developed and/or revised to ensure consistent implementation and include requirements for all accounts on the FEMA LAN, including generic, shared
				X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating

	characters, to ensure that strong passwords are used.
	• FEMA was unable to provide evidence of account authorization for 10 Active Directory (AD) individual user accounts created in FY 2010.
	• While policies and procedures over the authorization of generic, shared group, and service accounts on the FEMA LAN have been finalized, approval of these accounts is not consistently documented according to policy. Specifically, of a selection of 45 generic, group, and service LAN accounts created during FY 2010:
	  • 2 did not have a clearly defined business need or justification documented;
	  • 26 did not have IT Security or system owner approval documented;
	  • 19 were created prior to supervisory certification; and
	  • 2 did not have any authorizing documentation provided for our review.
	• FEMA has not established procedures and implemented a process over the periodic recertification of FEMA LAN accounts to ensure that access is still necessary and appropriate for each account as required by FEMA and DHS policy.
	• We compared a listing of active FEMA LAN/AD accounts against a list of FEMA employee separations that had occurred since October 1, 2009 and determined that 85 accounts remained active and unlocked after the account holder's
		group, service, and LAN end-user accounts not included in the NACS.
		Develop and implement a formal process for performing a periodic recertification of all FEMA LAN accounts which defines requirements and addresses accounts not included during the planned recertification of NEMIS application access.
		Evaluate and, if appropriate, revise existing procedures over removal of separated user access to the FEMA LAN to ensure the timely removal of separated individuals from the network.
		Ensure that procedures are implemented consistently to remove FEMA LAN accounts for all separated users immediately upon notification of separation, in accordance with FEMA, DHS and NIST guidance.			

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	separation from FEMA.				
FEMA-IT-10-23	In FY 2010, we determined that while change management procedures have been developed and implemented for applications hosted by the NFIP LAN, including Traverse, the documented procedures do not specifically address patch management policies and procedures for the NFIP LAN in accordance with DHS requirements. Specifically, controls over the approval, testing, and deployment of operating system patches are not addressed.	We recommend that FEMA OCIO and NFIP management finalize and implement comprehensive patch management policies and procedures for the NFIP LAN supporting Traverse, in accordance with DHS policy. Additionally, FEMA and NFIP management should ensure that these procedures include requirements for authorizing, testing, and approving patches to be implemented into production and responding to DHS Security Operations Center and DHS EOC notifications to ensure compliance with the timely implementation of required patches.		X	2
FEMA-IT-10-24	During FY 2010, we noted that weaknesses over the Certification and Accreditation (C&A) of NFIP continue to exist. Specifically, • FEMA approved Conditional ATOs for the NFIP/LSS on May 22, 2009 and August 20, 2010 for two one-year periods. However, we noted that in the absence of a full ATO, DHS policy allows "interim" ATOs only for systems that are either under development testing or in the prototype phase of development, not operational systems such as the NFIP/LSS. Additionally, "interim" ATOs cannot exceed two consecutive six-month periods. • During the initial Conditional ATO period that began on May 22, 2009, FEMA did not complete C&A efforts, including the risk assessment and security testing and evaluation (ST&E) needed to fully assess risk associated with the system, so that a full ATO could be issued. Consequently, from May 2010, when the initial Conditional ATO expired, through August 2010 when the second Conditional ATO was approved, the system	We recommend that NFIP continue to work with the FEMA OCIO to complete the recertification and accreditation of the NFIP Legacy Services System (LSS), including documentation of all required artifacts in accordance with applicable DHS policies and Federal guidance.		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	operated without any authorization. • During our integrated audit fieldwork period, NFIP was unable to provide us with evidence that C&A activities required to be performed for a full ATO to be granted had been completed.				
FEMA-IT-10-25	During the FY 2010 FEMA Integrated Audit, we noted that the following conditions related to management of FEMA VPN accounts continue to exist: • The VPN Rules of Behavior for Users Behind Corporate Firewalls, dated December 5, 2002, requires individual's manager approval and Enterprise Service Desk (ESD) validation of all VPN Access Request forms prior to granting access. However, approval by the system owner or a designated representative is not required. • VPN Access Request forms include an approval block titled "For FEMA OCS Use Only," and the form states that all VPN requests must be approved by the FEMA Office of Cyber Security (OCS). However, OCS does not currently exist as a FEMA Division due to FEMA's reorganization. Consequently, existing policies and procedures do not reflect the current security management structure at FEMA nor do they assign responsibility to a current entity within the agency. • A periodic recertification of FEMA VPN access accounts is not currently performed to ensure that remote access is still necessary and appropriate for each individual. • Of the selection of 45 VPN Access Request forms reviewed: • Two did not specify the date that access was	• Revise and implement current policies and procedures for documenting, reviewing, and approving all remote access accounts to the FEMA LAN including VPN and iPass access. Specifically, roles and responsibilities should be defined to ensure that sufficient resources are dedicated to appropriately authorize accounts on behalf of the system owner or a designee prior to granting remote access, according to FEMA and DHS policy. • Develop and implement policies and procedures to perform a periodic recertification of all remote user access and retain auditable records as evidence that recertifications are conducted and completed in accordance with DHS and FEMA policy.		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	approved by the requestor's supervisor. • Three were granted supervisory approval after VPN access was established for the user. • The section of each form that required "OCS" level review and approval was not completed. Additionally, we conducted further testwork over remote access granted through the iPass utility, which is used to provide dial-up access to the FEMA network via the VPN gateway. This access is managed through a separate access authorization process from VPN. During our testwork, we noted the following new conditions in FY 2010 related to management of access to iPass: • While iPass User Agreement forms require Section Chief (or equivalent) approval and IT certification for iPass remote access, requests are not approved by the system owner or a designated representative, as required by DHS policy. Additionally, policies and procedures do not exist related to the granting and management of users of the iPass remote dial-up utility. • Of the selection of 45 iPass User Agreement forms reviewed: • Three did not specify the date that access was approved by the requestor's section chief (or equivalent). • One was granted supervisory approval after VPN access was established for the user. • One was granted supervisory approval by the same individual that the requested VPN account was for, indicating a violation of				

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	segregation of duties in the management review and approval of information system access.				
FEMA-IT-10-26	The following weaknesses noted in FY 2009 continue to exist in FY 2010: • IFMIS-Merger application user accounts were not properly approved or authorized. Specifically, of the 25 active application users selected for review, FEMA was unable to provide documented evidence that initial account creation or the most recent modifications to account privileges for 6 accounts were authorized. • Policies and procedures over the management of accounts on the IFMIS-Merger Oracle database do not specify requirements for performing a periodic recertification of database accounts to validate the continued appropriateness of access. • IFMIS-Merger Oracle database user accounts were not properly approved or authorized. Specifically, of the eight active database users selected for review, approval for six user accounts was not documented prior to creation of the accounts. Approval was not documented for these accounts until after the audit request for documentation was received. • The FY 2010 recertification of IFMIS-Merger Oracle database user accounts was neither completed consistently nor in accordance with FEMA policy. Specifically, we requested a selection of recertification forms for 8 IFMIS-Merger database user accounts and determined that 3 were granted to contractors, but COTR approval	• Identify and implement appropriate monitoring controls to ensure compliance with initial authorization and modification requirements for accounts on the IFMIS-Merger application. • Document policies and procedures over the periodic recertification of all accounts on the IFMIS-Merger database. • Dedicate resources to fully implement FEMA and DHS requirements for a recertification of all IFMIS-Merger database accounts at least annually, including revoking access for any accounts not currently in compliance with the annual recertification. • Identify and implement appropriate monitoring controls to ensure compliance with initial authorization, modification, and periodic recertification requirements for accounts on the IFMIS-Merger database.		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	was not documented.				

FEMA-IT-10-27	As noted during the FY 2009 audit, the following weaknesses in G&T IFMIS Oracle database user account password controls continued to exist in FY 2010:
	• We determined that FEMA performed manual reviews of inactive G&T IFMIS database accounts on a monthly basis to disable accounts which had not been used in the prior 90 days. However, since G&T IFMIS is categorized as a high impact system, reviews are required to disable accounts that have been inactive for 45 days, according to DHS policy.
	• The G&T IFMIS database account security policy did not enforce password requirements in accordance with DHS policy. Specifically:
	  • The database did not enforce a password history or prevent reuse of passwords.
	  • The database did not enforce complexity requirements, including definition of a password verification function to ensure strong passwords are used. Specifically, password length and requirements over the use of mixed-case, alphanumeric and special characters to enforce restrictions over the use of dictionary words, are not defined.
	  • The database did not enforce password expiration after a predetermined length of time.
	• FEMA had not established a formal process for approving emergency and temporary access to the
		There is no recommended corrective action specific to this finding because of the decommissioning of G&T IFMIS in June 2010.		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	G&T IFMIS database that is compliant with DHS requirements. Specifically, emergency and temporary access to the database for individuals with elevated privileges, including access for contractor development personnel, is approved by the Financial Systems Section (FSS) Chief and/or his/her staff, not by the FEMA CISO or a designee, as required by DHS policy. Additionally, a formal process specifically addressing procedures for the granting of temporary access to the database and ensuring that access is removed in a timely manner was not documented within existing IFMIS access control policies and procedures. Furthermore, we determined that through this process the G&T IFMIS Oracle database access was granted to contracted development personnel in order to implement database changes to G&T IFMIS, which continues to conflict with segregation of duties principles. While we noted that the merger of the G&T IFMIS and Core IFMIS instances occurred in February 2010 and the existing G&T IFMIS Oracle database was decommissioned in June 2010, the weaknesses noted existed for the majority of the fiscal year.				
FEMA-IT-10-28	Weaknesses noted in FY 2009 over C&A of the FEMA LAN and subsystems that host in-scope financial applications continue to exist in FY 2010. During our FY 2010 audit, we noted that FEMA has classified regional LANs as subsystems and included them within the defined system boundary of the FEMA Switched Network (FSN)-2. We noted the following weaknesses in the C&A of the FSN-2 General Support System (GSS) that includes the FEMA LANs: • The FSN-2 GSS C&A was not completed in	• Continue to fully identify and decouple all components of the FSN-2 platform, including regional LANs and General Support Systems, which host or support IFMIS and NEMIS, and perform all required Certification & Accreditation activities over each component as required by DHS policy and NIST guidance. • Formally assign and document security responsibilities for all components of the FSN-2 platform, including regional LANs and General Support Systems, which host or support IFMIS		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	compliance with DHS and NIST requirements and has not been updated to accurately reflect the current GSS environment. Specifically: • The authorizing officials and individuals noted as responsible for the security roles for multiple regional LANs and subsystems are not accurately reflected in the SSP included in the C&A package as employees with specified roles no longer work for FEMA in the capacity noted. • While the Maryland National Processing Service Center is identified as a subsystem in the overarching FSN-2 GSS C&A package SSP, C&A activities have not been performed over this subsystem. • DHS policy requires annual testing of IT contingency plans for information systems with a high impact availability categorization, such as the FSN-2 GSS. However, the most recent test of the FSN-2 IT contingency plan was performed and documented during FY 2008. • DHS policy requires that risk assessments be conducted for information systems no less frequently than every three years. However, the most recent ST&E was documented during FY 2006. • The most recent ATO granted by the FEMA CIO expired on January 22, 2010, and the FSN-2 GSS is currently operating without authorization from FEMA management. • Although the C&A package references various	and NEMIS.			

