Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the FY 2009 DHS Integrated Audit

(Redacted)

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

OIG-10-110

August 2010

Office of Inspector General

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

Homeland Security

AUG 17 2010

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 2009 DHS financial statement audit as of September 30, 2009. It contains observations and recommendations related to information technology internal control that were summarized within the *Independent Auditors' Report*, dated November 13, 2009 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 2009 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated December 9, 2009; and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control or provide conclusion on 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

December 9, 2009

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, 2009, and the related statements of custodial activity for the years then ended (referred to herein as "financial statements"). We were also engaged to examine the Department's internal control over financial reporting (ICOFR) of the balance sheet as of September 30, 2009, and statement of custodial activity for the year then ended. We were not engaged to audit the statements of net cost, changes in net position, and budgetary resources, for the year ended September 30, 2009 (referred to herein as "other fiscal year [FY] 2009 financial statements"), or to examine internal control over financial reporting over the other FY 2009 financial statements. Because of matters discussed in our *Independent Auditors' Report*, dated November 13, 2009, the scope of our work was not sufficient to enable us to express, and we did not express, an opinion on the financial statements. In addition, we were unable to perform procedures necessary to form an opinion on DHS' ICOFR of the FY 2009 balance sheet and statement of custodial activity.

In connection with our FY 2009 engagement, we examined DHS' internal control over financial reporting by obtaining an understanding of DHS' internal control, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls. As noted above, the scope of our work was not sufficient to enable us to express, and we did not express, an opinion on the effectiveness of ICOFR. Further, other matters involving ICOFR may have been identified and reported had we been able to perform all procedures necessary to express an opinion on the DHS balance sheet as of September 30, 2009, and the related statement of custodial activity for the year then ended, and had we been engaged to audit the other FY 2009 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, and system security 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. These matters are described in the *IT General Control and Financial System Functionality Findings by Audit Area* section of this letter.

The material weakness described above is presented in our *Independent Auditors' Report*, dated November 13, 2009. This letter represents the separate restricted 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 by Audit Area* 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. In addition, we have provided: a description of key DHS' financial systems and IT infrastructure within the scope of the FY 2009 DHS financial statement audit engagement in Appendix A; a description of each IT finding and recommendation in Appendix B; the current status of the prior year NFRs in Appendix C, and managements comment in Appendix D. 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 December 9, 2009.

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

APPENDICES

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 statement audit. FISCAM also provides guidance to IT auditors when considering the scope and extent of review that generally should be performed when evaluating general controls and the IT environment of a federal agency. FISCAM defines the following six control functions to be essential to the effective operation of the general IT controls environment.

- *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 and/or monitor access to computer resources (data, programs, equipment, and facilities) to protect against unauthorized modification, loss, and disclosure.
- *Configuration Management (CM)* – Controls that help to prevent the implementation of unauthorized programs or modifications to existing programs.
- *Segregation of Duties (SD)* – Controls that constitute policies, procedures, and an organizational structure to prevent one individual from controlling key aspects of computer-related operations, thus deterring unauthorized actions or access to assets or records.
- *Contingency Planning (CP)* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

To complement our IT general controls audit, we also performed technical security testing for key network and system devices. The technical security testing was performed from within select DHS facilities and focused on test, development, and production devices that directly support DHS' financial processing and key general support systems.

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

- *Application Controls* - Application controls are the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, payroll, grants, or loans.

During FY 2009, 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. Additionally, DHS has had limited Department-wide financial system development or improvement activities. Consequently, ongoing financial system functionality limitations

are contributing to the Department's challenges of addressing systemic internal control weaknesses and strengthening the over-all control environment.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2009, DHS components took steps to improve their financial system security and address prior year IT control weaknesses, which resulted in the closure of more than 60% of our prior year IT control findings. However, new IT findings were identified during the year. The two primary reasons for the new findings included:

- New applications were included within the scope of the FY 2009 IT Audit and
- The lack of operating effectiveness of key IT general controls

As a result, we identified over one hundred (100) new IT general control deficiencies, which was over a 100% increase from last year. 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; and 3) security management deficiencies in the area of background investigations, the certification and accreditation process and system acquisition and development impacting DHS' ability to ensure that DHS financial data is available when needed. 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). The IT findings were combined into one material weakness regarding IT Controls and Financial Systems Functionality for the FY 2009 audit of the DHS consolidated financial statements.

Conditions: Our findings related to IT controls and financial systems functionality follow:

Related to IT controls:

The IT general control areas that continue to present risks to DHS financial data confidentiality, integrity, and availability include:

- *Access controls* – Key DHS financial systems and applications have access control weaknesses, including: weaknesses in security documentation and approvals; lack of recertification for user accounts on an annual basis; inconsistent disabling of user account accesses upon termination; inadequate or weak system passwords; workstations, servers, or network devices without necessary software patches; lack of sufficient workstation inactivity time-outs; out of date anti-virus software; and insufficient audit logging. In addition we identified the following instances where DHS policy was not adhered to:
  - 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 issued badges.
  - 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.
- *Configuration management* – We identified configuration management processes that are not fully defined, followed, or effective, including:

  - Instances where changes made to financial systems were not always properly approved, tested, or documented in accordance with the required System Change Request (SCR) process; and
  - Instances where policies and procedures regarding change controls were not in place to prevent users from having concurrent access to financial system development, test, and production environments, or for restricting access to application system software and system support files.

- *Security management* – We identified security management practices that do not fully and effectively ensure that financial systems are certified, accredited, and authorized for operation prior to implementation; and that all operational financial systems are accounted for in DHS' system inventory and monitored for compliance with security requirements in DHS' Trusted Agent FISMA system. Not following DHS standards in the area of background investigations and security and technical requirements for financial systems have not been considered and planned for in an integrated fashion during systems development and acquisition initiatives.

Related to financial system functionality:

We noted that financial system functionality limitations are contributing to control deficiencies which are inhibiting progress on corrective actions at several DHS components. Systemic conditions related to financial system functionality include:

- Segregation of key accounting functions needs to be manually maintained;
- Financial system audit logs are not readily generated and reviewed;
- DHS-required system passwords are not being followed due to financial systems that cannot support the policy;
- Financial systems do not provide flexible, user-friendly functionality; and
- Production versions of operational financial systems are outdated, no longer supported by the vendor, and do not provide the necessary core functional capabilities (e.g., general ledger capabilities).