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	subsystems supporting and hosting IFMIS and NEMIS, FEMA management was unable to identify and confirm the FSN-2 subsystems (including regional LANs) that host the production servers for NEMIS and IFMIS applications. Consequently, we were unable to test the hosting environment supporting financial applications in-scope for the FY 2010 environment.				
FEMA-IT-10-29	During the FY 2009 FEMA Integrated Audit, we noted that a C&A of PARS had not been performed and the system had not received an ATO since becoming operational in the FEMA environment. While improvements were noted in this condition for FY 2010, we determined that the following C&A weaknesses over PARS continue to exist: In FY 2010, the PARS database was included within the accreditation boundary for the IFMIS-Merger system, which was granted an ATO in June 2010. However, prior to that date, the PARS database was not certified and accredited and consequently, operated without an ATO for the majority of FY 2010. • All other system components of PARS, including the web and application servers, continued to operate without an ATO, and evidence that C&A efforts for these components of PARS were completed and approved by FEMA management could not be obtained from FEMA for review during the FY 2010 audit. • At the time of our test procedures, an ISSO had not been formally designated by FEMA management for the PARS web server and application. While we were informed by FEMA IT Security Management that the PARS database was administered by an ISSO under the Core IFMIS,	• Formally designate an ISSO for the PARS web server and application environment. • Certify and accredit the PARS web server and application environment, including documentation of all required artifacts in accordance with applicable DHS policies and Federal guidance.		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	we determined that no formal designation of this responsibility was assigned until FY 2010 because the PARS database was not included in the C&A boundary for Core IFMIS and no additional designation letters were issued. As a result, the PARS database did not have a formal designation of security responsibilities for the majority of the fiscal year.				
FEMA-IT-10-30	As noted during the FY 2009 audit related to Core IFMIS, we determined that weaknesses over the authorization of emergency and temporary access to the IFMIS – Merger Oracle database continue to exist in FY 2010. Specifically, FEMA has not established a formal process for approving emergency and temporary access to the IFMIS-Merger database that is compliant with DHS requirements. During our FY 2010 testing, we determined that emergency and temporary access to the database for individuals with elevated privileges, including access for contractor development personnel, is approved by the Financial Systems Section (FSS) Chief and/or his/her staff, not by the FEMA CISO or a designee, as required by DHS policy. Additionally, a formal process specifically addressing procedures for the granting of temporary access to the database and ensuring that access is removed in a timely manner has not been documented within existing IFMIS-Merger access control policies and procedures. Furthermore, we determined that through this process the IFMIS-Merger Oracle database access is granted to contracted development personnel in order to implement database changes to IFMIS-Merger, which continues to conflict with segregation of duties principles.	We recommend that FEMA document and implement a formal process for granting emergency and temporary access to the IFMIS-Merger database that includes guidance over all types of accounts authorized for temporary and emergency access, segregation of duties considerations, and appropriate approval from FEMA management in accordance with DHS policy.		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-10-31	During our unannounced enhanced security testing performed during the FY 2010 integrated audit, we noted that the FEMA Security Operation Center (SOC) proactively tracked and reported incidents related to social engineering attempts performed at FEMA headquarters and regional offices through implemented ad hoc processes. However, weaknesses noted during the FY 2009 integrated audit related to FEMA's incident response program continue to exist in FY 2010. Specifically, standard operating procedures for the management of FEMA IT security incidents have not been formally approved and implemented by FEMA management. Consequently, FEMA has not implemented DHS policy requirements to establish a documented and formally approved component-level incident response framework or capability, including roles, responsibilities, and processes related to the identification, evaluation, and resolution of all security incidents.	We recommend that FEMA formally approve and implement procedures for managing security incidents. Specifically, procedures should clearly outline roles and responsibilities required to maintain a continuous incident response capability and define processes related to the identification, evaluation, and resolution of all security incidents, as required by DHS and FEMA policy.		X	3
FEMA-IT-10-32	In FY 2009, we identified weaknesses over FEMA's patch management program as it relates to Core IFMIS and G&T IFMIS. During the FY 2010 integrated audit, we determined that while FEMA has finalized and formally implemented the *FEMA Office of the Chief Information Officer (OCIO) Standard Operating Procedure (SOP) for Vulnerability Patch Management*, the SOP was not approved until April 8, 2010. Consequently, FEMA did not have a formal patch management procedure applicable to the IFMIS environments for a majority of the fiscal year. Given the timing of the SOP's approval, the patch management procedures could not be implemented when G&T IFMIS was operational as it was merged with Core IFMIS in February 2010.	We recommend that FEMA further dedicate resources to document and fully implement comprehensive system-specific patch management procedures to ensure that IFMIS-Merger operating system and database patches are tested and deployed in a timely manner, in accordance with DHS and FEMA policy. No corrective action specific to the portion of this finding related to G&T IFMIS will be provided because of the decommissioning of that system in June 2010.		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Additionally, we determined that FEMA has not fully and consistently implemented the requirements and procedures documented in the SOP for IFMIS-Merger in accordance with FEMA and DHS guidance.				
FEMA-IT-10-33	Weaknesses noted in FY 2009 over FEMA's information security vulnerability management program as it relates to NEMIS continue to exist in FY 2010. Specifically: • FEMA does not have documented and approved procedures that establish formal requirements, processes, and responsibilities for performing regular vulnerability scans of NEMIS. • The list of NEMIS servers currently scanned by the SOC is incomplete and does not represent the current NEMIS system boundary as defined by system owners and IT security management. Additionally, NEMIS system owners are not receiving listings of all vulnerabilities noted on their system components to ensure corrective action is tracked and remediated. • Corrective action over vulnerabilities identified through SOC internal scans of NEMIS production servers is not formally tracked via the Plan of Actions & Milestones (POA&M) process, as required by DHS policy.	• Establish and implement documented procedures that define formal requirements, processes, and responsibilities for performing periodic vulnerability scans of NEMIS production servers. Additionally, ensure these procedures include requirements for reporting and tracking resolution of weaknesses identified during internal NEMIS vulnerability scans in accordance with DHS POA&M guidance. • Revise listing of NEMIS servers scanned by the FEMA SOC to ensure that vulnerability scans performed include all NEMIS servers within the current operating environment. Additionally, develop and implement procedures to ensure that this listing is periodically re-evaluated and updated as appropriate. • Revise the SOC distribution listing of NEMIS system owners and other appropriate IT security management to further define personnel responsible for remediating and formally tracking all vulnerabilities identified over the various NEMIS components. Additionally, develop and implement procedures to ensure that this listing is periodically re-evaluated and updated as appropriate.		X	2
FEMA-IT-10-34	Weaknesses noted in FY 2009 over FEMA's information security vulnerability management program as it relates to G&T IFMIS and IFMIS-Merger continue to exist in FY 2010. Specifically:	We recommend that FEMA establish and implement documented procedures that define formal requirements, processes, and responsibilities for performing regular vulnerability scans of IFMIS-Merger. Additionally, procedures should include		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• FEMA did not have documented and approved procedures that establish formal requirements, processes, and responsibilities for performing regular vulnerability scans of G&T IFMIS and IFMIS-Merger. • For one of the three months selected for testing, vulnerability scans were not performed for the G&T IFMIS production server. • For all three months selected for testing, vulnerabilities reported by the FEMA SOC over the G&T IFMIS and IFMIS-Merger production servers were not formally tracked via the POA&M process, as required by DHS policy.	requirements for reporting and tracking resolution of weaknesses identified during internal IFMIS-Merger vulnerability scans in accordance with DHS POA&M guidance. No corrective action specific to the portion of this finding related to G&T IFMIS will be provided because of the decommissioning of that system in June 2010.			
FEMA-IT-10-35	In FY 2009, we identified weaknesses over FEMA's patch management program related to NEMIS. During the FY 2010 integrated audit, we determined that while FEMA has finalized and formally implemented the FEMA OCIO SOP for Vulnerability Patch Management, the SOP was not approved until April 8, 2010. Consequently, FEMA did not have a formal patch management procedure applicable to the NEMIS environment for a majority of the fiscal year. Additionally, we determined that FEMA has not fully and consistently implemented the requirements and procedures documented in the SOP for all NEMIS components in accordance with FEMA and DHS guidance.	We recommend that FEMA further document and fully implement comprehensive system-specific patch management procedures to ensure that NEMIS operating system and database patches are tested and deployed in a timely manner, in accordance with DHS and FEMA policy. Additionally, these policies and procedures should include formal designation of responsibilities for oversight and implementation of required patch management activities for all NEMIS components to ensure compliance at the system level.		X	2
FEMA-IT-10-36	Weaknesses identified in FY 2009 related to the testing of NEMIS production database backup tapes continue to exist in FY 2010. Specifically: • During two quarters of FY 2010, FEMA conducted restoration tests of backup tapes for one specific	• Develop and implement backup policies and procedures to ensure that all NEMIS components are backed up and backup media is stored in/rotated to an off-site facility according to FEMA and DHS requirements. • Revise or develop policies and procedures to		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	NEMIS database while FEMA's SOP for Tape Backup Testing documents requirements for the testing of 39 databases. Consequently, we determined that FEMA did not regularly test backup tapes containing all NEMIS production database data during the fiscal year. • Additionally, while we noted that the Standard Operating Procedure for Tape Backup Testing assigns responsibility for testing backup tapes in accordance with a defined schedule to NEMIS IT security management, administrators, and system owners, the SOP was not updated to reflect the required schedule for performing tape restoration tests. Furthermore, we noted the following new weaknesses related to controls over the performance of NEMIS database backups: • FEMA has not formally defined and documented procedures that outline processes for performing backups of NEMIS production databases and for rotating and physically securing backup tapes off-site. • FEMA was unable to provide requested documentation to evidence that any of the 39 NEMIS production databases identified in the Standard Operating Procedure for Tape Backup Testing are currently being backed up.	periodically test and document testing of the NEMIS backups in compliance with FEMA and DHS requirements. In addition, ensure that policies and procedures are implemented to perform periodic restoration testing of all NEMIS production databases in accordance with established requirements.			
FEMA-IT-10-37	During our social engineering testing, several personnel provided us with user IDs and/or passwords. It should be noted that several personnel that we contacted by phone during our social engineering phone calls challenged our requests for user access	We recommend that FEMA management review the effectiveness of existing security awareness programs designed to protect "need-to-know" information, including IT system access credentials, and ensure that individuals are adequately instructed and reminded of their roles in the protection of sensitive system	X		3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	credentials by looking up our assumed names in the FEMA directory to determine if we were FEMA personnel, requesting employee IDs, asking for help desk ticket numbers associated with our calls, and reporting our attempts to supervisors. While individuals contacted represented several offices in multiple FEMA regions as well as Headquarters, our selection of individuals was not statistically derived. Therefore, we are unable to project these results to FEMA as a whole.	information from unauthorized individuals through formal, periodic communications and/or security awareness training.			
FEMA-IT-10-38	During our after-hours physical security testing conducted on July 20, 2010, we noted instances of improperly protected authentication credentials, system information, information technology assets, and PII in the facilities inspected. Some of the instances of improperly secured PII noted in the table above consisted of large stacks of documents or compiled spreadsheets that contained PII for numerous individuals conducting business for or with FEMA. Exceptions categorized as "Other' consisted of laptops and other IT assets not physically secured/locked to workspaces, unsecured bank account and government travel card information, and the lack of adequate locking mechanisms on a server room door. Our selection of areas at each facility that were inspected was not statistically derived, and therefore, we are unable to project results to FEMA as a whole.	We recommend that FEMA management review the effectiveness of existing security awareness programs designed to protect electronic and physical data, PII, and FOUO agency information and ensure that individuals are adequately instructed and reminded of their roles in the protection of both electronic and physical FEMA data and hardware through formal, periodic communications and/or security awareness training.		X	2
FEMA-IT-10-39	As noted during the FY 2009 audit, weaknesses continue to exist over the segregation of duties controls for the migration of IFMIS-Merger changes into production. Specifically:	We recommend that FEMA document and implement policies and procedures to limit IFMIS-Merger developer access to the production environment to "read only" and segregate the responsibility for deploying application code changes into production		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• The FEMA development contractor continues to deploy changes into the UNIX production environment through the use of the shared "ifmiscm" account. We noted that FEMA change management personnel are following SOPs that outline the controls intended to mitigate the risk associated with the IFMIS-Merger developers having the ability to migrate changes to the IFMIS-Merger production environment. In particular, the *Office of the Chief Financial Officer (OCFO) IFMIS System Change Request (SCR) SOP* requires the locking and unlocking of the "ifmiscm" account by system administrators during the implementation of software changes into production. However, we determined that while the SCR SOP states that system administrators will periodically monitor production directories to detect updates, no formal procedures or processes are included in the SOP or documented elsewhere for detailing how to monitor the directories or the requirements for performing the reviews to verify that only authorized changes to the "ifmiscm" directory and sub-directories are implemented into production by the developers. • We determined that although informal reviews of the directories were performed during the fiscal year, they were not routinely relied upon by FEMA management as they did not provide the level of detail required for adequate monitoring, and FEMA personnel were not able to distinguish the types of changes made to the system from the "ifmiscm" account.	from the development contractor to an independent control group. If business needs require that the segregation of duties cannot be immediately implemented, FEMA should document and implement policies and procedures to mitigate the risk associated with the segregation of duties weakness noted in accordance with DHS guidance, including a formalized process for performing and documenting reviews of activity performed by developers within the IFMIS-Merger environment.			
FEMA-	As noted during the FY 2009 audit, weaknesses	There is no recommended corrective action specific to		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
IT-10-40	continued to exist over the segregation of duties controls for the migration of G&T IFMIS changes into production during FY 2010. Specifically, the "ifmiscm" account was used by the FEMA development contractor to deploy changes into the UNIX production environment. Per our review, we noted that the G&T IFMIS application programmers responsible for maintaining and developing changes for the G&T IFMIS application were also responsible for migrating application code changes into the production environment using the "ifmiscm" account. We were informed by FEMA personnel that the controls over this account did not change from FY 2009 and that the account remained unlocked while G&T IFMIS was operational between October 2009 and June 2010 when the system was decommissioned. We were further informed by FEMA personnel that access to the "ifmiscm" account was not limited or monitored on a periodic basis, allowing the development contractor unrestricted access to the production environment. Additionally, we noted that FEMA has documented policies and procedures that require the IFMIS-Merger "ifmiscm" account to be locked and use of the account to be monitored. However, we noted that no established procedures or controls were in place for G&T IFMIS to mitigate the risk associated with this account. Consequently, we determined that while the G&T IFMIS application server was decommissioned in June 2010, the weaknesses over segregation of duties controls in the G&T IFMIS configuration management process continued to exist for the majority of FY 2010, and prior year NFR FEMA-IT-09-59 is reissued.	this finding because of the decommissioning of G&T IFMIS in June 2010.			

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-10-41	Password, patch management, and configuration management weaknesses were identified during vulnerability assessment technical testing. *Note: Due to the nature of this finding, see the tables in associated NFR for the specific details of the conditions.*	Implement the specific corrective actions listed in the NFR for each technical control weakness identified.		X	3
FEMA-IT-10-42	During the FY 2010 integrated audit, we noted the following weaknesses over the completeness and accuracy of certain C&A artifacts that support the Authorizing Official's decision to grant an ATO for the IFMIS – Merger: • A risk assessment for IFMIS-Merger had not been completed or documented prior to granting an ATO, in accordance with DHS and NIST requirements. Additionally, FEMA does not plan to conduct and document a risk assessment or the results of the required risk assessment activities for IFMIS-Merger as FEMA management has indicated that it is not required for FY 2010. • The ATO was signed in June 2010, more than three months after the IFMIS-Merger system was operational in late February 2010. • Per our review of the security assessment report, the assessment performed over IFMIS-Merger prior to granting ATO did not include evaluation of any of the controls identified within the SSP. The assessment was limited to vulnerability and compliance scans. • The ST&E was not properly conducted because the baseline controls in the Requirements Traceability Matrix were not consistent with DHS requirements.	• Update and complete all required C&A artifacts for IFMIS-Merger in accordance with DHS policy and NIST guidance. • Ensure that C&A artifacts, including the risk assessment or the results of the required risk assessment activities, the ST&E, and the Security Assessment Report (SAR) are conducted and documented in accordance with established DHS baseline controls according to the security categorization of the system.	X		3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-10-43	During the FY 2010 integrated audit, we noted that the most recent ATO for NEMIS was signed on October 29, 2009. However, we identified weaknesses in the completeness and accuracy of certain C&A artifacts that support the Authorizing Official's (AO) decision to grant the ATO for NEMIS. Specifically, the NEMIS Risk Assessment, ST&E, and SAR were completed in 2006, and thus outdated as DHS policy requires C&A artifacts supporting ATOs to be updated within the 13 months prior to granting the most recent ATO, and NIST requires each to be conducted every 3 years.	We recommend that FEMA update and complete all required C&A artifacts for NEMIS in accordance with DHS policy and NIST guidance.	X		3
FEMA-IT-10-44	Conditions noted in FY 2009 related to weaknesses over controls in place to monitor and restrict access to highly-privileged system accounts within the UNIX environment that supports IFMIS-Merger and G&T IFMIS continue to exist in FY 2010. Specifically: • Access to the "root" account is not properly restricted and system administrator activities are not appropriately logged. Specifically, the password to access the UNIX "root" administrator account is shared between the administrators and remote access to the root account is not locked down. • System administrator actions are not monitored and attributable to individual administrators. Specifically, FEMA has not enforced the use of the "sudo" command, which requires system administrators to login with their individual user ID and then switch over to the root account to ensure who is accessing the account is logged and authorized. • System logs and reports of administrator activity, including the "sudo" log which monitors actions performed by administrators while acting as the	We recommend that FEMA document and implement appropriate technical and management controls to restrict and monitor access to privileged system administrator accounts on the IFMIS-Merger operating system, including use of the "root" account, in accordance with DHS and FEMA policy. Additionally, policies and procedures should include requirements to ensure that system logs and records of administrator activity, including the "root" account, are retained and reviewed by IT security management independent of the system administration team, especially where individual traceability for the account is not possible. There is no recommended corrective action specific to the portion of this finding related to G&T IFMIS because of the decommissioning of G&T IFMIS in June 2010.		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	"root" account, were not reviewed by FEMA management personnel independent of the system administration staff.				
FEMA-IT-10-45	In FY 2009, we noted weaknesses over suitability determinations for federal employees and contractors with sensitive IT system access that continued to exist in FY 2010. Specifically, of 15 federal employee positions selected for testing: • Three did not have evidence of a completed background investigation on file that met minimum investigative requirements specified by DHS policy. • For one employee, FEMA was unable to provide any documentation to evidence that the employee's background investigation was performed and maintained within ISMS, FEMA's personnel suitability and investigation recordkeeping utility. • Nine that are defined as "high risk" according to FEMA policy did not have an appropriate position sensitivity designation that reflected the risk level required by DHS policy. During our FY 2010 test work over contractors, we determined that no formal procedures have been developed or implemented by FEMA to address DHS requirements surrounding the suitability screening of contractors accessing DHS IT systems. Additionally, we selected a population of 15 contractors with access to multiple FEMA information systems who hold sensitive IT security positions at FEMA such as system administrators, database administrators, and systems development contractors and determined that FEMA has not appropriately conducted suitability	• Further define and refine documented processes to ensure that background investigations for all Federal employees are performed and procedures are implemented in accordance with DHS directives. • Re-evaluate and assign the correct position sensitivity levels to all Federal employees with access to DHS information systems in accordance with DHS policy. Additionally document and/or revise, and fully implement procedures to ensure that program managers are aware of requirements and appropriate position sensitivity levels are designated for all sensitive IT positions in the future. • Document and fully implement procedures within FEMA Acquisitions, FEMA Personnel Security, and FEMA IT to ensure a more centralized and coordinated process for tracking and completing background investigations over contractor personnel in accordance with DHS policy. • Ensure that all system owners document and correctly define the appropriate sensitivity designations for contractor personnel needing access to their information systems in accordance with DHS policy. Additionally, ensure that position sensitivity designations are assigned based on the type of privileges needed, and require contractors to have their suitability investigations completed prior to being granted access to the system in accordance with FEMA and DHS policy.		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	investigations. Specifically: • For two, FEMA was unable to provide any documentation to evidence that the contractor's record was maintained within ISMS, including the status of any background investigations performed. • Six did not have evidence of a completed background investigation on file that meets minimum investigative requirements specified by DHS policy. Of the six, two had records maintained within ISMS; however, FEMA was unable to provide evidence that background investigations for each were performed. • None had position sensitivity designations defined by FEMA for the sensitive IT position they held at the time of our test work, as required by DHS policy.				
FEMA-IT-10-46	During the FY 2010 integrated audit, we noted weaknesses in controls over the configuration management of application, web, and database servers within the NEMIS production environment. Specifically: 1. Access to the multiple application, web, and database servers that comprise the NEMIS production environment for deploying approved code changes is limited to IT Enterprise Operations staff. However, no formalized change management procedures exist for deploying changes to ensure the movement of production code for the NEMIS production environment is appropriately controlled.	• Document and implement a formalized process and procedures for deploying NEMIS changes to ensure the movement of production code for the NEMIS production environment is appropriately controlled. Procedures should include requirements for restricting and, monitoring access and documenting reviews to the NEMIS production environment to ensure that the principles of least privilege and segregation of duties are enforced, in accordance with DHS guidance. • Ensure that adequate technical controls are implemented to enforce least privilege and segregation of duties requirements for the implementation of system changes. If individual		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	2. Access to a shared service account is used for the deployment of Linux changes. However, FEMA was unable to provide any system documentation or associated artifacts demonstrating that FEMA was appropriately restricting and controlling access to the NEMIS production application, web, and database servers.	accounts are not possible for deploying changes, implement logical access controls, including configuration of system audit logs, on NEMIS production servers to establish individual accountability for all FEMA personnel with access to the environment through the shared service account, in accordance with DHS and FEMA policy. Additionally, for these shared service accounts, document, implement, and approve standard operating procedures for the implementation and formal review of NEMIS system changes on production servers.			
FEMA-IT-10-47	In FY 2009, we noted that FEMA's OCFO and NFIP financial systems development and acquisition projects were undertaken and progressed without (1) proper oversight of and direction to contractors, (2) development and approval of required project documentation, (3) the continual involvement of the OCIO to ensure appropriate consideration and integration of IT security, and (4) the joint communication and decision-making of FEMA OCFO, OCIO and NFIP management. As a result, we recommended that FEMA management define and implement formal and repeatable processes to ensure that financial systems development and acquisition projects are conducted in compliance with DHS SELC and acquisition requirements as well as Federal guidance. During the FY 2010 integrated audit, we determined that FEMA management has not implemented corrective actions or developed a corrective action plan to address the prior year weaknesses noted. Specifically, entity level corrective actions to integrate and develop sufficient and effective methods of communication to ensure that significant financial-	• Define and implement formal and repeatable entity level control processes to ensure that financial systems development and acquisition projects are conducted in compliance with DHS System Engineering Life Cycle (SELC) and acquisition requirements as well as Federal guidance. The processes should define steps to include, but are not limited to, formal approval of required project documentation, sufficient contractor oversight, definitions of project roles and responsibilities so that decision making includes the appropriate involvement of all stakeholders and relevant FEMA management, establishment of ADEs at each SELC phase, and integration of IT security considerations throughout all project phases. • Identify and formally assign stakeholders associated with the remediation efforts over aligning the DHS SELC methodology with FEMA's acquisition development process to ensure appropriate participation from all required organizations within FEMA in both the development of policies and procedures and integration of the financial systems acquisitions life cycle stages as required by DHS policy.		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	related system development and acquisition projects involve all relevant stakeholders, including the OCFO, have not been established. Additionally, FEMA management has not taken action to enhance and further develop current acquisition management processes to ensure that organization-specific requirements exist and are implemented so that each project meets organizational mission needs and functional and technical requirements as required by DHS and NIST guidance.				
FEMA-IT-10-48	FEMA IT security management responsibilities were not consistently or adequately assigned and performed over the FEMA POA&M process for FY 2009 IT audit findings, in accordance with DHS guidance. Specifically: • POA&Ms created by FEMA management in response to FY 2009 IT financial statement audit findings were not consistently categorized with the appropriate criticality level in accordance with DHS policy. Specifically, for 52 POA&Ms provided by FEMA on May 3, 2010, criticality was either undefined or erroneously defined as "Annual Assessment Finding" rather than "Initial Audit Finding" or "Repeat Audit Finding," as required. • FEMA management did not consistently document detailed corrective action plans or appropriate milestones, including required tests of design and effective implementation for financial system POA&Ms. • FEMA management did not consistently assign POA&M stakeholder ownership for corrective action plans or related milestones.	• Establish and document a formalized process to provide IT security management oversight to ensure that adequate periodic review and assessment of security controls are performed and corrective actions are appropriately assigned and implemented over identified security weaknesses through the POA&M process. • Dedicate resources to fully implement DHS requirements over the POA&Ms for audit findings of FEMA financial systems, including the proper categorization of audit findings, documentation of all stakeholders with remediation responsibilities, and monitoring of POA&M activities to validate that corrective actions are appropriately documented with associated milestones and evidence of remediation is developed and retained. • Develop and implement a training program for personnel with IT security responsibilities, such as system owners and ISSOs, to ensure that they fully understand their roles and responsibilities to correctly categorize the findings, formally define milestones, and validate the documentation and testing of the corrective action implemented. • Develop and implement review procedures to ensure developed POA&Ms are detailed enough to		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		demonstrate that the root cause of the issue has been assessed and the milestones address the necessary steps to fully remediate the weaknesses as required by DHS policy.			
FEMA-IT-10-49	During the FY 2010 follow-up testwork, we determined that weaknesses noted in FY 2009 continue to exist. Specifically, we determined that no additional policies and procedures to establish a process for implementing change controls for the maintenance of system security functions have been developed by FEMA or the IT developer of IFMIS-Merger. FEMA has not adequately ensured that appropriate privileges granted to users are created, documented, and approved. We were informed by FEMA personnel that the system security functions are created and modified to provide additional functionality under specific menus in the IFMIS-Merger application. As a result, these changes to the menu provide additional functionality to the users with access to those menus. However, current documentation over IFMIS-Merger, including access authorization forms, change management plans and System Security Plans, do not define how to manage and document changes to these functions to ensure that approved changes are made and appropriate and traceable access is granted to IFMIS-Merger users. While FEMA has received the IFMIS Security Functions Reference Guide dated 2007 from the software vendor, we determined that the documentation is a technical reference manual that defines the capabilities of the system, usage of the various system security functions, menu options and related permissions for each function. However, the guide does not address the management of these system	• Dedicate resources to assess the usage of IFMIS-Merger system security functions against DHS policy requirements and determine gaps that exist within existing system documentation over the security functions. • Develop and implement policies and procedures documenting the process of adding, deleting, and modifying IFMIS-Merger system security functions to ensure that proper controls are in place for approving, testing and documenting these functions prior to implementation, in accordance with DHS policy. These policies and procedures should include requirements over independent monitoring of the creation, modification and deletion of system security functions, and requirements for updating system documentation to reflect the impact of the changes to user account privileges. • Develop and implement procedures to ensure that functions updated through the change management process are formally approved and documented and that appropriate system documentation for IFMIS-Merger system security functions is updated and retained, in accordance with DHS policy.		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	security functions from a change control and access control perspective for FEMA. Additionally, the guide does not include requirements for updating system documentation and tracking these system security function changes to privileges in the system. Consequently, based on our testwork, we concluded that a formalized process for modifying specific IFMIS-Merger system security functions to ensure that appropriate privileges are created, documented, approved, and monitored does not exist.				
FEMA-IT-10-50	During the FY 2010 FEMA integrated audit, we determined that the following conditions related authorization of external connections to the FEMA VPN continue to exist: • Two-factor authentication is not used for VPN access, as required by DHS policy. • The existing documentation that defines the process for granting and maintaining VPN access to the FEMA network does not include requirements for administering the site survey process, including requirements for the authorization of the sites surveys, recertification of site surveys, and the security requirements associated with the various aspects of the process. • FEMA has not formally identified and documented the roles and responsibilities necessary within FEMA to properly authorize and administer VPN access to individuals using non-DHS equipment to access the FEMA network. • Access for state emergency management agencies and FEMA contractors to load the VPN client onto state or contractor owned equipment to connect to	• Implement and require two-factor authentication for all remote access to the FEMA network, as required by DHS policy and FIPS 140-2. • Revise and implement policies and procedures for documenting, reviewing, and approving the security controls in place over non-DHS equipment connecting to the FEMA network via VPN access. Specifically, clearly define and document a formalized process for the authorization, review, and maintenance of VPN access agreements between FEMA and external entities. Additionally, ensure that within the policies and procedures, appropriate roles and responsibilities over the process are defined to include authorizations by the CISO/ISSM to connect to non-DHS equipment. • Ensure that agreements related to VPN access are reviewed and recertified when a major system change occurs or every three years, in accordance with DHS policy. • Formally identify and document appropriate roles and responsibilities related to management of remote access to the FEMA network, including iPass and VPN.		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	the FEMA LAN is approved by the SOC. However, DHS policy requires that any non-DHS equipment connecting to a DHS network must be authorized by the Component CISO/ISSM. • FEMA's *VPN Rules of Behavior for Users Behind Corporate Firewalls*, dated December 5, 2002, requires an Inter-Agency VPN Agreement between FEMA and external organizations before permitting VPN access to the FEMA network through non-Government issued equipment such as contractor or state agency workstations. However, we determined that Inter-Agency VPN Agreements have not been documented and that this requirement is inconsistent with DHS policy, which requires ISAs or (MOUs/MOAs prior to establishing a VPN connection from equipment operating on an external network. • FEMA's approval of requests for network connections to external organizations through VPN access for remote users is based on security control information submitted by the external entities via site surveys. Based upon our review of existing site surveys and the site survey process, we noted that: • The site surveys do not contain the level of technical granularity describing the external network security controls required to appropriately approve a connection to the FEMA LAN, and the FEMA SOC does not independently verify the accuracy of information in the site surveys submitted by external entities prior to approving the connection and subsequently granting VPN access to users.	• Document and implement policies and procedures to ensure that formalized ISAs, MOUs, or MOAs, delineating security responsibilities by FEMA and external organizations when connecting through non-DHS equipment to the FEMA network via VPN access are used. Such agreements should include evidence of validation by FEMA management that security controls in place on external entity networks are appropriate and satisfy requirements for minimum security controls on DHS and FEMA systems prior to connection in accordance with DHS policy.			