While the recommendations made by us should be considered by DHS, it is the ultimate responsibility of DHS management to determine the most appropriate method(s) for addressing the weaknesses identified based on their system capabilities and available resources.

The individual weaknesses and findings that compose this deficiency are detailed in the following section.

IT GENERAL AND APPLICATION CONTROL FINDINGS BY AUDIT AREA

Conditions: In FY 2009, the following IT and financial system functionality deficiencies were identified at DHS. Forty percent of the deficiencies identified during our FY 2009 engagement were repeat issues identified during FY 2008. In addition, over 100 new IT deficiencies were identified this fiscal year, which is a 100% increase over the previous year. The following IT and financial system functionality deficiencies result in IT being reported as contributing to a material weakness for financial system security as part of the FY2009 DHS Integrated Audit.

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

- Initial and modified user access, roles, and privileges to financial applications, databases, and networks, including remote access were not documented and/or appropriately authorized;
- Policies and procedures that require periodic recertifications of user accounts were not in place;
- Periodic recertifications of user access and privileges to financial application, database, network, and/or remote user access were not formally performed in accordance with DHS policy;
- Financial application, database, network, and/or remote user accounts were not disabled or timely removed in accordance with DHS policy;
- Passwords were not configured to meet DHS requirements;
- Comprehensive and/or adequate policies and procedure that provide formal guidance for configuring and reviewing audit logs in accordance with DHS policy were lacking;
- Audit logs were not configured, reviewed, and/or monitored in accordance with existing requirements;
- An approved DHS Waiver and Exceptions Request Form associated with a financial database audit logging weaknesses was granted based on inconsistently or inaccurately described mitigating and compensating security controls. In addition, the controls required as a condition of DHS approval were not implemented;
- The use of generic or default user accounts was identified;
- Root access to financial systems is granted and not appropriately restricted and monitored;
- Physical access to sensitive facilities and resources was ineffective;
- Processes in place for sanitization of equipment and media were lacking;
- The process for authorizing and managing remote virtual private network (VPN) access to external agencies and contractors did not comply with the component and DHS requirements. Specifically, existing documentation did not define the requirements for administering VPN access for external organizations or identifying component roles and responsibilities for managing VPN access granted to external individuals using non-DHS equipment to access the network;
- Emergency and temporary access to financial applications and databases was not properly authorized and/or granted;

- A formalized process did not exist to guide staff in the modification of sensitive system accounts to ensure that appropriate privileges are created, documented, and approved for a specific security function. Additionally, the use of function modification privileges was not monitored;
- End-user workstations were not properly configured to activate a password-protected screensaver after five minutes of inactivity, as required by policy;
- Weaknesses in processes for recertifying data center access were present;
- Invalid login attempt settings did not comply with DHS requirements; and
- Accounts were not configured to be disabled after 45 days of inactivity within a full fiscal year, as required by component and DHS policy.

2. Configuration Management - At the following DHS components: USCG, CBP, FLETC, FEMA, ICE, DHS Headquarters, TSA, and USCIS, we noted:

- Password, security patch management, and configuration weaknesses were identified during our vulnerability assessments on hosts supporting the key financial applications and general support systems;
- System Engineering Life Cycle (SELC) documentation was not finalized;
- The Standard Operating Procedure (SOP) for monitoring sensitive access to operating system software was not implemented and did not include all operating system servers that are within scope. Additionally, there was no application or tool in place to support the audit logging function on the servers;
- Emergency and non-emergency changes to financial application system software were not consistently documented, tested, approved, controlled, tracked, and retained on file;
- Contracted developers/programmers were granted unrestricted access to the production environment;
- A finalized patch management policy for installing system patches was not implemented;
- Formal procedures were not implemented to require monitoring of developers' changes to a system's directories and sub-directories to review and validate implemented changes and informal reviews of developer activities were not routinely performed and documented;
- The configuration management plans did not comprehensively provide guidance to address all configuration management control elements required by component and DHS policy;
- System changes were not appropriately approved and tracked prior to implementation into production;
- Monitoring process of their service provider's configuration management process and activities was not fully developed nor operating effectively;
- Procedures for approving, testing, and ensuring timely installation of operating system patches were not developed and implemented;
- Formal procedures for conducting internal scans were not developed, remediation of vulnerabilities identified during internal scans were not tracked and monitored, and select workstations were excluded from the scope; and

- 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.

3. Security Management – At the following DHS components: USCG, CBP, FEMA, ICE, DHS Headquarters, and TSA we noted:

   - Procedures for transferred/terminated personnel exit processing are not finalized;
   - Computer access agreements and exit clearance procedures have not been consistently implemented;
   - Policies and procedures requiring completion of a training program by personnel in IT security positions were not finalized;
   - IT Security training is not mandatory nor is compliance monitored;
   - Background investigations as well as reinvestigations for all civilian and contractor employees have not been completed per DHS guidance;
   - Procedures for the program managers on how to set the correct and consistent risk levels and position sensitivity designations for contract employees were not finalized;
   - Four systems were not properly certified and accredited in accordance with DHS guidance;
   - Information System Security Officers (ISSO) and Designated Authorizing Authorities (DAA) were not formally designated;
   - Vulnerabilities identified during periodic internal scans and related corrective actions were not reported and tracked in accordance with DHS policy;
   - Two systems were not included in the system inventory and neither system was being tracked via the Trusted Agent Federal Information Security Management Act repository;
   - The revised system security plan for one system did not fully document the systems boundaries, define all subsystems and major applications, nor establish security responsibilities for all system components;
   - For the majority of FY 2009, a finalized and executed Memorandum of Understanding and an Interconnection Sharing was not in place between a DHS component and the Department of the Treasury;
   - Information Security Agreements for all identified participating government agencies have not been documented as required by the DHS component and DHS policies;
   - Procedures for managing IT security incidents were not developed, approved, and implemented and the audit's unannounced vulnerability assessment scanning activity was not detected and appropriately reported by the DHS component, and in accordance with DHS and the DHS component's incident response policy;
   - 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 Office of the Chief Information Officer (OCIO)

to ensure appropriate consideration and integration of IT security, and (4) the joint communication and decision-making of the DHS component and DHS management;