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• DHS guidance indicates that a single ISA may be used for multiple connections provided that the security accreditation is the same for all connections covered by that ISA. However, we determined that the security accreditation of the connecting networks is not being evaluated by the FEMA SOC during the review of site surveys to ensure the security requirements are appropriately implemented.				
FEMA-IT-10-51	In FY 2009, we identified weaknesses over configuration management controls related to NEMIS program libraries and directories within the TDL environment. During the FY 2010 integrated audit, we determined that the following weaknesses continue to exist: • Controls to segregate access within the TDL environment have not been appropriately implemented. Specifically, IT Systems Integration personnel do not grant separate privileges to development code, which is moved to TDL by the systems developer, and pre-production code, which has completed User Acceptance Testing (UAT) and is pending deployment to the NEMIS production environment. As a result, developers have read, write and execute privileges to all code in the TDL environment. • Code approved for implementation is not locked down within the TDL environment prior to deployment to production. Additionally, while an ad-hoc review is performed over the directories to monitor the modification dates on the production code directories, this process is not performed consistently or documented to mitigate the risk associated with not restricting access to the	• Document and implement formalized policies and procedures for restricting and monitoring access to the NEMIS TDL directories to ensure that the principles of least privilege and segregation of duties are enforced, in accordance with DHS guidance. The process should include requirements over periodic monitoring and documented reviews of NEMIS TDL directories to verify that no changes have occurred after the approval of NEMIS system changes. • Implement technical controls within the NEMIS TDL environment to limit developers' access to pre-production directories containing "locked" application code changes to "read only". If business needs require that the segregation of duties cannot be immediately implemented, FEMA should document and implement policies and procedures to compensate for the risk associated with the segregation of duties weakness noted, in accordance with DHS guidance.		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	approved code.				
FEMA-IT-10-52	Conditions noted in FY 2009 related to weaknesses over vulnerability assessments for the Windows server environment within the NFIP LAN supporting the Traverse application continue to exist in FY 2010. Specifically: • While procedures have been developed, the NFIP contractor has not fully implemented the process for conducting internal vulnerability scans for information systems and for assessing, reporting, and correcting identified weaknesses through the POA&M Process in accordance with FEMA and DHS guidance. • FEMA does not have documented and approved procedures that establish formal requirements, processes, and responsibilities for conducting monitoring and oversight of regular vulnerability scans performed over the NFIP LAN which supports Traverse to meet DHS vulnerability assessment requirements. • Furthermore, while ad hoc scans were performed in previous years by the contractor, evidence of periodic NFIP network scanning conducted in FY 2010 could not be obtained. Additionally, we inquired with FEMA and determined that scans over the NFIP LAN supporting the Traverse application were not performed by the FEMA SOC.	• Document and implement formal policies and procedures that outline the processes and requirements for performing internal vulnerability scans over all NFIP information systems as well as the process for assessing, reporting, and correcting weaknesses identified during scans as required by FEMA and DHS policy. • Ensure that policies and procedures formally designate responsibilities of FEMA OCIO and NFIP IT security management for the implementation, monitoring, and oversight of the vulnerability scanning process, so that the scope of vulnerability scans conducted include all NFIP workstations and servers and include requirements for formally tracking and monitoring the remediation of vulnerabilities identified during the internal scans of the NFIP LAN through the POA&M process, in accordance with DHS policy.		X	2
FEMA-IT-10-53	During our FY 2010 integrated audit test work, we noted that NFIP has not established or implemented an effective process to periodically recertify user access, including service accounts, on the TRRP mainframe. Currently, NFIP requires users to sign security	• Complete the revision, documentation, and full implementation of TRRP access control policies and procedures, and ensure that they include a formalized process for the recertification of all accounts on the mainframe, including service		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	awareness and training certifications on an annual basis. However, no review of users' access and privileges is conducted by management on a periodic basis to ensure system access remains appropriate and commensurate with job responsibilities in accordance with DHS guidance. Additionally, we noted through inspection of the TRRP access procedures that no process has been established to formally document both the approval and business need for service accounts.	accounts, on an annual basis to determine that access remains appropriate and commensurate with job responsibilities in accordance with DHS policy. • Document and implement policies and procedures over the creation of service accounts to ensure that they are appropriately authorized and that a clear business need is established and documented justifying the creation and use of these types of accounts in accordance with DHS policy.			
FEMA-IT-10-54	During the FY 2010 integrated audit, we determined that weaknesses existed in the implementation of DHS SELC requirements over the IFMIS-Merger Project. Specifically, throughout the lifecycle of the project, FEMA management did not adequately define and implement required elements of the DHS SELC process, including: • A detailed and comprehensive Project Tailoring Plan to define required stages, activities, artifacts and exit criteria for the project per DHS SELC guidance was not developed and approved by FEMA management. • Approvals for project critical documentation demonstrating that all required stakeholders reviewed and approved the results before advancing to subsequent SELC stages could not be provided. • FEMA could not provide a Data Migration Plan and Test Strategy to demonstrate that critical DHS SELC requirements were documented and approved prior to implementation of the data migration.	We recommend that FEMA management conduct and document a lessons learned report related to the IFMIS-Merger project per DHS SELC guidance. By conducting such an activity, FEMA management will be able to maintain a record of lessons learned in order to increase the probability of success for future acquisitions through the improvement of processes, tools, and other project related entities. Additionally, we determined that the root cause associated with the weaknesses noted over the SELC process is related to the entity level control issue identified in FEMA-IT-10-47, FEMA Management Needs to Improve Planning, Management, and Communication Related to Financial Systems Development and Acquisition Projects. While the IFMIS-Merger project has been completed, corrective action over the establishment of a process to provide oversight to the implementation of the SELC methodology must be completed. Please see NFR FEMA-IT-10-47 for recommendations related to the establishment of this process.	X		3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• System security requirements and milestones were not documented and integrated into key project documentation, such as Business Requirements documents, project schedules, Project Management Plans, and Risk Management Plans. • Project documentation including the Project Management Plan, the Risk Management Plan, and Business Requirements documents were not updated and revised throughout the project duration as required by the DHS SELC. • Key information such as roles and responsibilities of all stakeholders, guidelines for developing business requirements documentation, requirements for stage reviews, and key exit criteria before moving to the next stage of the project were not integrated into the project schedule, Project Plan, and Communications Plan. • FEMA management did not provide adequate oversight of the contractors implementing the IFMIS-Merger Project. Specifically, documented evidence supporting the approval, validation, and retention of required artifacts associated with the data migration and other key project management documents could not be provided by FEMA or were insufficient based on DHS requirements.				
FEMA-IT-10-55	During our FY 2010 integrated audit test work, we noted the following weaknesses related to the management and monitoring of user accounts and activity on the NFIP LAN supporting Traverse: • NFIP has not established or implemented a formal process to periodically recertify all accounts with access to the NFIP LAN supporting Traverse, as	• Complete the revision, documentation, and full implementation of access control policies and the NFIP LAN system account management procedures to align with DHS requirements such as recertification of accounts and audit log reviews. Specifically, ensure that they include a formalized process for the recertification of all accounts on the	X		2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	required by DHS and FEMA policy. Specifically, six system and/or service accounts on the FEMA LAN remained active absent an acceptable documented business need and justification. We were informed by NFIP management that these accounts were no longer needed, and they were removed from the system during test work. • Audit logs generated and reviewed on the NFIP LAN do not include changes to user account privileges as required by DHS and FEMA policy. • Audit logs for the NFIP LAN are not retained for at least 90 days, in accordance with DHS policy.	NFIP LAN, including service accounts, on an annual basis to determine if access remains appropriate and commensurate with job responsibilities in accordance with DHS policy. • Document and implement policies and procedures over the creation of service accounts to ensure that they are appropriately authorized and that a clear business need is established and documented justifying the creation and use of these types of accounts in accordance with DHS policy. • Configure the NFIP LAN audit logs to include changes to user account privileges and ensure that storage capacity settings of audit logs are configured to retain the logs for 90 days online as required by DHS and FEMA policy.			
FEMA-IT-10-56	During our FY 2010 integrated audit, we noted the following weaknesses related to the monitoring of user accounts and activity on the TRRP mainframe: • Segregation of duties is not properly implemented over the review and maintenance of TRRP audit logs. Specifically, the TRRP system administrator is responsible for reviewing TRRP audit logs, and a second independent reviewer is not required. • Audit logs generated and reviewed on the TRRP mainframe do not include changes to user account privileges as required by DHS and FEMA policy.	• Develop and implement TRRP audit logging policies and procedures that include requirements for audit log configurations and the review of logs by IT security management independent of the system administration team in accordance with DHS policy. • Configure the TRRP audit logs to include changes to user account privileges as required by DHS and FEMA policy.	X		2
FEMA-IT-10-57	During our FY 2010 integrated audit test work, we noted that NFIP has not established or implemented a formal process to authorize or periodically review remote access to the LAN hosting the TRRP mainframe environment in accordance with DHS and NIST guidance.	• Develop, document, and fully implement policies and procedures over documenting, reviewing, and approving remote access to the NFIP LAN hosting the TRRP mainframe environment in accordance with FEMA and DHS requirements. • Develop, document, and fully implement policies and procedures to perform a periodic recertification of all remote user access and retain	X		2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		auditable records as evidence that recertifications are conducted and completed in accordance with DHS and FEMA policy.			
FEMA-IT-10-58	While improvements were noted over the documentation of Traverse change management procedures during the FY 2010 integrated audit test work, we determined that certain weaknesses identified in FY 2009 continue to exist over the Traverse configuration management process in comprehensively addressing FEMA and DHS change management policy. For example, we determined that: • Established procedures do not include guidance for initial approvals as we were informed that Traverse currently does not fall under review of the NFIP Change Control Board (CCB). • Requirements for managing the change management program have not been adequately established and implemented to ensure that NFIP CCB and/or TRC approvals are granted prior to implementing changes into the Traverse production environment, as required by FEMA and DHS policy. • Adequate oversight and involvement from FEMA management is not integrated into the configuration management requirements. Specifically, FEMA is not involved in testing and/or reviewing testing and approving changes to Traverse prior to implementation. • Traverse changes are not required to be tested prior to implementing the change into production as no testing environment exists. • Limited testing requirements exist to guide personnel in the development of test plans and	• Ensure the NFIP contractor continues to dedicate resources to establish and implement documented policies and procedures over the Traverse change management process for non-emergency and emergency changes which are in line with DHS configuration management requirements. Particular emphasis must be placed on approval by the NFIP CCB and/or TRC, initial change approvals, testing and testing requirements, final approvals, and retention of required change management artifacts to track all changes throughout their lifecycle. These phases should also include an integrated process to address system change requirements and stakeholder change requirements to ensure adequate testing and approvals are completed by the appropriate parties. • Establish and implement a formal process to conduct user acceptance testing in a test environment prior to implementation in production. • Allocate qualified NFIP management and OCIO IT security resources to provide adequate oversight for the configuration management process. Oversight activities should encompass requirements such as a NFIP Program Configuration Management Board responsible for managing and participating in the NFIP CCB and/or TRC to ensure that all required elements in the configuration management process are formally defined and implemented in accordance with DHS and FEMA guidance.		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	guidance over the testing that should be performed and documented. Additionally, roles and responsibilities over test plan procedures to ensure that plans are sufficient, document expected outcomes, and are reviewed and approved prior to development, are not documented. • Requirements for Traverse emergency changes have not been formally defined.	• Dedicate the resources to fully review and finalize approval of all NFIP contractor's configuration management policies and procedures to ensure the revised procedures are compliant with DHS requirements.			

FEMA-IT-10-59	While improvements were noted over the documentation of TRRP change management procedures during the FY 2010 integrated audit testwork, we determined that certain weaknesses identified in FY 2009 continue to exist over the TRRP configuration management process in comprehensively addressing FEMA and DHS change management policy. For example, we determined that:
	• Requirements for managing the change management program have not been adequately established and implemented to ensure that CCB and/or TRC approvals are granted prior to implementing changes into the TRRP production environment, as required by FEMA and DHS policy. Specifically:
	  • While a CCB has been established by NFIP management, adequate oversight and involvement from FEMA management has not been integrated into the configuration management requirements including mandatory FEMA participation in the CCB and CCB approval of changes after testing has occurred.
	  • FEMA management, including IT security and financial personnel, are not involved in testing
		• Ensure the NFIP contractor continues to dedicate resources to establish and implement documented policies and procedures over the TRRP change management process for non-emergency and emergency changes which are in line with DHS configuration management requirements. Particular emphasis must be placed on initial change approvals, testing and testing requirements, final approvals, and retention of required change management artifacts to track all changes throughout their lifecycle. These phases should also include an integrated process to address system change requirements and stakeholder change requirements to ensure adequate testing and approvals are completed by the appropriate parties.
		• Allocate qualified NFIP management and OCIO IT security resources to provide adequate oversight for the configuration management process. Oversight activities should encompass requirements such as a NFIP Program Configuration Management Board responsible for managing and participating in the NFIP CCB and/or TRC to ensure that all required elements in the configuration management process are formally defined and implemented in accordance with DHS and FEMA guidance.
				X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	and/or reviewing testing and approving changes to TRRP prior to implementation. • CCB reviews are not conducted for approval of final changes prior to implementation into production as required by FEMA and DHS guidance. • Limited testing requirements exist to guide personnel in the development of test plans and guidance over the testing, including user acceptance testing, that should be performed and documented prior to approval and implementation into production. Additionally, roles and responsibilities over test plan procedures to ensure that plans are sufficient, document expected outcomes, and are reviewed and approved prior to development, are not documented. • Requirements for TRRP emergency changes have not been formally defined in writing. Furthermore, we performed testwork over initial and final approvals for a selection of 25 TRRP changes made in FY 2010 and noted the following exceptions: • Documentation for 3 of the 25 changes could not be provided • 17 of 22 changes tested did not have initial approvals documented prior to developing the change • 9 of 22 changes tested changes did not have all the required approvals prior to implementation • 1 of 22 changes tested was implemented prior to	• Dedicate the resources to fully review and finalize approval of all NFIP contractor's configuration management policies and procedures to ensure the revised procedures are compliant with DHS requirements.			

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	change documentation being completed				
FEMA-IT-10-60	Weaknesses identified in FY 2009 related to controls to restrict access and control movement of Traverse program libraries and data continue to exist in FY 2010. Specifically: • Implementation procedures over Traverse changes have not been established, and current processes do not incorporate segregation of duties requirements. Specifically, NFIP IT contractors use their individually assigned system administrator accounts to logon and create sessions to allow a third-party development vendor to install Traverse system changes. • NFIP does not have a formal process for monitoring changes that the vendor makes in Traverse while logged in as an administrator.	• In accordance with policy, enforce requirements over individual user accounts by not allowing vendors to a use a system administrator's account to access the system and deploy changes into production. • Document and implement policies and procedures to limit Traverse developer and application support vendor access to the NFIP production environment to "read only" through an assigned user account and segregate the responsibility for deploying application code changes into production from the development/support vendor to an independent control group. Additionally, procedures should include implementation process requirements for controlling access to production directories. If business needs require that the segregation of duties cannot be immediately implemented, FEMA should document and implement policies and procedures to mitigate the risk associated with the segregation of duties weakness noted in accordance with DHS guidance, including a formalized process for performing and documenting reviews of activity performed by third-party vendors within the Traverse environment.		X	2
FEMA-IT-10-61	As noted during the FY 2009 audit, weaknesses over contingency planning for both the Traverse and TRRP systems continue to exist in FY 2010. Specifically: • While the NFIP Legacy System Services (NFIP/LSS) Contingency Plan, which pertains to the contingency planning around Traverse and the NFIP LAN, has been updated for FY 2010, the following elements are not in compliance with	• Develop, document, and fully implement an IT Contingency Plan for NFIP components, including TRRP and Traverse. Additionally, ensure that contingency planning documentation includes detailed instructions for restoring operating system software and critical applications in the event of a disaster, contingency, or disruption of service in accordance with DHS and NIST policy requirements for systems categorized at the high		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	DHS and NIST requirements: • The NFIP/LSS IT Contingency Plan does not document detailed instructions for restoring operating systems and critical applications in the event of a disaster, contingency, or disruption of service. • The NFIP/LSS IT Contingency Plan does not designate the current alternate processing facility for the operating environment. • Testing of the NFIP/LSS IT Contingency Plan has not been performed in the 12 months, as required by DHS policy. • FEMA and NFIP management have not documented or approved a current IT Contingency Plan for the mainframe environment supporting the TRRP system in accordance with FEMA and DHS requirements. • Contingency testing over TRRP was not sufficiently conducted in accordance with DHS and NIST requirements. While a limited disaster recovery test of the NFIP mainframe environment, including TRRP, was performed in October 2009 to test restoration of data, all elements required to be tested under the DHS requirements for an IT Contingency Plan were not sufficiently addressed and could not be used to validate the effectiveness of the organization's contingency planning controls. • The NFIP contractor's Continuity of Operation Plan (COOP) for Traverse and TRRP could not be provided for auditor review.	impact availability objective. • Conduct and document annual tests of the TRRP and Traverse IT Contingency Plan(s) that address all critical phases of the plan(s), and update contingency planning documentation with lessons learned, as necessary and in accordance with DHS and NIST requirements. • Dedicate resources to establish and implement an alternate processing site for the NFIP systems in accordance with DHS policy requirements. • Until an alternate processing site is established, develop and submit an exception for approval in accordance with DHS policy, and ensure that compensating controls over the lack of an alternate processing site have been implemented and are effective, and documentation of their effectiveness is maintained as auditable records. • Document, implement, and maintain the NFIP COOP to ensure required elements for Traverse and TRRP are included in accordance with DHS guidance for high impact systems.			

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-10-62	Conditions noted in FY 2009 related to weaknesses over the NEMIS configuration management process continue to exist in FY 2010. Based on our testwork, we concluded that NEMIS configuration management is not adequately and centrally controlled, documented, or managed throughout the lifecycle of the FEMA configuration management process. Specifically, we identified the following weaknesses: • NEMIS configuration management policy and procedures which outline FEMA's responsibilities and processes for initiating, monitoring, testing, and approving NEMIS non-emergency and emergency changes that are developed under the various development contracts have not been documented and approved by FEMA management, in accordance with DHS and FEMA policy. • FEMA does not have a centralized program management function or process to monitor and track NEMIS Software Change Requests (SCRs) throughout the configuration management lifecycle, from initial approval through implementation into the production environment.	• Document and establish a centralized and integrated change management process over NEMIS to ensure that adequate controls are implemented throughout the lifecycle of the configuration management process, in accordance with DHS and FEMA policy. • Formally designate FEMA management responsibilities for oversight and implementation of controls for initiating, monitoring, testing, and approving all NEMIS non-emergency and emergency changes; • Establish a centralized, formal process to monitor, document, and track NEMIS software changes throughout the configuration management lifecycle, from initial approval through implementation into the production environment.		X	3
FEMA-IT-10-63	During the FY 2010 integrated audit, we noted weaknesses over the IFMIS-Merger Configuration Management Plan. Based on our testwork, we concluded that the IFMIS configuration management process does not meet comprehensive change management process requirements and procedures as required by DHS and NIST guidance because it is not adequately documented. For example, we identified the following weaknesses: • The IFMIS CMP provided in July 2010 is in draft and has not been updated to reflect the new IFMIS-	• Revise, document and fully implement a comprehensive configuration management program that includes a Configuration Management Plan for IFMIS-Merger, which aligns with all applicable DHS and FEMA requirements and reflects the current IFMIS-Merger operating environment and all applicable IT components. • Include in policies and procedures (a) clearly defined and formalized responsibilities for change management oversight bodies including a Configuration/Change Control Board and (b) sufficiently detailed responsibilities and	X		2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Merger operating environment. Specifically, the plan includes Core IFMIS and G&T IFMIS, but does not address the IFMIS-Merger instance that began operations in February 2010. • Infrastructure information for the in-scope applications does not include the server information for G&T IFMIS, which was operational when the plan was last revised in November 2009. • The CCB has not been formally and fully integrated into the FEMA change management process. While we were informed that a CCB for IFMIS was established on March 22, 2010, we determined that the requirements over the roles and responsibilities as well as the membership of the CCB were not clearly defined, implemented, and documented to ensure that DHS requirements are met. • Membership of the "SCR Review Team" responsible for initial approval for development of any changes to the application is not formally defined. • Requirements that security impact analyses be performed prior to implementation of changes have not been documented. • Limited testing requirements exist to guide FEMA personnel in the development of test plans and guidance over the testing that should be performed and documented. Additionally, roles and responsibilities over test plan procedures to ensure that plans are sufficient, document expected outcomes, and are reviewed and approved prior to	requirements for security impact analyses, test plan development, and approval for non-emergency and emergency change procedures.			

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	development, are not documented. • Requirements over emergency changes have not been defined in writing.				

Department of Homeland Security
FY 2010 Information Technology - Notice of Findings and Recommendations – Detail

- **Federal Law Enforcement Training Center**

Department of Homeland Security
Information Technology Management Letter
September 30, 2010

Notice of Findings and Recommendations – Detail
Federal Law Enforcement and Training Center

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
FLETC-IT-10-01	During our FY 2010 review of FLETC's configuration management policies and procedures, we noted that FLETC does not conduct the following: • Momentum and Glynco Area Network (GAN) changes are not being documented throughout the change control process from the testing of changes to the final approval of the changes prior to implementation, and; • Distribution and implementation of Momentum and GAN changes are not being controlled.	The FLETC management will update and enforce current procedures to ensure changes are fully documented throughout the change control process to include the results of testing the change, review of the change test results, and final approval to proceed with the implementation.	X		2
FLETC-IT-10-02	During the FY 2009 financial statement audit, we noted several weaknesses with the logical access controls for the Glynco Administrative Network (GAN). During our review in FY 2010, we reviewed the logical access controls over the GAN. Per our review, we noted that FLETC has remediated all of the logical access controls over the GAN; however, KPMG noted that the GAN was configured to reset the lockout counter after 20 minutes. This does not meet the DHS 4300A requirement of 24 hours. Upon notification, FLETC immediately remediated the configuration issue. However, the configuration was inappropriately configured for the majority of the fiscal year.	Due to remediation of this finding within the fiscal year, no recommendation is required.		X	3
FLETC-IT-10-03	In FY 2009, KPMG conducted After-Hours walkthrough testing to complement our IT audit testing efforts as part of the FY 2010 DHS Financial Statement Audit and Audit of Internal Control over Financial Reporting. We also performed after-hours	Finance Division, Building 66 Safeguarding of PII and Credit Card data: Modifications to Building 66 have recently been completed which provide secure file storage rooms and entry controls for all access points in the building. An SOP will be		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects include physical access to equipment that houses financial data and information residing on the desks of FLETC personnel, which could be used by others to inappropriately access financial information. For our review in FY 2010 follow up test work was performed at various FLETC buildings in the Glynco, Georgia complex. The designated FLETC Technical Point of Contact and representatives from the DHS Office of Inspector General, the DHS Office of Information Security, and the FLETC Office of Physical Security accompanied KPMG to monitor testing and validate the results. After gaining access to the facilities, we inspected a random selection of desks and offices, looking for items such as improper protection of system passwords, unsecured information system hardware, documentation marked FOUO, and unlocked network sessions. Our selection of desks and offices was not statistically derived, and therefore we are unable to project results to the component or department as a whole. We reviewed over 90 desks and cubicles within the four locations.	drafted to address Safeguarding of PII and Credit Card data in the Finance Division, implement use of the secure file storage rooms, and address entry controls for access points in the building. This will be developed and implemented by November 15, 2010. Additionally, specific requirements for Safeguarding of PII and Credit Card data will be added to each Finance Division employee's FY 2011 (and future) Annual Performance Work Plan to ensure there is no misunderstanding regarding each employee's responsibilities in this area. Finance Office, Building 66 User Name and Passwords: Remedial training will be conducted regarding safeguarding User Name and Passwords. Additionally, specific requirements for safeguarding User Name and Passwords will be added to each Finance Division employee's FY 2011 (and future) Annual Performance Work Plan to ensure there is no misunderstanding regarding each employee's responsibilities in this area. For the CIO Operations and Support Division (OSD) in Bldg 681, remedial training will be conducted to ensure employees and contractors lock their doors and safeguard sensitive information. OSD will ensure the workstation screensaver feature is enabled on its workstations.			
FLETC-IT-10-04	During the FY 2009 financial statement audit, KPMG determined that logs of auditable events in the Gylnco Administrative Network (GAN) are not being reviewed to identify potential incidents. During our FY 2010 review, KPMG determined that FLETC has implemented the Security Information	FLETC's current SIM solution provides no capability to correlate or aggregate audit logs which results in an arduous, un-trackable and unmanageable audit log review process when handling millions of records each day. FLETC is currently in the process of procuring ArcSight ESM as a replacement SIM solution to address		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	Management System (SIM) with capabilities to manage and store logs of auditable events. However, we determined that management does not have a formal process for reviewing the audit logs on a periodic basis.	these and other shortcomings with the current solution. ArcSight ESM allows for both simplified and exceptionally complex event correlation rule authorship. FLETC will deploy the ArcSight ESM solution during FY 2011. Users, such as ISSOs, will be provided focused dashboards with correlated information pertinent to their areas of responsibility. Audit logs will be reviewed as correlated and aggregated data and can be drilled down to in detail and reviewed when suspicious or anomalous records are found. Customized reports and automated alerts will be configured for each system and tailored for the audit log reviewer. Audit logs of access to the SIM itself will also be generated and reviewed to ensure users such as ISSO's and the SOC are utilizing the system and reviewing audit records and responding to the configured automated alerts in a timely manner.			
FLETC-IT-10-05	During the FY 2009 financial statement audit, KPMG determined that access control weaknesses existed over Momentum access authorizations for user's profiles created or modified during the fiscal year. During the FY 2010 financial statement audit, KPMG determined that access control weaknesses still existed over Momentum access authorizations for user's profiles created or modified during the fiscal year. Specifically, we learned that new users and profile changes are not being tracked by FLETC.	FLETC has implemented profile logging, however, due to the overwhelming volume of events logged by the system, this has proven to be unusable in terms of identifying relevant activity. FLETC is working to better analyze and manage the profile logging reports. An SOP will be drafted to implement management oversight for Momentum access authorizations for user's profiles created or modified during the fiscal year. This process will be developed and implemented by November 30, 2010.		X	3
FLETC-IT-10-06	During the FY 2009 financial statement audit, we noted several weaknesses around access controls for the Student Information System (SIS) including:	The FLETC will update the existing Risk Acceptance to include the password exceptions noted in the condition above.		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	• SIS is configured to have a password history of two passwords stored. • SIS is not configured to reset the account failed logon counter • Users were not locked out after three invalid access attempts. • SIS system administrators share a 'root' username and password to perform administrative responsibilities. • A sample of audit logs that track changes to system data could not be provided. • User profile creation is not tracked and a listing of profile creation dates could not be provided. • Evidence of periodic review of user accounts could not be provided. In FY 2010, we inquired with FLETC and noted that although some corrective actions have taken place, the following has not yet been implemented. • Users are not being locked out after 3 invalid attempts. • SIS password length minimum is configured a minimum of six. • SIS does not require a combination of alphabetic, numeric, and special characters. • Audit logs that track changes to system data are not being reviewed. • Profile creation and changes are not being tracked and a listing of profile updates could not be provided. • Periodic review of user accounts is not being conducted.				

Department of Homeland Security
FY 2010 Information Technology - Notice of Findings and Recommendations – Detail

▪ Immigration and Customs Enforcement

Department of Homeland Security
Information Technology Management Letter
September 30, 2010

Notice of Findings and Recommendations – Detail
Immigration and Customs Enforcement

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
ICE-IT-10-01	During the FY 2009 financial statement audit, KPMG performed an inspection of a sample of personnel that had terminated/transferred from their employment with ICE during the fiscal year. KPMG requested evidence that exit clearance forms were completed for each employee to determine ICE management's compliance with exit clearance procedures. Of the 25 terminated/transferred ICE personnel sampled, evidence of compliance with exit clearance procedures could not be provided for 12 employees. During the FY 2010 financial statement audit, KPMG was informed that a policy and procedure has not been developed for the Personnel Exiting Process. ICE management stated that the Office of Human Capital (OHC) has implemented a multi-year mission action plan to address this and various other issues, but there has been no corrective action taken at this time.	ICE should establish and implement a policy governing the exit clearance process, identifying the procedures separating employees and contractors must take to ensure the return and\or safeguarding of government property, equipment, and systems; and the roles and responsibilities of ICE offices involved in the exit clearance process.		X	3
ICE-IT-10-02	During the FY 2009 audit, KPMG inquired of ICE OCIO personnel about FFMS password settings. We determined that the FFMS password settings require the use of an underscore and does not allow the use of any other special characters such as !, @, #, $, %, or *, which is not compliant with DHS policy. The DHS policy requires that passwords contain a combination of alphabetic, numeric, and special characters. During the FY 2010 audit, we performed follow-up inquiry to determine the status of this weakness and learned that the FFMS password setting control weakness has not been remediated. ICE management	ICE should update the FFMS password configuration settings to ensure that they are in compliance with DHS 4300A policies.		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	stated that a change to the system has been requested to include two additional characters in the password complexity. The special characters that will be added once the change is implemented are the #, $, and underscore. KPMG noted that Oracle uses the following characters (!, @, %, ^, &, *) as function key, therefore, they cannot be included in the password complexity. The remediation completion date is scheduled for November 2010.				
ICE-IT-10-03	During the FY 2009 audit, KPMG inquired of ICE OCIO personnel about the process for recertifying FFMS user access (review of access privileges) and found that this process is not formally documented. Furthermore, KPMG found that the review for the access privileges for each FFMS account is not adequately recorded and no audit trail is available to support that a recertification was completed. During the FY 2010 financial statement audit, we performed follow-up inquiry to determine the status of this weakness and learned that procedures have been documented and implemented for the FFMS recertification process, however, a formal policy has not been documented. KPMG found that users' logical access privileges were reviewed, recorded, and maintained, therefore this portion of the PY NFR as been remediated. However, per inquiry with ICE management, KPMG found that a formal policy still does not exist for the recertification of FFMS accounts.	ICE management should establish and implement policies and procedures to formally document the recertification of FFMS user privileges. This activity is the responsibility of OFM and the ISSO. This process should include a method to document user recertification and a process to maintain evidence of the reviews.		X	
ICE-IT-10-04	During the FY 2009 financial statement audit, KPMG performed an inspection of a listing of FFMS users and their assigned roles/responsibilities and determined that six users had Originator, Funds Certification Official, and Approving Official profiles	ICE should enforce policies and procedures to ensure that assigned roles and responsibilities are commensurate with personnel job functions.		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	that were in violation of FFMS segregation of duties policies. During the FY 2010 financial statement audit, we performed follow-up inquiry to determine the status of this weakness and learned that draft FFMS segregation of duty policy is in place, but, is not being followed. In addition, KPMG inspected a listing of FFMS users and their assigned roles/responsibilities and determined that one user had Originator, Funds Certification Official, and a Approving Official profile, which is a violation of the FFMS segregation of duties policy.				
ICE-IT-10-05	During the FY 2010 financial statement audit, KPMG determined that FFMS audit logs were not generated or reviewed during the period October 2009 through February 2010. As of March 2010, the logs were generated and reviewed, however, no supporting evidence could be provided. Additionally, we determined that audit log policy and procedures have been drafted, however, they have not been finalized, approved, and implemented.	ICE Office of Financial Management (OFM) will finalize, seek approval, and formally implement the draft policy and procedures. In the meantime, the draft policy will be used to provide an accurate audit log.	X		3
ICE-IT-10-06	During the FY 2009 financial statement audit, KPMG determined that weaknesses exist over ADEX access. Specifically, KPMG found that 14 users, which were separated from ICE, still had active ADEX accounts that were not removed upon their termination/transfer. During the FY 2010 financial statement audit, we performed follow-up inquiry to determine the status of this weakness and learned that ICE has implemented a compensating control that will disable users account after 45 days of inactivity to mitigate the control weakness. However, KPMG found that a separated	Ensure implementation of the ICE Exit Clearance Directive which will establish the process for separating employees, both Federal and contractors, and formalize a process to ensure that separating employees have their access to all ICE information technology systems removed.		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	employee's account was not disabled in a timely manner as the account was accessed after the employee's termination date. Therefore, the 45-day window was inappropriately delayed. In addition, we determined that DHS access controls policies are not being followed as users are not properly identified and authenticated. Based on ICE management's response to this weakness "either another user logged on as the terminated user or Information Technology Field Officer (ITFO) logged in using the terminated employee's credentials."				
ICE-IT-10-07	During the FY 2010 financial statement audit, KPMG determined that several physical and environmental controls exist within the OCS Datacenter. Specifically, we noted the following: • OCS Data Center Risk Assessment is not documented. • Re-entry procedures for personnel after an emergency evacuation are not documented. • Fire suppression testing documentation is not maintained. • Water damage was visible on the data center wall where FFMS servers are housed with no incident report of the event. • UPS testing documentation is not maintained.	As of July 2010 FFMS has been moved from the Department of Commerce OCS to Data Center 2 (DC2). DC2 will be reviewed and monitored to ensure compliance with all physical and data security requirements.	X		2
ICE-IT-10-08	During the FY 2010 financial statement audit, we determined that the environmental controls in the PCN computer room need improvement. Specifically, we found that environmental test results are not documented and maintained for the following devices: AC units, fire extinguishers, and back-up power supply.	Ensure that environmental systems (Heat Ventilation Air Conditioner, fire extinguishers, and Universal Power Supply) are tested annually with test results made available for review.	X		2
ICE-IT-10-09	Social engineering is defined as the act of attempting to manipulate or deceive people into taking action that is inconsistent with DHS policies, such as divulging sensitive information or allowing/enabling	Social Engineering is covered in the Annual Information Assurance Awareness Training (IAAT) – which is a requirement for all ICE employees. The IAAT should continue to stress		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	computer system access. The term typically applies to trickery or deception for the purpose of information gathering, or computer system access. During the course of our social engineering test work, the objective was primarily focused on attempting to identify user IDs and passwords. Posing as DHS technical support employees, attempts were made to obtain this type of account information by contacting randomly selected employees by telephone. A script was used to ask for assistance from the ICE user in resolving a network issue in the component. For each person we attempted to call, we noted whether the individual was reached and whether we obtained any information from them that should not have been shared with us according to DHS policy. Our selection of desks and offices was not statistically derived, and therefore we are unable to project results to the component or department as a whole. During the FY 2010 financial statement audit, we learned that ICE continues to promote security awareness training by distributing a weekly newsletter to employees and contractors about security awareness. However, KPMG found that the prior year security weakness still exists.	social engineering risks and greater outreach should be achieved.			
ICE-IT-10-10	We performed after-hours physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects include physical access to equipment that houses financial data and information residing on an ICE employee's desk which could be used by others to inappropriately access financial information. The testing was performed at various ICE locations that process and/or maintain component financial data. After gaining access to the facilities via an ICE	Security Awareness is covered in the Annual IAAT – which is a requirement for all ICE employees. The IAAT should continue to stress security awareness risks and greater outreach should be achieved.	X		3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	employee designated to assist with and monitor our testwork, we inspected a random selection of desks and offices looking for items such as improper protection of system user names and passwords, unsecured information system hardware, documentation containing PII or marked FOUO, and unlocked network sessions. Our selection of desks and offices was not statistically derived, and therefore we are unable to project results to the component or department as a whole. For each location visited, we noted the type of unsecured information or property we identified and included the total exceptions noted by location, as well as by type of information or property identified. During the FY 2010 financial statement audit, we learned that ICE continues to promote security awareness training and distributes a weekly newsletter to employees and contractors about security awareness. However, KPMG found that security weaknesses still exist.				
ICE-IT-10-11	In FY 2009, we found that ICE lacked policies and procedures requiring completion of a training program by personnel in IT security positions. During the FY 2010 financial statement audit, we learned that to correct the prior year NFR, ICE follows DHS 4300A policy for training personnel in IT security positions, therefore, this portion of the NFR is closed. However, during our testwork we determined that weaknesses still exist over training personnel in IT security positions. Specifically, we determined that 27 out of 45 IT security personnel have not completed specialized training.	OCIO will provide management oversight and guidance for training personnel with significant responsibilities for information security.		X	2
ICE-IT-10-12	During the FY 2010 financial statement audit, KPMG determined that physical safeguard weaknesses exist at	ICE should ensure that re-entry procedures are properly documented at the Clarksville data center	X		2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	the DC2 datacenter. Specifically, we determined the following: • Re-entry procedures after an emergency have been implemented, however, the procedures are not documented. • FFMS server is inappropriately marked with a label that identifies the application/data on the server.	and make certain that servers are not inappropriately identified.			
ICE-IT-10-13	During KPMG's internal vulnerability assessment efforts of ICE's FFMS network, servers and databases performed in August 2010, KPMG identified several High/ Medium Risk vulnerabilities, related to configuration management such as: • Hot Standby Router Protocol (HSRP) default installation on Cisco routers and switches • Default "Oracle Listener Program (tnslsnr)" service password on server installation • Outdated Microsoft Operating Systems • Bonjour (also known as ZeroConf or mDNS) listening protocol • Remote web server HTML form fields transmits data in clear text	ICE should take the necessary steps to begin examining the default configuration installations and system services installed on FFMS devices and determine if the default configurations can be set to increase FFMS's security or, in the case of unnecessary system services, deleted to reduce FFMS vulnerability to attack.	X		3
ICE-IT-10-14	During KPMG's internal vulnerability assessment efforts of ICE's FFMS network servers and databases performed in August 2010, KPMG identified several High/ Medium Risk vulnerabilities, related to several configuration and patch management weaknesses within the configuration of the FFMS ICE and CIS Oracle database instances such as: • Clear text passwords stored in database • Outdated patches • Table security configurations • User account privileges	ICE should take the necessary steps to begin applying the appropriate FFMS database patches to ensure patch compliance.	X		3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	• Password settings for users and database				
ICE-IT-10-15	During KPMG's internal vulnerability assessment efforts of ICE's FFMS network servers and databases performed in August 2010, KPMG identified several High/ Medium Risk vulnerabilities, related to missing or inadequate patches such as: • Microsoft Patches • Adobe Reader • Apache Tomcat • Java Runtime Environment (JRE) • Oracle Database (server installation) • HP System Management • Internet Explorer • MySQL database	ICE should take the necessary steps to begin applying the appropriate FFMS patches to the FFMS network servers and databases to ensure patch compliance.	X		3
ICE-IT-10-16	During KPMG's internal vulnerability assessment efforts of ICE's ADEX network servers and devices performed in August 2010, KPMG identified a default installation and configurations for the HSRP on the Cisco routers.	ICE should ensure that password configuration settings are properly and effectively applied.	X		3