- A process is lacking for tracking the status of contractors or an effective and formal process for notifying the OCIO of changes in contractor status so that user accounts could be appropriately disabled, removed, or modified in a timely manner;
- Data from all component organizations to ensure a complete and accurate listing of all contractors was not properly captured. Additionally, through inspection of data on current contractors, it was noted that there were data validity issues in the component's contractor tracking system, including inaccurate start dates, as well as duplicate hash IDs;
- A complete and up-to-date listing of all workstations is not maintained, specifically, workstations maintained within Active Directory (AD) can not be accounted for in a reasonable manner;
- Twenty-four out of 60,750 Active Directory (AD) workstations did not have virus protection installed, which is a negligible amount. However, it could not be determined what percentage of non-AD workstations have virus protection installed, as non-AD workstations do not communicate with the ePolicy Orchestrator system that is used to maintain and update virus protection across the component's workstations and networks;
- Non-disclosure agreements (NDA) for eight out of 45 selected contractors were signed several months after their hire date. Additionally, one NDA did not have a witness signature, indicating that the NDA was not appropriately completed; and
- Ten out of 40 selected individuals with systems access across the country did not have a signed rules of behavior on record. Additionally, 11 individuals signed the rules of behavior months after the component's requirement to sign the rules of behavior. These individuals have had access during fiscal year 2009.

4. Service Continuity – at the FEMA we noted:
   - An alternate processing site was not established and implemented. Additionally, the approved DHS waiver was expired and documented controls for restoring the system servers from back up tapes to compensate for the lack of an alternate processing site were ineffective;
   - A system's backup tapes were not regularly tested in accordance with policy at one DHS component;
   - A full scale testing of a system's contingency plan was not conducted and the plan did not adequately and comprehensively include information for fully restoring the system in accordance with requirements for a high impact availability system. Additionally, the waiver approved by DHS that identified table-top testing as a compensating control for the component's inability to fully test the system was expired; and
   - An existing systems contingency plan and the disaster recovery and continuity of operations plan were not current or tested for systems recovery and failover capability at the alternate processing site. Additionally, the systems alternate processing facility and critical data files were not documented in the existing disaster recovery and continuity of operations plan.
5. Segregation of Duties – At the following DHS components: CBP, FEMA, ICE, and USCIS we noted:
   - Segregation of duties controls were not enforced through access authorizations in one system;

- Incompatible duties that must remain segregated when granting and maintaining user access and processes for segregating incompatible duties within a system are not formally documented in existing policies and procedures;
- One system is not currently configured to restrict access to least privilege for performing job functionality as required by component policy; and
- For one system, six users had Originator, Funds Certification Official, and Approving Official profiles that were in violation of the component's segregation of duties policies.

Application Controls

- At CBP, a weakness in the drawback controls existed within a system. Specifically, the system does not support the tracking of drawback items to the line item level. Rather, it only tracks drawbacks on a summary level. This control weakness was also identified in FYs 2003 through 2008. Additionally, we noted the certification of drawbacks is required before a drawback can be processed. However, the system currently automatically certifies drawbacks that have not been certified by a supervisor, circumventing this control.

Financial System Functionality

We noted that financial system functionality limitations are contributing to control deficiencies which are inhibiting progress on corrective actions in several DHS components. Systemic conditions related to financial system functionality include:

- Segregation of key accounting functions needs to be manually maintained because financial systems cannot enforce automated segregation of duties.
- Financial system audit logs are not readily generated and reviewed because financial systems cannot offer the necessary functionality.
- DHS-required system passwords are not being used because some financial systems cannot support the policy.
- Financial systems do not provide flexible, user-friendly, functionality to completely and accurately report financial data or track property, plant, and equipment information.
- Production versions of operational financial systems are outdated, no longer supported by the vendor, and do not provide the necessary core functional capabilities (e.g., general ledger capabilities).

Other Findings in IT General Controls

After-Hours Physical Security Testing

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 a DHS component employee's desk, which could be used by others to inappropriately access financial information. The testing was performed at various DHS component locations that process and / or maintain financial data. After gaining access to the facilities via a DHS employee who was designated to assist with and monitor our test work, we inspected a random selection of desks or offices, looking for items such as improper protection of system passwords, unsecured information system hardware, documentation marked "For Official Use Only" (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.

The after hours testing at each DHS component was performed separately over a three month period. During the initial phase of our testing it came to our attention that DHS component management became aware of our testing efforts and notified their employees to be aware of auditors conducting random security testing. As a result, there is the belief that the future testing results of the later DHS components during the testing phase were compromised and fewer exceptions were identified as a result.

For each DHS component tested, 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. See table below for specific details of the result of our testing at each of the components included in the scope of this audit work:

	DHS Components						**Total Exceptions by Type**
Exceptions - Items Unsecured	**CBP**	**Coast Guard**	**FEMA**	**FLETC**	**ICE**	**TSA**	
Passwords	10	11	42	84	26	4	**177**
For Official Use Only (FOUO)	26	0	2	4	4	0	**36**
Keys/Badges	7	0	2	7	2	0	**18**
Personally Identifiable Information (PII) Data	23	0	2	83	15	0	**123**
Server Names/IP Addresses	2	0	1	0	2	0	**5**
Laptops	3	2	1	6	3	0	**15**
External Drives	4	0	4	2	6	0	**16**
Credit Cards	2	2	0	12	1	0	**17**
Common Access Cards (CAC)	0	4	0	0	0	0	**4**
Other – Workstation logged on without screen saver activated	0	0	0	4	2	0	**6**
Other –U.S. Government passport	1	0	0	0	0	0	**1**
Total Exceptions by Component	**78**	**19**	**54**	**202**	**61**	**4**	**418**

Social Engineering Testing

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 computer system access. The term typically applies to 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 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 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.

The social engineering testing at each DHS component was performed separately over a two month period. During the initial phase of our testing it came to our attention that DHS component management became aware of our testing efforts and notified their employees to be aware of auditors conducting random security testing. As a result, there is the belief that the testing results of the DHS components later in the testing phase were compromised and fewer exceptions were identified as a result.

Our selection of individuals was not statistically derived, and therefore we are unable to project results to the component or department as a whole.

For each DHS component tested, we noted the number of calls made, the number of DHS employees who answered our calls and the number of DHS employees that in appropriately provided their password to the KPMG auditors. See table below for specific details of the result of our testing at each of the components included in the scope of this audit work:

DHS Component	Total Called	Total Answered	Number of people who provided a password
CBP	30	10	2 passwords provided
Coast Guard	38	14	1 password provided
FEMA	50	15	No passwords provided
FLETC	44	20	No passwords provided
ICE	65	20	5 passwords provided
TSA	20	5	No passwords provided
Totals	247	84	8 passwords provided

Recommendations: We recommend that the DHS Office of Chief Information Officer (OCIO), in coordination with the 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 Office of Chief Information Officer (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.