Department of Homeland Security
FY 2010 Information Technology - Notice of Findings and Recommendations – Detail

- **Office of Financial Management**
- **Office of Chief Information Officer**

Department of Homeland Security
Information Technology Management Letter
September 30, 2010

Notice of Findings and Recommendations – Detail
Office of Financial Management
Office of Chief Information Officer

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CONS-IT-10-01	During our follow-up on this prior year issue, we noted that the following password configurations for the DHS Internet domain, which controls access to the DHSTIER and CFO Vision, are not in compliance with DHS 4300A requirements: • The account lockout counter is configured to reset after 30 minutes rather than (24 hours as required by DHS policy; and • Workstation idle sessions termination is configured to lock workstations after 15 minutes of inactivity rather than 5 as required by DHS policy.	We recommend that DHSNET logical access configuration be aligned with DHS 4300A requirements concerning account lockout and workstation idle session termination.		X	1
OCIO-IT-10-01	DHS is in the process of becoming fully compliant with the Federal Desktop Core Configuration (FDCC) security configurations. Each DHS component agency has begun testing or implementing the FDCC security configurations; however, full compliance with FDCC security configurations for all DHS components is not planned to be completed until the end of FY 2011.	We recommend that the DHS OCIO: • Finalize the DHS Hardening Guides for Windows desktop operating systems and distribute them to all DHS component agencies. • Continue with the full implementation of FDCC security configurations across all DHS component agencies.		X	2
OCIO-IT-10-02	During the FY 2010 financial statement, we noted two weaknesses within DHS policies that require further evaluation and clarification. The following observations were noted for management consideration over access to PII and Segregation of Duties principles: • DHS Sensitive Systems Policy (DHS MD 4300A Section 3.14.1) refers to the DHS Handbook for Safeguarding Sensitive PII. We found that section 2.4.4 is too broad when assessing that when PII is	DHS should revise the DHS Handbook for Safeguarding Sensitive PII to clarify that access to PII be restricted to those with a need to know. DHS should revise DHS 4300A Policy and Handbook, 7.1.1, Section 5.3 Auditing, to clarify that the review of logs should be independent adhering to segregation of duties principles.	X		1

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	physically secure; all staff with access to the workspace have a "need to know" and can access the PII. • A violation of segregation of duties exists within the DHS 4300A Section Version 7.1.1, Section 5.3 Auditing. The policy allows the system administrator to review the audit records for financial systems or for systems hosting or processing PII on a monthly basis. The review of the audit logs should be independent (e.g., system administrator of a separate application, security administrator) since the system administrator typically has full access rights and the authority to make changes to the system that may go unnoticed.				

Department of Homeland Security
FY 2010 Information Technology - Notice of Findings and Recommendations – Detail

▪ Transportation Security Administration

Department of Homeland Security
Information Technology Management Letter
September 30, 2010

Notice of Findings and Recommendations – Detail
Transportation Security Administration

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
TSA-IT-10-01	To complement our IT audit testing efforts as part of the FY 2010 DHS Integrated Audit, we also performed social engineering and after hours physical security testing During our testing we identified the following During our after-hours physical security testing, we identified one instance of an unsecured laptop computer; During our social engineering testing, we were provided with three user's passwords.	We recommend TSA in the area of physical Security to: • Continue to execute the IT Security Awareness Training program; • Conduct internal Physical Security walkthrough on a bi-annual basis; • Conduct one-on-one training with individuals failing physical security after-hours testing; • Take administrative actions, if needed, on a case-by-case basis; and • TSA will conduct a communications campaign to address the effects of improper handling of Physical Security. We recommend TSA in the area of social engineering to: • Continue to execute the IT Security Awareness Training program; • Conduct internal Social Engineering testing on a quarterly basis; • Conduct one-on-one training with individuals failing social engineering attempts. • TSA will take administrative actions, if needed, on a case-by-case basis. • TSA will conduct a communications campaign via broadcast warning against social engineering.		X	1
TSA-IT-10-02	*Core Accounting System (CAS) & Financial Procurement Desktop (FPD)* During our FY 2010 IT test work, we determined that TSA had created an Internal Standard Operating Procedure (ISOP)	We recommend TSA to take the following corrective actions: CAS/FPD:		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	to detail how quarterly access reviews were to be performed. We compared a listing of TSA CAS and FPD users to the master listing of users who needed modifications or deletions for three quarters (Q1, Q2, and Q3). We did not identify any exceptions for Q1 and Q2; however, for the 3rd quarter, one CAS user was not deleted or modified within 50 days after the end of the completion of the 3rd quarter. In addition, we noted 115 FPD users were not deleted or modified within 51 days after the completion of the 3rd quarter. *Sunflower* During our FY 2010 test work, we determined that the Office of Property Management (OPM) performs monthly access reviews over Sunflower user accounts. OPM runs three Sunflower reports each month, and the Deputy Property Management Officials (DPMOs) and OPM Access Manager review the reports and provide dates and initials by each user reviewed. However, for the three months sampled, we determined that three Sunflower users, who had update privileges, had not had their access removed in a timely manner. All users were reviewed in January, but two were not removed until July, and the other user was not removed until August.	• Have FINCEN update its helpdesk procedures to provide the correct guidelines so that its helpdesk staff will no longer grant additional Standard FPD roles that were not requested on Account Access Request (AAR). TSA should closely monitor the requests implemented by FINCEN to ensure that the updated procedures are being followed. • TSA should improve the timeline and process of its Quarterly Review. TSA should update its procedures to monitor the timeliness, accuracy and quality of the Quality Review process. a. Update Quarterly Review ISOP to add the expected timeline to complete the quarterly review. b. Conduct timely follow-up and review of the actual FINCEN implementation of the AARs to ensure that the AARs were implemented as requested. • TSA should work with FINCEN to identify and implement the best solution to remove the one Sunflower role from the user's profile. • TSA should work with FINCEN to research and identify options to enhance the automated AAR process. Sunflower: • TSA will provide more training and oversight for any new access manager to ensure the process is thoroughly followed. • TSA will closely monitor and follow-up with FINCEN to ensure requests are implemented timely and correctly.			

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
		• TSA will review and identify alternate reporting processes in cases of technical difficulties where supervisors cannot access the master files on SharePoint.			
TSA-IT-10-03	During our FY 2010 audit test work, we selected a sample of the following forms required by the TSA directive and determined the following: • Form 1403 Computer Access Agreement: Per the TSA IT Security Policy Handbook, all TSA personnel, including contractors, are required to review and sign Form 1403: Computer Access Agreement upon commencement of working for the agency. Our testing noted that of the five forms sampled, one form was completed one month after the user was granted access to a TSA system.	We recommend that TSA take the following corrective action: Supervisors and Contracting Officer's Technical Representatives within each program office in TSA should ensure, as required by the IT Security Policy Handbook, that evidence be maintained on file for each TSA employee and contractor the Computer Access Agreement form, signed prior to any financial system access is granted.		X	1
TSA-IT-10-04	During the FY 2010 IT audit, we determined that TSA has fully implemented the TSA ISOP: Process for Validation of Controls over the USCG Script Process to monitor scripts run at FINCEN. Specifically, we noted that TSA has implemented an extensive review of the scripts that impact TSA on a weekly, monthly, quarterly and ad hoc basis. Additionally, a baseline review was performed to ensure that all scripts that were run in production prior to 4/1/2010, this was approximately 160 scripts and that they were reviewed for their purpose and the financial impact of the scripts were understood by the various stakeholders in the script review process, which included the Script Technical Lead, Script Module Leads (SMLs), and Subject Matter Experts (SMEs). Any script that was not included in the baseline review was considered new and was included in the weekly, monthly, quarterly and ad hoc review process. The reviews conducted by TSA included validation and verification steps to ensure that the Coast Guard is properly tracking the TSA scripts and that those scripts go through the proper configuration management processes.	We recommend that TSA work with the DHS Chief Financial Officer and the DHS Chief Information Officer to ensure that Coast Guard Headquarters' completes, in a timely manner, the planned corrective actions to: • Update the scripting policies and procedures to include additional and more detailed test documentation; • Develop training that addresses all aspects of script testing (including documentation of test documents) and provide training to appropriate CM staff; • Develop an RP with associated supporting business case(s) to address the database audit logging requirements; • Develop procedures and perform regular account revalidation for Serena to ensure privileges remain appropriate; and • Conduct an assessment over the ICFOR process related to identifying and evaluating	X		2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	We noted no exceptions during our testing of the TSA Script Configuration Management Oversight Process. Configuration Management Controls Over the Coast Guard Scripting Process The analysis conducted over the Coast Guard script configuration management process reflects the assessment of the control environment for the entire fiscal year. Weaknesses identified over the process are risks that existed in the environment from October 2009 to September 2010 unless otherwise noted. • Based upon follow-up test work performed in FY 2010, we determined that some previously noted weaknesses were remediated (particularly in the second half of FY 2010), while other control deficiencies continued to exist. The remaining control deficiencies that were present throughout FY 2010 vary in significance, however three key areas that impact the Coast Guard Script control environment are: 1) Script Testing Requirements, 2) Script Testing Environment, and 3) Script Audit Logging Process. - Script Testing Requirements: Limited testing requirements exist to guide FINCEN staff in the development of test plans and guidance over the functional testing that should be performed. Additionally, we determined that there are no detailed requirements over the review and testing of functional changes to the data. FINCEN only tracks and documents the number of transactions updated on scripts that have a financial impact and not the detailed dollar amounts associated with the financial impact transactions.	scripts that have a financial statement impact. This assessment can be included in the Configuration Management Oversight Process as part of Coast Guard's annual A-123 efforts or performed independent of the A-123 process. We recommend that this assessment (1) be performed early in the FY 2011, in time to remediate deficiencies before the end of the third quarter, and (2) involve process documentation and sufficient testing to fully assess both design and operating effectiveness of controls. The objective being to have a reliable process and internal controls in place that allow the auditor to test, and rely on those controls, during the fourth quarter of FY 2011. TSA Specific Recommendation: Continue to conduct an assessment over the ICFOR process related to identifying and evaluating scripts that have a financial statement impact. Findings will be communicated and coordinated with USCG, as appropriate. This assessment can be included in the testing of the TSA Script Configuration Management Oversight Process as part of TSA's annual A-123 efforts. Further, we recommend that this assessment (1) be performed early in the FY 2011, in time to remediate deficiencies before the end of the third quarter, and (2) involve process documentation and sufficient testing to fully assess both design and operating effectiveness of controls. The objective being to have a reliable process and internal controls in place that allow the auditor to test, and rely on those controls, during the fourth quarter of FY 2011.			

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	- Script Testing Environment: Not all script changes were tested in the appropriate CAS Suite test environments as required. FINCEN management informed us that the testing environments, CAS4 and LUFSFQT3, were offline for these exceptions due to a refresh of the databases and that testers used CAS3 and Alpha as alternate testing environments instead. However, FINCEN management informed KPMG that these environments are refreshed on an as needed basis and no further information could be provided over how frequently the CAS3 and Alpha databases were refreshed to verify that the scripts were adequately tested in the appropriate environment. Furthermore, we determined that guidance is not provided over the use of alternate testing environments for the testing of scripts to ensure they are adequately tested. - Script Audit Logging Process: The CAS, FPD, and Sunflower databases are logging changes to tables as well as successful and unsuccessful logins. However, no reconciliation between the scripts run and the changes made to the database tables is being performed to monitor the script activities and ensure that all scripts run have been approved through change management script system (CMSS) or Serena. In addition, we noted that FINCEN has not established a formal process to monitor and review changes made to the Sunflower database including the tables and activities modified by the database administrators. Internal Control Over Financial Reporting – Financial Statement Impact. The USCG has established certain processes to identify and assess the validity of scripts that may have a financial				

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	statement impact [on both USCG and TSA financial statements]. This process is performed by one primary individual, and two identified backup personnel, who performs a review of the script for accuracy and propriety, provides feedback to the source, and ultimately approves the application. This process has certain control deficiencies that have been communicated to USCG (see NFR # CG-IT-10-05), which have lead, in part, to TSA's adoption of certain redundant controls to review TSA scripts for propriety. Furthermore, the rationale documenting the impact of the script, whether deemed as having financial impact or not, is not documented and retained. In addition, within the CAS Suite environment, there are over 200 scripts run on a weekly basis. During FY 2010, through this review TSA has discovered various errors that USCG was required to correct. The exceptions noted by TSA are indicative of weaknesses in the USCG process. We also consider this control aspect to be principally important for TSA to monitor Coast Guard's corrective actions taken. In addition, TSA should consider, as part of their annual A-123 efforts, adding their own A-123 testing procedures in identifying and evaluating the financial impact of TSA scripting at the Coast Guard.				

Department of Homeland Security
FY 2010 Information Technology
Notification of Findings and Recommendations – Detail

- **United States Citizenship and Immigration Services**

Department of Homeland Security
Information Technology Management Letter
September 30, 2010

Notice of Findings and Recommendations – Detail
United States Citizenship and Immigration Services

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CIS-IT-10-01	During the FY 2010 financial statement audit, we performed inquiry follow-up to determine the status of this weakness and learned that the access roles at the National Benefits Center (NBC) for CLAIMS3 LAN have not be defined and documented. USCIS has begun some corrective action; however, these issues have not been fully remediated.	The USCIS Office of Information Technology will finalize the CLAIMS 3 LAN Account Management Procedures that address account identification, set-up, recertification, and termination and access request form maintenance. These procedures reflect how all CLAIMS 3 LAN accounts will be managed at each facility that utilizes the CLAIMS 3 LAN.		X	3
CIS-IT-10-02	During the FY 2010 financial statement audit, we performed inquiry follow-up to determine the status of this weakness and learned that the weakness has not been remediated for CLAIMS3 LAN periodic user access reviews. USCIS has begun some corrective action; however, these issues have not been fully remediated.	The USCIS OIT will continue to review CLAIMS 3 LAN accounts for those that have been inactive for 45 days manually and to remove user's that appear on the Office of Human Capital and Training (HCT) attrition bi-weekly list. OIT will finalize the CLAIMS 3 LAN Account Management Procedures that address account identification, set-up, recertification, and termination and access request form maintenance. OIT will continue to work with the OIT Account Management Group, the IT Project Manager and each installation site to recertify CLAIMS 3 LAN accounts and ensure a current and valid access request form is filed. OIT will continue to work with HCT to ensure their exit clearance process includes procedures to promptly notify OIT when employees leave or transfer. OIT will also finalize the USCIS Account Management, Management Directive (Agency Policy).		X	3
CIS-IT-10-03	During the FY 2010 financial statement audit, we performed inquiry follow-up to determine the status of the prior year NFR and learned that the weakness still exist for incomplete or inadequate access request forms for CLAIMS 3 LAN and CLAIMS 4. USCIS	The USCIS OIT will finalize the CLAIMS 3 LAN and CLAIMS 4 Account Management Procedures that address account identification, set-up, recertification, and termination and access request form maintenance. OIT will continue to work		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	has begun some corrective action; however, these issues have not been fully remediated.	with the OIT Account Management Group, the IT Project Manager and each installation site to recertify CLAIMS 3 LAN and CLAIMS 4 accounts and ensure a current and valid access request form is filed.			
CIS-IT-10-04	In FY 2009, KPMG performed an inspection of a sample of personnel that had terminated/transferred from their employment with USCIS during the fiscal year. KPMG requested evidence that exit clearance forms were completed for each employee to determine USCIS management's compliance with termination/transfer procedures. Of the 28 terminated/transferred USCIS personnel sampled, evidence of compliance with exit clearance procedures could not be provided for 19 employees. During the FY 2010 financial statement audit, we learned that USCIS Human Resource Division revised the existing terminated/transferred procedures for exit processing; however, the procedures have not been approved nor implemented.	We recommend USCIS management issue and adhere to exit clearance policies and procedures to be followed in the event of transfer, termination or separation of federal and contract personnel. Resources should be made available to communicate the updated procedures to personnel, train mission support staff who have a critical role in the updated process, and enforce and monitor compliance with the exit procedures and policies.		X	2
CIS-IT-10-05	During the FY 2010 financial statement audit, we performed inquiry follow-up to determine the status of this weakness and learned that equipment and media policies and procedures are not current. USCIS has begun some corrective action; however, these issues have not been fully remediated.	The USCIS OIT will finalize the USCIS Media Protection Management Directive and the USCIS Media Protection Procedures and ensure they are readily available to USCIS personnel. OIT will continue to work with the Office of Administration to ensure there is a standardize process to label, track, sanitize, refurbish, and/or destroy USCIS media using approved equipment and software.		X	1
CIS-IT-10-06	During KPMG's internal vulnerability assessment of FFMS performed in August 2010, KPMG identified several High/ Medium Risk vulnerabilities, related to the following: • FFMS mainframe production databases were installed and configured without baseline security	USCIS will monitor the Mission Action Plans (MAP) of the associated ICE NFRs: IT-10-12, IT-10-13, IT-10-14, IT-10-15 and request periodic status updates.	X		3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	configurations, including the USCIS Oracle instance • FFMS servers have missing or inadequate patches In addition, we found physical safeguard weaknesses at the DHS DC2 data center, which impact USCIS operations. Specifically, we determined the following: • Re-entry procedures after an emergency have been implemented; however, the procedures are not documented. • FFMS server is inappropriately marked with a label that identifies the application/data on the server.				
CIS-IT-10-07	During the FY 2009 financial statement audit, KPMG performed inspection of the CLAIMS 4 password configuration settings. Per our inspection, KPMG determined that CLAIMS 4 has been configured to prohibit password reuse for 6 generations, which does not meet the DHS 4300A requirement of 8 password generations. During the FY 2010 financial statement audit, we performed inquiry follow-up to determine the status of this weakness and learned that the weakness has not been remediated for CLAIMS4 password configuration. USCIS has begun some corrective action; however, these issues have not been fully remediated.	The USCIS OIT will continue to evaluate the risk imposed on the CLAIMS 4 system by not changing the password history from 6 to 8. If it is deemed that the risk is low, OIT will submit a Waivers and Exceptions Request Form to the DHS CISO. If the risk is deemed medium or high, OIT will continue to implement the password changes as outlined in the FY 2009 USCIS OIT MAP.		X	2
CIS-IT-10-08	During the FY 2010 financial statement audit, we performed inquiry follow-up to determine the status of this weakness and learned that ineffective safeguards still exist over physical access to sensitive facilities and resources. USCIS has begun some corrective action; however, these issues have not been fully remediated.	The USCIS OIT will continue to finalize the Media Protection Procedures for the Vermont Service Center. OIT will test VSC's OIT Visitor Policy and Procedures to ensure they address the physical security concerns listed in the condition statement.		X	1
CIS-IT-10-09	In FY 2009, we determined that the USCIS lacks policies and procedures over audit logging of application and server audit logs for CLAIMS 3 LAN	OIT will continue to finalize the USCIS Audit and Accountability Management Directive and implement enterprise audit logging software. OIT		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	and CLAIMS 4 system. Specifically, we learned that CLAIMS3 LAN generates audit logs; however, the USCIS does not require that the logs are reviewed or maintained. In addition, we determined that the USCIS does not have policies or procedures in place for maintaining and reviewing the audit logs. For CLAIMS4, we noted that Computer Service Corporation (CSC) contractors capture and review the logs of user access to CLAIMS4; however, no reviews of significant changes in the application or to system files are conducted. Additionally, no policies or procedures have been established for conducting and monitoring the audit log reviews. During the FY 2010 financial statement audit, we learned that USCIS has begun some corrective action; however, these issues have not been fully remediated. Therefore, this finding is being reissued.	will ensure CLAIMS 3 LAN and CLAIMS 4 audit logs are provided to the enterprise audit logging software for analysis. Once the integration of CLAIMS 3 LAN and CLAIMS 4 and the enterprise audit logging software is complete, develop CLAIMS 3 LAN and CLAIMS 4 audit and accountability procedures.			
CIS-IT-10-10	During the FY 2010 financial statement audit, we performed inquiry follow-up to determine the status of this weakness and learned that weak logical access controls still exist over CLAIMS 4. USCIS has begun some corrective action; however, these issues have not been fully remediated.	The USCIS Office of Information Technology (OIT) will finalize the CLAIMS 4 Account Management Procedures that address account identification, set-up, recertification, and termination and access request form maintenance. OIT will continue to work with the OIT Account Management Group, the IT Project Manager and each installation site to recertify CLAIMS 4 accounts and ensure a current and valid access request form is filed. OIT will also finalize the USCIS Account Management, Management Directive (Agency Policy). OIT will continue to review CLAIMS 4 accounts for those that have been inactive for 45 days manually and to remove users that appear on the Office of HCT attrition bi-weekly list. OIT will continue to work with HCT to ensure their exit		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
		clearance process includes procedures to promptly notify OIT when employees leave or transfer. The HCT must finalize Exit Clearance Process policies and procedures and ensure that these documents are disseminated agency-wide. Specifically, ensure that contracting officers, contacting officers' technical representatives, managers and supervisors are informed about these documents and understand their importance.			
CIS-IT-10-11	During the FY 2010 financial statement audit, we performed inquiry follow-up to determine the status of this weakness and learned that CLAIMS3 LAN still lacks policy and procedures for separated employees. USCIS has begun some corrective action; however, these issues have not been fully remediated.	The USCIS OIT will continue to review CLAIMS 3 LAN accounts for those that have been inactive for 45 days manually and to remove user's that appear on the Office of HCT attrition bi-weekly list. OIT will finalize the CLAIMS 3 LAN Account Management Procedures that address account identification, set-up, recertification, and termination and access request form maintenance. OIT will continue to work with HCT to ensure their exit clearance process includes procedures to promptly notify OIT when employees leave or transfer. OIT will also finalize the USCIS Account Management Directive (Agency Policy). The HCT must finalize Exit Clearance Process policies and procedures and ensure that these documents are disseminated agency-wide. Specifically, ensure that contracting officers, contacting officers' technical representatives, managers and supervisors are informed about these documents and understand their importance.		X	2
CIS-IT-10-12	During the FY 2010 financial statement audit, we learned that the IT security awareness training weakness has not been remediated, therefore, this finding was reissued.	For initial information security awareness training, OIT will continue to update and provide training materials for the Office of HCT New Employee Orientation Program (NEOP). The HCT should		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
		continue to implement the NEOP agency-wide. HCT must provide OIT a monthly report of all new hires and the date they completed initial information security awareness training during NEOP. For annual information security awareness refresher training, OIT will continue to use the Department of Status (DOS) Computer Security Awareness Training (CSAT) tool to provide information security awareness training to all USCIS employees with access to agency information systems.			
CIS-IT-10-13	During roll forward testing for the FY 2010 financial statement audit, KPMG performed inspection of Active Directory and Exchange (ADEX) access request forms. Per our inspection, KPMG determined that one out of the forty-five access forms requested was not provided. Additionally, three out of the forty-five access forms requested were created on the same day of the request.	The Office of Information Technology will finalize and issue the USCIS MD on Information System Account Management. The MD stipulates polices on records management of access requests and standardizes the USCIS Network Access Request Form.	X		2
CIS-IT-10-14	ICE - During KPMG's internal vulnerability assessment efforts of ICE's ADEX network servers and devices performed in August 2010, KPMG identified a default installation and configurations for the HSRP on the Cisco routers. USCIS - Although USCIS does not have direct responsibility for the controls over ADEX and ICE financial applications, USCIS does have a responsibility to proactively manage its service provider relationship with ICE. USCIS should require ICE to provide a detailed Corrective Action Plan (CAP) containing the planned remediation of the security vulnerabilities affecting USCIS data integrity.	USCIS will monitor the MAP of the associated NFR# ICE-IT-10-16 and request periodic status updates.		X	3

Department of Homeland Security
Information Technology Management Letter
September 30, 2010

APPENDIX C

Status of Prior Year Notices of Findings and Recommendations and Comparison to Current Year Notices of Findings and Recommendations at DHS

Department of Homeland Security
Information Technology Management Letter
September 30, 2010

Current Year Notices of Findings and Recommendations

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
CBP-IT-09-03	Contractor Tracking Deficiencies	X	
CBP-IT-09-12	[redacted] Install		10-11
CBP-IT-09-13	Complete List of CBP Workstations		10-11
CBP-IT-09-21	Review of Changes to Security Profiles in ACS		10-14
CBP-IT-09-27	[redacted] Administrator Access Authorization Weaknesses	X	
CBP-IT-09-29	Completion of CF-241 Forms for Terminated Employees		10-09
CBP-IT-09-34	Installation of Anti-Virus Protection		10-11
CBP-IT-09-41	Weaknesses in the Process of Separating CBP Contractors		10-08
CBP-IT-09-44	Completion of Non Disclosure Agreements for US CBP Contractors		10-10
CBP-IT-09-45	Log configuration weakness for [redacted] System.	X	
CBP-IT-09-48	Lack of Effective ACS Access Change Log Review Procedures		10-19
CBP-IT-09-56	ACE Audit Log Reviews		10-03
CBP-IT-09-57	NDC LAN Audit Logs	X	
CBP-IT-09-58	Novell Password Settings	X	
CBP-IT-09-59	Formal Procedures for Mainframe System Utility Logs	X	
CBP-IT-09-60	Configuration for Mainframe Security Violation Control Option		10-20
CBP-IT-09-61	Completion of Initial Background Investigations and Periodic Background Reinvestigations for CBP Employees and Contractors		10-21
CBP-IT-09-62	Rules of Behavior Not Consistently Signed by CBP Employees and Contractors	X	
CBP-IT-09-63	ACE does not disable accounts after 45 days	X	
CBP-IT-09-64	ACS PGA ISAs Not Completely Documented		10-16
CBP-IT-09-65	Documentation of ACE Access Change Requests		10-06
CBP-IT-09-66	Separated Employees on ACE Access Listing		10-01
CBP-IT-09-67	Inadequate Documentation of ACS Access Change Requests		10-17
CBP-IT-09-68	Vulnerabilities in Configuration and Patch Management	X	
CBP-IT-09-69	Inadequate SAP Profile Change Review	X	
CBP-IT-09-70	Overuse of ACS Emergency/Temporary Access Roles	X	
CBP-IT-09-71	Inadequate Documentation of SAP Emergency/Temporary Access Requests	X	
CBP-IT-09-72	ACE Segregation of Duties Controls are Not In Place		10-02
CBP-IT-09-73	Inadequate Documentation of ACE SCO Access Requests and Approvals	X	
CBP-IT-09-74	Inadequate Protection of CBP Information and Property		10-05 10-07
CG-IT-09-10	Contractor Background Investigation Weakness		10-02
CG-IT-09-14	Weaknesses with Specialized Role-based Training for Individuals with Significant Security Responsibilities		10-10
CG-IT-09-23	Shore Asset Management (SAM) Audit Log Review Weakness		10- 22
CG-IT-09-25	WINS Access Controls Need Strengthening	X	
CG-IT-09-31	Weaknesses Exist in the Configuration Management Controls		10-05