Cause/Effect: A contributing cause to repeated findings is that DHS lacks an effective component-wide prioritization of financial system weaknesses, including the development of a stable centralized financial

system platform for the Department. The time and resources needed to implement corrective actions necessary to mitigate these weaknesses are significant.

The conditions supporting our findings collectively limit DHS' ability to ensure that critical financial and operational data is kept secure and is maintained in a manner to ensure confidentiality, integrity, and availability. Many of these weaknesses, especially those in the area of access and configuration management controls, may result in material errors in DHS' financial data that are not detected in a timely manner and in the normal course of business. In addition, as a result of the presence of IT control weaknesses and financial system functionality weaknesses, there is added pressure on other mitigating manual controls to be operating effectively at all times. Because mitigating controls often require more manually performed procedures, there is an increased risk of human error that could materially affect the financial statements.

Criteria: The *Federal Information Security Management Act* (FISMA) passed as part of the *E-Government Act of 2002,* mandates that Federal entities maintain IT security programs in accordance with the OMB guidance and other applicable requirements. In addition, OMB Circular No. A-130, *Management of Federal Information Resources,* describes specific essential criteria for maintaining effective general IT controls. Further, the *Federal Financial Management Improvement Act* (FFMIA) sets forth legislation prescribing policies and standards for Executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems. The purpose of FFMIA is to: (1) provide for consistency of accounting by an agency from one fiscal year to the next, and uniform accounting standards throughout the Federal Government; (2) require Federal financial management systems to support full disclosure of Federal financial data, including the full costs of Federal programs and activities; (3) increase the accountability and credibility of federal financial management; (4) improve performance, productivity and efficiency of Federal Government financial management; and (5) establish financial management systems to support controlling the cost of Federal Government. FFMIA requirements are complemented by Financial Systems Integration Office (FSIO) requirements, which set forth core financial management functionality required by Federal financial systems. Finally, DHS' *Sensitive Systems Policy, 4300A*, documents policies and procedures adopted by DHS intended to improve the security and operation of all DHS IT systems.

MANAGEMENT'S COMMENTS AND OIG RESPONSE

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

OIG Response

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

Appendix A

Description of Key Financial Systems and IT Infrastructure within the Scope of the FY 2009 DHS Integrated Audit Engagement

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

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

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

Checkfree
Checkfree is a commercial product used to reconcile payment information retrieved from the United States Department of the Treasury (Treasury). It reconciles items that Treasury has paid with items CAS has sent to that Department. This system is hosted on a Windows server and resides at the FINCEN.

- Oracle Database 9.2.0.8.0 – 48 GB
- 12x750mhz RISC Processor; fundx.world
- Checkfree Operating System - HP Unix; 11.11; ARGUS 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 - 2 Sunfire 4800, 3 Sunfire 880, 1 Sunfire 4500, and 1 Sunfire v240 server
- Operating System - Sun Solaris 2.8
- Database - Oracle 9.2.0.6
- Software - Peoplesoft HCM 8.0
- Security Software – Tivoli

Global Pay (Direct Access II)
Global Pay provides retiree and annuitant support services. Global Pay 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.

- Oracle RDMS v 10.x
- IBM x Series 336

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

Customs and Border Protection

SAP R/3
SAP is a client/server-based financial management system that was implemented beginning in FY 2004 to ultimately replace the AIMS mainframe-based financial system using a phased approach. The SAP Materials Management module was implemented and utilized in FY 2004. Since FY 2005, the Funds Management, Budget Control System, General Ledger, Internal Orders, Sales and Distribution, Special Purpose Ledger, and Accounts Payable modules have been implemented. Therefore, the entire SAP R/3 financial management system was included in the FY 2008 financial statement audit and is under a full scope ITGC review. The SAP R/3 system is located in

Automated Commercial System (ACS)

ACS is a collection of mainframe-based applications used to track, control, and process all commercial goods, conveyances and private aircraft entering the United States territory, for the purpose of collecting import duties, fees, and taxes owed the Federal government. The ACS system is included in full scope in the FY 2008 financial statement audit. The ACS system is located in

Automated Commercial Environment (ACE)
ACE is the commercial trade processing system being developed by CBP to facilitate trade while strengthening border security. ACE is being deployed in phases, with a final full deployment scheduled for FY 2010. As ACE is partially implemented now and processes a significant amount of revenue for CBP, ACE was included in a full scope for this year's financial statement audit. The ACE system is located in .

Federal Law Enforcement and Training Center (FLETC)

Financial Accounting and Budgeting System (FABS)

- Processing Location*:* FLETC Headquarters in Glynco, GA
- General System Description:

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 6.1.6 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)
- Treasury Information Executive Repository (TIER)
- US Coast Guard Interface
- Kansas City Financial Center (KFC)

Glynco Administrative Network

- Processing Location*:* FLETC Headquarters in Glynco, GA
- General System Description:

The purpose of the Glynco Administrative Network (GLYADLAN) is to provide access to Information Technology (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 Finical 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

Student Information System (SIS)
- Processing Location*:* FLETC Headquarters in Glynco, GA
- General System Description:

The purpose of the SIS is to capture and facilitate the FLETC student registration process and billing. SIS stores, processes, and transmits Sensitive But Unclassified (SBU) information, which includes individual student personal information. Additional data types include specific course information (e.g., course numbers, dates, associated agencies, locations, and billing costs). All users of SIS are internal to the FLETC network. Students do not directly enter data into SIS.
- Hardware: HP Server.
- Operating System: HP-UX 11.0
- Database: Informix
- Security Software: DHS Firewall

Interfaces:
No direct interconnection

Federal Emergency Management Agency

Core Integrated Financial Management Information System (IFMIS)
- Processing Location*:* Mount Weather Emergency Operations Center (MWEOC) in Bluemont, VA

General System Description:

Core IFMIS is the key financial reporting system, and has several feeder subsystems (budget, procurement, accounting, and other administrative processes and reporting). It was developed and is currently maintained by the Digital Systems Group Incorporated (DSG).
- Hardware: Two (2) HP-N4000 servers
- Operating System: HPUX (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
- Treasury Information Executive Repository (TIER)

Grants and Training (G&T) IFMIS
Processing Location*:* Mount Weather Emergency Operations Center (MWEOC) in Bluemont, VA

General System Description:
G&T IFMIS was moved from the Department of Justice into the FEMA environment in FY 2007. The system stores former G&T financial information.

- Hardware: HP-N4000 server
- Operating System: HPUX (Unix) version 11.11
- Database: Oracle 9i Enterprise Edition
- Security Software: Servers are protected by a CISCO PIX Firewall

Interfaces:

- PARS

Payment and Reporting System (PARS)
Processing Location*:* Mount Weather Emergency Operations Center (MWEOC) in Bluemont, VA

General System Description:
PARS is a standalone web-based application that resides on the G&T IFMIS UNIX server. Through its web interface, PARS collects and stores SF269 information from grantees. Chron jobs are run daily to update the grant information from PARS into G&T IFMIS. Additionally, through these chron jobs, PARS is also updated with the obligation information from G&T IFMIS to provide updated information to its users.

- Hardware: HP-N4000 server
- Operating System: HPUX (Unix) version 11.11
- Database: Oracle 9i Enterprise Edition
- Security Software: Servers are protected by a CISCO PIX Firewall

Interfaces:

- G&T IFMIS

National Emergency Management Information System (NEMIS)
Processing Location*:* Mount Weather Emergency Operations Center (MWEOC) in Bluemont, VA

General System Description:

NEMIS is an integrated system to provide FEMA, the states, and certain other federal agencies with automation to perform disaster related operations. NEMIS supports all phases of emergency management and provides financial related data to IFMIS via an automated interface.

- Hardware: HP Servers
- Operating System: Linux, Microsoft NT and Microsoft 2000
- Database: Replicated Oracle 10g, 9i, and 8i database
- 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

General System Description:
Traverse is the general ledger application currently used by the 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 in Lanham, 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)

Interfaces:
No known system interfaces

Transaction Recording and Reporting Processing (TRRP)
Processing Location*:* Norwich, CT

General System Description:
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 – z/OS 1.4
- Database - FOOCUS

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 9170 Mainframe with ZOS 1.9 platform. The FFMS operating system operates off an IBM ZOS, Version 1.9 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 a National Finance Center payroll interface. The FFMS mainframe component and two network servers are hosted at the Department of Commerce (DOC) Office of Computer Services (OCS) facility located in Springfield, Virginia. FFMS currently interfaces with the following systems:

- Direct Connect for transmission of DHS payments to Treasury
- The Travel Manager System (TMS)
- The Biweekly Examination Analysis Reporting (BEAR) and Controlling Accounting Data Inquiry (CADI), for the purpose of processing National Finance Center (NFC) user account and payroll information.
- The Debt Collection System (DCOS)
- Bond Management Information System (BMIS) Web (starting October 31, 2008 and will replace DCOS)

ICE Network
The ICE Network, also know 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 BL4p 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.

- Commercial Off the Shelf (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 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

Sunflower
Sunflower is a customized third party commercial off the shelf (COTS) product used for TSA and Federal Air Marshals (FAMS) property management. Sunflower interacts directly with the OF FA module in CAS. Additionally, Sunflower is interconnected to the FPD system.

- Sunflower 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

United States Citizenship and Immigration Services (USCIS)

Claims 3 Local Area Network (LAN)
Claims 3 LAN provides USCIS with a decentralized LAN based system that supports the requirements of the Direct Mail Phase I and II, Immigration Act of 1990 (IMMACT 90) and USCIS forms improvement projects. The Claims 3 LAN is located at each of the service centers (Nebraska, California, Texas, Vermont, and the National Benefits Center). 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 interfaces with the following systems:

- CLAIMS 3 Mainframe
- Integrated Card Production System (ICPS)
- Receipt and Alien-File Accountability and Control System (RAFACS)
- CLAIMS 4
- FD-258 EE
- E-filing
- Benefits Biometric Support System (BBSS)
- IBIS
- CHAMPS

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 of 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)
- Computer-Linked Application Information Management System 3 (CLAIMS 3)
- Refugee, Asylum, and Parole System (RAPS)
- Performance Analysis System (PAS)
- National File Tracking System (NFTS)
- Receipt and Alien-File Accountability and Control System (RAFACS)
- Interactive Voice Response System (IVRS)

Appendix B

FY2009 Notice of IT Findings and Recommendations at DHS

Notice of Findings and Recommendations – 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 DHS in the development of its corrective action plans for remediation of the deficiency.

Department of Homeland Security
FY2009 Information Technology - Notice of Findings and Recommendations – Detail

- **United States Coast Guard**

Department of Homeland Security
Information Technology Management Letter
September 30, 2009

Notification of Findings and Recommendations – Detail

United States Coast Guard

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CG-IT-09-10	The current Coast Guard Instruction does not include specific guidance for the Program Managers on how to set the correct and consistent risk levels and position sensitivity designations that correspond to CLINs and labor categories. Therefore, there is insufficient guidance over the level of clearance required which may result in inconsistent risk levels and position sensitivity designations.	Update the policies and procedures currently in place to include clear guidance for Program Managers and Contracting Officers to assign contractor risk level(s) and position sensitivity designation requirements in order to verify that all contracts issued by the Coast Guard include the appropriate investigation level requirements.		X	2
CG-IT-09-14	The Role-Based Industry Standards for Coast Guard Information Assurance (IA) Professionals Commandant Instruction remains in draft form.	• Update the Role-Based Industry Standards for Coast Guard IA Professionals Commandant Instruction to include the procedures by which Direct Access will be used to monitor and verify that training has been completed by all Coast Guard Government personnel with significant information security responsibilities. In addition, the instruction should include the procedures by which Coast Guard contractor compliance will be monitored and verified. • Finalize, communicate, and implement the Role-Based Industry Standards for Coast Guard IA Professionals Commandant Instruction. • Continue with efforts to implement Direct Access as the centralized method for		X	1