	Over the Scripting Process		
CG-IT-09-32	Lack of Documented Contractor Tracking System Reconciliation Procedures	X	
CG-IT-09-33	Lack of a Consistent Contractor, Civilian, and Military Account Termination Process for Coast Guard Systems		10-01
CG-IT-09-34	WINS Change Control Weakness	X	
CG-IT-09-40	Civilian Background Investigation Weakness		10-03
CG-IT-09-42	Non-Compliance with Federal Financial Management Improvement Act (FFMIA) – Information Technology		10-24
CG-IT-09-43	Recertification Weakness within the User Management System (UMS)	X	
CG-IT-09-45	FINCEN data center access is not restricted to appropriately authorized personnel	X	
CG-IT-09-46	Configuration and Patch Management - Vulnerability Assessment	X	
CG-IT-09-49	JUMPS Audit Log Review Weakness	X	
CG-IT-09-50	Audit Trail Weaknesses within the Direct Access Application		10-28
CG-IT-09-51	Audit Trail Weaknesses within the Global Pay Application	X	
CG-IT-09-52	Recertification Weakness within the Direct Access Application		10-12
CG-IT-09-53	Security Awareness Issues Associated with the Protection of Sensitive Information		10-06
CIS-IT-09-01	Inefficient definition and documentation of access roles at the National Benefits Center for CLAIMS3 LAN		10-01
CIS-IT-09-02	Periodic user access reviews are not performed for CLAIMS3 LAN users.		10-02
CIS-IT-09-03	Incomplete or inadequate access request forms for CLAIMS3 LAN and CLAIMS4 system users.		10-03
CIS-IT-09-04	Periodic Active Directory (ADEX) system administrator access reviews are not performed at USCIS.	X	
CIS-IT-09-06	Weak data center access controls exist	X	
CIS-IT-09-07	Equipment and media policies and procedures are not current.		10-05
CIS-IT-09-08	Weak access controls for security software exist within the Password Issuance and Control System (PICS).	X	
CIS-IT-09-09	Weak access controls exist in CLAIMS3 LAN.	X	
CIS-IT-09-10	Weak password configuration controls around CLAIMS4.		10-07
CIS-IT-09-11	Background investigations are not conducted in a timely manner.	X	
CIS-IT-09-12	Procedures for transferred/terminated personnel exit processing are not finalized		10-04
CIS-IT-09-13	Ineffective safeguards over physical access to sensitive facilities and resources		10-08
CIS-IT-09-14	Weak access controls exist within FFMS	X	
CIS-IT-09-15	Lack of policies and procedures for CLAIMS 3 LAN and CLAIMS 4 audit logs		10-09
CIS-IT-09-16	Weak logical access controls exist over CLAIMS 4		10-10
CIS-IT-09-17	Training for IT security personnel is not mandatory	X	
CIS-IT-09-18	Lack of policies and procedures for separated CLAIMS3 LAN accounts		10-11
CIS-IT-09-19	IT Security Awareness Training compliance is not monitored		10-12
CIS-IT-09-20	Default installation and configuration of Cisco routers on ICE		10-14

	Network Impact USCIS Operations.		
CONS-IT-09-13	Evidence of Security Management Review of DHSTIER's Oracle Activity Audit Reports is Not Retained	X	
CONS-IT-09-14	CFO Vision Password Parameters are Not Configured in Accordance with DHS Policy		10-01
CONS-IT-09-15	Operating System Patch Management Procedures for DHSTIER and CFO Vision Not Documented.	X	
CONS-IT-09-16	Periodic Review of DHS Stennis Data Center Access Privileges is Not Performed	X	
FEMA-IT-09-02	Configuration Management Weaknesses on IFMIS, NEMIS, and Key Support Servers (vulnerability assessment finding)		10-41
FEMA-IT-09-03	Weaknesses Exist over Recertification of Access to IFMIS		10-14
FEMA-IT-09-06	Documentation Supporting the IFMIS User Functions Does Not Exist		10-49
FEMA-IT-09-12	NEMIS Access Controls Need Improvement		10-01
FEMA-IT-09-13	Employee Termination Process for Removing System Access Should be More Proactive		10-21
FEMA-IT-09-17	System Programmers Have the Ability to Migrate Code into the IFMIS Production Environment		10-39
FEMA-IT-09-19	Monitoring of NEMIS System Software Needs Improvement		10-04
FEMA-IT-09-22	Alternate Processing Site for NEMIS Has Not Been Established		10-02
FEMA-IT-09-24	NEMIS Backups Are Not Tested in Accordance with Policy		10-36
FEMA-IT-09-25	The NEMIS Contingency Plan Is Not Tested		10-20
FEMA-IT-09-28	NEMIS Configuration Management Process for Non-Emergency Changes Needs Improvement		10-62
FEMA-IT-09-29	NEMIS Emergency Change Process Needs Improvement		10-62
FEMA-IT-09-38	Segregation of Duties Not Enforced for Traverse	X	
FEMA-IT-09-39	Traverse Contingency Plan Not Tested and NFIP Disaster Recovery and COOP Needs Improvement		10-61
FEMA-IT-09-45	IFMIS User Access is not Managed in Accordance with Account Management Procedures		10-26
FEMA-IT-09-46	IFMIS System Interconnections Agreements Have Not Been Reauthorized	X	
FEMA-IT-09-48	Corrective Action over NEMIS Vulnerabilities is Not Formally Documented		10-33
FEMA-IT-09-50	Weaknesses Exist over IFMIS Application and Database Audit Logging		10-11
FEMA-IT-09-51	NEMIS Oracle Audit Logging is Not Tracked		10-09
FEMA-IT-09-52	Existing NEMIS Patch Management Guidance Needs to be Implemented		10-35
FEMA-IT-09-38	Segregation of Duties Not Enforced for Traverse	X	
FEMA-IT-09-39	Traverse Contingency Plan Not Tested and NFIP Disaster Recovery and COOP Needs Improvement		10-61
FEMA-IT-09-45	IFMIS User Access is not Managed in Accordance with Account Management Procedures		10-26
FEMA-IT-09-46	IFMIS System Interconnections Agreements Have Not Been Reauthorized	X	
FEMA-IT-09-48	Corrective Action over NEMIS Vulnerabilities is Not Formally Documented		10-33

FEMA-IT-09-50	Weaknesses Exist over IFMIS Application and Database Audit Logging		10-11
FEMA-IT-09-51	NEMIS Oracle Audit Logging is Not Tracked		10-09
FEMA-IT-09-52	Existing NEMIS Patch Management Guidance Needs to be Implemented		10-35
FEMA-IT-09-77	FEMA and NFIP Planning, Management and Communication Related to Financial Systems Development and Acquisition Projects Needs to be Improved		10-47
FEMA-IT-09-78	Weaknesses Exist in the NEMIS Configuration Management Process under the EADIS contract		10-62
FEMA-IT-09-79	Weaknesses Exist over Management of FEMA LAN Accounts		10-22
FEMA-IT-09-80	Vulnerability Assessments of the NFIP LAN is Inadequate		10-52
FEMA-IT-09-81	Improvements are Needed in Core and G&T IFMIS Internal Scanning Procedures and Processes		10-34
FEMA-IT-09-82	Core and G&T IFMIS Patch Management Weaknesses		10-32
FEMA-IT-09-83	EADIS NEMIS Access Restrictions to Program Directories Needs Improvement		10-51
FEMA-IT-09-84	PARS Database Security Controls are Not Appropriately Established		10-05
FEMA-IT-09-85	TRRP Password Configurations have not been Configured in Accordance with DHS Policy	X	
FEMA-IT-09-86	Weaknesses Exist over the Implementation of Traverse System Changes		10-60
FEMA-IT-09-87	Weaknesses Exist in FEMA's Incident Response Program		10-31
FEMA-IT-09-88	Weaknesses exist over access authorizations for TRRP		10-53
FEMA-IT-09-89	Weaknesses exist over FEMA Background Investigations for Federal Employees and Contractors		10-45
FEMA-IT-09-90	FEMA LAN Certification and Accreditation Package is not Adequate		10-28
FEMA-IT-09-91	FEMA Contractor Tracking Program is Inadequate		10-10
FLETC-IT-09-03	Momentum System Software is Not Logged or Reviewed	X	
FLETC-IT-09-26	System Engineering Lifecycle (SELC) is not finalized	X	
FLETC-IT-09-31	Configuration Management Weaknesses on the Procurement Desktop, Momentum, and GSS.	X	
FLETC-IT-09-33	Momentum Audit Logs are not Reviewed		10-04
FLETC-IT-09-34	GAN audit logs are not reviewed		10-05
FLECT-IT-09-35	Weak access controls around Momentum		10-02
FLETC-IT-09-36	Ineffective logical access controls over the Glynco Administrative Network		10-03
FLETC-IT-09-37	Physical Security and Security Awareness Issues Identified during Enhanced Security Testing		10-06
FLETC-IT-09-38	Ineffective logical access controls over SIS	X	
ICE-IT-09-11	Ineffective physical security controls at facility entrances	X	
ICE-IT-09-12	Ineffective/non-compliant account lockout counter settings	X	
ICE-IT-09-13	Ineffective password settings in FFMS		10-02
ICE-IT-09-14	Ineffective ADEX user access recertification process	X	
ICE-IT-09-15	Ineffective FFMS access recertification process		10-03
ICE-IT-09-16	Terminated/transferred personnel are not removed from ADEX in a timely manner		10-06

ICE-IT-09-17	Segregation of duty policies are not enforced in FFMS		10-04
ICE-IT-09-18	Background reinvestigations are not conducted in a timely manner for contractors.	X	
ICE-IT-09-19	Procedures for transferred/terminated personnel exit processing are not allowed.	X	10-01
ICE-IT-09-20	Training for IT security personnel is not mandatory		10-11
ICE-IT-09-21	Vulnerability Assessment - Network devices were installed with default configuration settings and protocols; inadequate patches; and weak/ generic passwords.		10-13 through 10-16
ICE-IT-09-22	Physical Security and Security Awareness Issues Identified during Enhanced Security Testing		10-09
ICE-IT-09-23	IT Security Awareness Training requirements are not enforced	X	
OCIO-IT-09-03	DHS has not fully implemented the FDCC security configurations requirements.		10-01
TSA-IT-10-20	TSA Computer Access Agreement Process		TSA-IT-10-03
TSA-IT-10-23	Configuration Management Controls Over the Coast Guard Scripting Process (Included a specific TSA condition)	X	
TSA-IT-10-28	Physical Security and Security Awareness Issues Identified during Enhanced Security Testing		TSA-IT-10-01
TSA-IT-10-29	CAS, FPD, and Sunflower Access Recertification		TSA-IT-10-02

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

Homeland Security

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General
Information Technology Audits

FROM: Peggy Sherry
Acting Chief Financial Officer

Richard Spires
Chief Information Officer

Robert West
Chief Information Security Officer

SUBJECT: Draft Audit Report - *Information Technology Management Letter for FY 2010 DHS Financial Statement Audit For Official Use Only (OIG Project No. OIG-11-037-ITA-MGMT)*

We have reviewed the Office of the Inspector General's (OIG) draft audit report, *Information Technology Management Letter (ITML) for FY 2010 DHS Financial Statement Audit*, dated December 9, 2010. We concur with the Financial Systems Security findings contained within your audit report.

The DHS Chief Information Officer (CIO) and Chief Financial Officer (CFO) continue to work jointly in ensuring the timely remediation of financial system security weaknesses and strengthening the Department's information systems controls environment. Major activities include:

- Issued the *FY 2010 Internal Control Playbook Management Assurance Process Guide* which includes DHS' approach to documenting and testing the design effectiveness of financial system Information Technology General Controls (ITGCs).
- Updated the CFO Designated Systems List for FY 2010 as a result of the ITGC A-123 assessments performed in FY 2009. The list specifies the financial systems that require additional management accountability to ensure effective controls exist over financial reporting.
- Developed and implemented modifications to the scope of A-123 assessments for FY 2010 to perform verification and validation procedures to ensure Plans of Action and Milestones (POA&Ms) address root causes of financial system security control deficiencies identified from the financial statement audits and Federal Information Security Management Act (FISMA) annual assessments. Validation and verification (V&V) procedures were performed at the following Components---U.S. Citizenship

and Immigration Services, Immigration and Customs Enforcement, Customs and Border Protection, Federal Law Enforcement Training Center, the DHS Management Directorate, and U.S. Secret Service. The V&V efforts consisted of a three-phased assessment approach:

1. Assess current state based on IT Notifications of Findings and Recommendations (NFRs) and OMB Circular A-123 assessment gaps;
2. Gain understanding of remediation activities and root cause analysis; and
3. Test design and operating effectiveness of remediated controls.

- Issued the FY 2010 DHS Information Security Performance Plan which includes the requirements to ensure key financial system security controls are tested annually and quality POA&Ms are developed and completed timely.
- Continued tracking of A-123 ITGC weaknesses through the weakness remediation metric on the FISMA Scorecard.
- Provided POA&M training which includes root cause analysis training to DHS Components.
- Improved process for tracking IT audit recommendations for classified systems to ensure traceability to POA&Ms in Classified TAF.

Additionally, in FY 2011, DHS has conducted individual risk assessments and required detailed briefings from all components contributing to the material weakness condition at the Department. The primary goals of these meetings were to determine audit readiness, evaluate the effectiveness of the corrective actions, and identify areas where additional reliance can be placed on automated controls.

The DHS CFO and CIO remain fully committed to working together to secure DHS financial systems and continue to raise the standards for ITGC's for securing all DHS financial systems information.

If you have any questions or would like additional information, please contact Emery Csulak, ISO, Compliance Director at (202) 357-6113 or Michael Wetklow, OCFO, Director Internal Control Program Management Office at (202) 447-5196.

Department of Homeland Security
Information Technology Management Letter
September 30, 2010

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 for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
DHS GAO OIG Audit Liaison
Chief Information Officer, Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, 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.