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
		monitoring and verifying Coast Guard personnel compliance with the specialized role-based training requirements.			
CG-IT-09-23	Although the Operation Systems Center (OSC) has begun reviewing Shore Asset Management (SAM) audit logs on a regular basis, detailed policies and procedures have not been created over the process and sufficient evidence is not maintained.	Develop and document comprehensive policies and procedures over the SAM audit log review process. These policies and procedures should establish the independence of the reviewer, the audit logs under review, and the supporting documentation requirements including results and remediation efforts.		X	1
CG-IT-09-25	Procedures do not include an annual review of all Workflow Imaging Network System (WINS) user accounts, as required by the DHS 4300A Sensitive Systems Handbook and required by the DHS Chief Information Officer.	Modify procedures to require an annual review of one hundred percent (100%) of WINS user accounts and their associated privileges that are greater than read-only. The updated procedures should include steps to verify that: a) all terminated individuals no longer have active accounts, b) inactive accounts are locked, and c) privileges associated with each individual/role are still authorized and necessary for that job function.		X	1
CG-IT-09-31	Weaknesses continued to exist over the script configuration management process. Specifically, weaknesses were noted in the areas of approvals, testing, monitoring, maintaining documentation, and audit logging. • Coast Guard lacks a formal process to distinguish between the module lead	Continue making improvements to implement and better document an integrated script configuration management process that includes enforced responsibilities of all participants in the process, and the continued development of documentation requirements. We recommend that the Coast Guard should:		X	3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	approvers for script approval requests. • Coast Guard Finance Center (FINCEN) analysts may run scripts without seeking further approval from the Functional Supervisors for approved recurring scripts. • Testing requirements are inconsistently followed for the testing of the Recurring Approval scripts and retaining evidence of testing. • No reconciliation between the scripts run and the changes made to the database tables is being performed to monitor the script activities using this report as it is too difficult to accurately and effectively reconcile the scripts to the audit log table changes. • The Script Tracking System does not consistently include all testing, approval, and implementation documentation for all scripts. • Variations in the way the Production Review Process (PRP) Approval Forms are populated and completed exist for fields such as financial impact, test strategy and baseline determinations. • Proper approval is not consistently obtained and documented prior to the running of each script.	• Continue to design, document, implement, and enforce the effectiveness of internal controls associated with the active (current and future) scripts. With respect to procedures already in place, Coast Guard should: • Update / Develop procedures and implement technical controls in the Core Accounting System (CAS) and Financial Procurement Desktop (FPD) databases to ensure that the appropriate monitoring and review of script activities is performed and documented. • Continue to update script policies and procedures to include clear requirements and more detailed guidance over requesting recurring scripts, testing and documentation requirements, monitoring/audit log reviews, and blanket approval requirements. Additionally, ensure that the policies and procedures include detailed guidance over the requirements for the testing of scripts and associated test plans to ensure that the appropriate financial impact of the script is evaluated, reviewed by the appropriate personnel, tested in an appropriate test			

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
		environment prior to being put into production, and documented prior to execution. • Further develop and implement policies and procedures governing the script change control process to ensure that all script records within the Change Management Script System are accurate and complete.			
CG-IT-09-32	Coast Guard has not created specific procedures to address how monthly contractor reports will be analyzed and does not maintain supporting evidence associated with this review.	Develop and finalize specific procedures over the review of the Contractor Verification System reports and reconciliation of contractor accounts to ensure that contractor data within the system remains current and accurate.		X	2
CG-IT-09-33	During our FY 2009 follow-up test work, we determined that Coast Guard is currently finalizing the business process that will be used to remediate the conditions identified in the prior year NFR. Once a business process has been finalized, a technical implementation will occur. Currently, Coast Guard HQ plans to use the Direct Access Human Resources (HR) system to notify system owners of HR status changes for all individuals within the system. This would include terminations. Direct Access is currently undergoing a phased upgrade from PeopleSoft 8.0 to PeopleSoft 9.0. Coast Guard informed us that while the functionality required is not	• Develop and document an enterprise-wide process that will notify all impacted system owners of terminated, transferred, or retired contractor, military, and civilian personnel; and • Develop and finalize entity management policies and procedures for verifying that terminated user accounts have been successfully removed.		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	included in the 8.0 version, it should be included in the 9.0 version. At this time, where this functionality fits into that upgrade schedule, has not yet been determined. In addition, Coast Guard has created a service request to track its remediation efforts and has identified the termination process currently conducted at Coast Guard's Personnel and Pay Center (PPC) as a potential solution. At PPC, a report is run within Direct Access whenever an individual separates, retires, or transfers which automatically removes system permissions. However, this process currently excludes contractors and civilians whose information is not currently in Direct Access.				
CG-IT-09-34	Not all WINS change requests were appropriately reviewed and approved by management prior to development and/or prior to implementation. In addition, one of the 25 WINS changes selected was identified as having a financial impact consideration to the Coast Guard Financial Statements and, as such, the appropriate Financial Representative approval was not obtained prior to implementation. We further noted that the criterion set forth in the Coast Guard Finance Center Financial Statement Impact Consideration Memo does not provide sufficient detail to assist in making a determination regarding the financial impact of a proposed change.	• Consistently enforce the newly implemented PRP process to ensure that all change requests are properly reviewed and approved prior to development and again prior to implementation. • Periodically verify FINCEN compliance with its PRP and related approval and CM processes. • Formally document detailed decision criteria to be used when determining if a change has a financial impact.		X	1

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CG-IT-09-40	During our FY 2009 follow up, we determined that Coast Guard actively monitors all civilians to verify whether they have a valid background investigation on record. We received documentation from Coast Guard that identified 94 individuals with an outstanding investigation. This number has been reduced significantly from the approximately 350 individuals identified in FY 2008. Coast Guard continues vetting individuals based on the Office of Personnel Management (OPM) requirements which require a National Agency Check and Inquiries (NACI) investigation for those position designations with the lowest risk. A NACI consists of written inquiries and searches of records covering specific areas of a person's background during the past five years including current and past employers, schools attended, references, and local law enforcement authorities. However, all DHS government positions that use, develop, operate, or maintain IT systems are considered at least moderate risk (not low), and per DHS, 4300A requirements, an Minimum Background Investigation (MBI) is the minimum standard of investigation. The MBI consists of the NACI as well as a credit record search, face-to-face personal interview between the investigator and the subject, and telephone inquiries to selected employers. Therefore, Coast Guard is not in compliance with these DHS requirements.	• Perform the initial background investigations for civilian employees in accordance with the DHS directives over position sensitivity designations; and • Conduct civilian background re-investigations as required by DHS directives, to ensure that each civilian employee has a favorably adjudicated, valid, and required background investigation.		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	In addition, Coast Guard does not complete background re-investigations due to the lack of the requirement under current OPM guidance for low risk positions even though re-investigations must be completed every 10 years for moderate risk positions per DHS Management Directive (MD) 11050.2, *Personnel Security and Suitability Program.*				
CG-IT-09-42	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) and we believe that Coast Guard has not fully addressed the recommendations in NFR CG-IT-08-42.	• Continue to implement and improve upon the monitoring of compliance with DHS, Coast Guard, and Federal security policies and procedures in the areas of the script configuration management controls. • Develop and implement corrective action plans to address and remediate the NFRs issued during the FY 2009 audit. These corrective action plans should be developed from the perspective of the identified root cause of the weakness both within the individual NFR and across related NFRs. The IT NFRs should not be assessed as individual issues to fix, but instead, should be assessed collectively based upon the control area where the weakness was identified. This approach		X	3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
		enables corrective action that is more holistic in nature, thereby leading to a more efficient and effective processes of addressing/fixing the controls that are not operating effectively.			
CG-IT-09-43	Coast Guard procedures do not include a review of all UMS user accounts, as required by DHS 4300A Sensitive Systems Handbook and required by the DHS-CIO. A full 100% review of accounts that exceed 'read-only' access would ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked, and that privileges associated with all UMS users are authorized and necessary.	Modify procedures to require an annual review of one hundred percent (100%) of UMS user accounts and their associated privileges that are greater than read-only. The updated procedures should include steps to verify that all terminated individuals no longer have active accounts, that inactive accounts are locked and that privileges associated with each individuals are still authorized and necessary.		X	2
CG-IT-09-45	Access was not authorized for two of the 15 individuals we tested who possessed badges allowing FINCEN data center access.	Include the badge software database during the data center access review process to ensure that no unauthorized individuals have badges that would allow them access to the FINCEN data center.	X		1
CG-IT-09-46	During our testing, we determined that all previous year conditions listed in NFRs CG-IT-08-36 and CG-IT-08-37 were properly remediated by USCG. As part of this year's testing, we identified nine security configuration management weaknesses (i.e., missing security patches and/or incorrect configuration settings) on hosts supporting CAS and FPD.	Implement the corrective actions for the recommendations listed within the NFR.	X		1
CG-IT-09-47	Direct Access passwords do not require a special character, which is a requirement set forth within DHS	Through our test work, we determined that the control weakness was remediated prior to the	X		1

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	4300A Sensitive Systems Policy Directive.	fiscal year-end; therefore, no recommendation is required for this NFR.			
CG-IT-09-48	Global Pay accounts are configured to expire after five (5) invalid login attempts, rather than three (3), which is a requirement set forth within DHS 4300A Sensitive Systems Policy.	Through our test work, we determined that the control weaknesses were remediated prior to the fiscal year-end, therefore, no recommendation is required for this NFR.	X		1
CG-IT-09-49	The quarterly JUMPS audit log review addresses unusual activity or unexplained access attempts which DHS 4300A Sensitive Systems Policy Directive requires to be done on a monthly basis.	Review audit logs containing unusual activity and unexplained access attempts on an at least monthly basis to meet the requirements set forth in DHS 4300A, perform the necessary follow up on any incidents identified and maintain sufficient evidence of the audit log reviews, and include copies of audit logs in hard copy or electronic form and evidence that the review of the audit logs was conducted.	X		1
CG-IT-09-50	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 monthly basis, which is a requirement set forth within the DHS Sensitive Systems Policy Directive.	• Identify the Direct Access application security-oriented audit logs that should be reviewed and then have the application system administrators review those Direct Access application security logs on at least a monthly basis, in accordance with DHS Policy. • Additionally, we recommend that the Coast Guard upgrade to a more current version of PeopleSoft and Oracle so that it uses a vendor supported product with more robust security controls and so that accountability may be established to	X		1

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
		document changes to security settings and user profiles.			
CG-IT-09-51	Only the last modification to the user account is documented by the COTS PeopleSoft application software, making it difficult to establish accountability for role changes within the Global Pay application. Additionally, role changes for the Global Pay Application are not reviewed on a monthly basis, which is a requirement set forth within DHS Policy.	Review role change logs on at least a monthly basis, in compliance with DHS Policy.	X		1
CG-IT-09-52	100% of Direct Access user accounts with greater than read-only access are not reviewed annually to verify that access remains appropriate, per the DHS 4300A Sensitive Systems Handbook and required by the DHS-CIO.	Modify procedures to require an annual review of one hundred percent (100%) of Direct Access user accounts and their associated privileges that are greater than read-only. The updated procedures should include steps to verify that all terminated individuals no longer have active accounts, that inactive accounts are locked and that privileges associated with each individual are still authorized and necessary.	X		2
CG-IT-09-53	During our after hours physical testing, we identified 11 passwords, two unsecured laptops, two credit cards, and four Common Access Cards (CAC). During our social engineering testing, we were provided with one password.	• Review its policies and procedures regarding Protection of Sensitive Information and update where required in order to address DHS and other Federal requirements, with emphasis being placed on the potential impacts of not consistently and adequately protecting this sensitive information. • Review, and update as required, its security awareness/training content to	X		1

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
		address the updated Protection of Sensitive Information policies and procedures. • Validate the effectiveness of the updated policies and procedures and associated training through mechanisms such as scheduled and unscheduled desk/floor reviews, awareness training testing, etc. and take appropriate corrective action to address any issued identified during this validation.			

Department of Homeland Security
FY2009 Information Technology
Notification of Findings and Recommendations – Detail

- **Customs and Border Patrol**

Notification of Findings and Recommendations – Detail

U.S. Customs and Border Protection

NFR #	Condition	+Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-03	During testing, we were informed that all data had not been completely captured from all organizations within CBP to ensure a complete and accurate listing . Additionally, through inspection of data on current contractors, we noted that there were data validity issues in the system, .	We recommend that CBP implement procedures to have data regularly reviewed and updated by to ensure the most accurate data is in the for use by all of CBP.		X	2
CBP-IT-09-12	We noted that is installed on a significant majority of workstations at CBP. These workstations are on the system. However, we noted that there are a significant number of non- workstations that do not appear on the listing of workstations, as maintained by the administrators. We noted that these workstations do not have installed as required.	We recommend that CBP research, identify and implement a method to consistently account for all CBP workstations and perform regular reviews to ensure that all CBP workstations have or some future solution, appropriately applied.		X	2

NFR #	Condition	+Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-13	We noted that while progress has been made in accounting for all CBP workstations, a complete and up-to-date listing of all CBP workstations is not maintained. Specifically, We noted that workstations maintained within Active Directory (AD) can be accounted for in a reasonable manner. However, workstations that are not in AD are difficult to account for, as they are not part of the Active Directory structure and can only be identified when connecting to the network, which may not occur regularly (i.e., laptops, unused equipment, etc).	We recommend that CBP work with administrators across the country to ensure that new and existing workstations are added to a centralized accounting structure such as AD or some other more appropriate solution, if identified, to allow for all workstations to be accounted for in an appropriate fashion.		X	2
CBP-IT-09-21	We noted that when changes to a user's ACS access profile are performed, the log of these events is not regularly reviewed by personnel independent from those individuals that made the changes.	We recommend that the review of these logs is implemented on a periodic basis by an independent reviewer and that CBP formalize these procedures in detail for the review of ACS security profile change logs.		X	2
CBP-IT-09-27	We noted that authorizations are still not being maintained for personnel that have administrator access to . Procedures have been implemented to require documented authorization however evidence could not be provided that these procedures are being implemented appropriately.	We recommend that CBP implement procedures that have been developed to restrict access to mainframe administrative capabilities and require documented authorization requests and approval for each person requiring access to the mainframe administrative capabilities.		X	2

NFR #	Condition	+Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-29	We selected 45 individuals that had separated in FY 2009 and noted that 19 of these individuals did not have a completed CBP-241 form on file. Additionally, We noted that two forms provided for two different individuals were incomplete and lacked a supervisor's signature.	We recommend that CBP develop a standardized method of maintaining the CBP-241 forms to ensure that all forms for all separating employees are completed in a timely manner and are easily accessible.		X	2
CBP-IT-09-34	We noted that 24 out of 60,750 Active Directory (AD) workstations, or 0.04 percent, did not have antivirus installed, which is a negligible amount. However, We could not determine what percentage of non-AD workstations have virus protection installed, as non-AD workstations do not communicate with the ePolicy Orchestrator system that is used to maintain and update virus protection across CBP workstations and networks.	We recommend that CBP research, identify and implement a method to consistently account for all CBP workstations and perform regular reviews to ensure that all CBP workstations have virus protection installed and that it is regularly updated.		X	2

NFR #	Condition	+Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-41	We noted that a Customs Directive was provided as separation procedures for contractors and that this directive was dated September 2001. The directive references Treasury policies as source documentation. This directive is out of date, as CBP is no longer a part of the Department of Treasury. A new directive was issued requiring the use of the Contractor Tracking System; however, the new directive still refers to the old directive, which has not been updated. Additionally, We noted that CBP-242 contractor separation forms are not completed consistently for separating CBP contractors. Specifically, we noted that three separated contractors out of 45 selected had their forms completed over one month after they separated from CBP.	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 CBP-242 forms for all separating contractors.		X	2
CBP-IT-09-44	We noted that non-disclosure agreements are still not consistently being signed by contractors at CBP. Specifically, we noted that NDAs for eight out of 45 selected contractors were signed many months after their hire date. Additionally, we noted that one NDA did not have a witness signature, indicating the NDA was not appropriately completed.	We recommend that CBP implement a more consistent method of ensuring that contractors sign an NDA. We also recommend that COTRs regularly review their contractors and ensure that there is an NDA for each contract under their supervision.		X	2

NFR #	Condition	+Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-45	Parameters for all mainframe audit and [redacted] are not configured to collect appropriate data. Specifically, We noted that one out of the six mainframe audit and system utility logs, [redacted], did not produce any data during the time of testing due to an inaccurate filtering configuration.	We recommend that CBP properly configure mainframe audit and system utility logs to capture appropriate data for the NDC Mainframe system.		X	2
CBP-IT-09-48	We noted the following weaknesses related to the ACS Security Audit Logs procedures: • Procedures do not define how often the ACS security profile change audit logs are reviewed. • Procedures do not describe the documented how 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.	We recommend that CBP create detailed procedures that document the review process for ACS profile change logs that includes the documented evidence of review.		X	2

NFR #	Condition	+Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-56	We noted that ACE audit logs are not being reviewed on a regular basis. We noted that procedures have been established, which requires that audit logs and events be reviewed on a weekly basis. However, at this time, procedures have not been implemented effectively.	We recommend that CBP implement the procedures that have been established for reviewing ACE audit logs on a weekly basis to be in compliance with DHS guidelines.	X		2
CBP-IT-09-57	We noted that five out of the 25 sampled audit logs did not contain any audit log information, such as login attempts, intruder detected, login failed, Access Control List (ACL) changed, object activity, etc. We did not receive audit log information for the following five selected dates: • February 16, 2009 • April 1, 2009 • April 7, 2009 • April 19, 2009 • May 4, 2009	We recommend that CBP conduct a more thorough review of audit logs to ensure that logs are capturing all necessary information and that no blank logs exist. Further, CBP should ensure that audit logs are configured properly to capture all information and activity on the system.	X		2
CBP-IT-09-58	We noted that passwords were not required to be case sensitive for a period of time during our testing and therefore did not meet CBP and DHS requirements. Further testing has shown that passwords currently are required to be case sensitive and that issue has now been resolved.	As this condition was addressed during the course of the audit fieldwork, therefore we have no further recommendation to CBP.	X		2

NFR #	Condition	+Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-59	We noted that formal procedures do not exist that describe the mainframe audit process and how to generate the system utility log reports for the mainframe ISSO's review.	We recommend that CBP create and implement formal procedures to document the generation of mainframe audit and system utility logs.	X		2
CBP-IT-09-60	We noted that one user was allowed 1,476 failed attempts to access a dataset to which they were not authorized before their access was suspended in the . We determined that the control option in the security software, which results in immediate suspension of any user who exceeds the specified number of violations, was not configured properly.	We recommend an adjustment to the Access Response control option to result in the immediate suspension of any user who exceeds the specified number of violations, which should be set a reasonably low number.	X		2

NFR #	Condition	+Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-61	We noted that there are six individuals within OIT that are in critical sensitive positions and have not had their periodic reinvestigations completed within the five year time frame. Specifically, of these six individuals, We noted the following: • Two individuals in critical positions had their reinvestigations completed a year or longer later than they should have been. • Four individuals in critical positions should have had their reinvestigations completed and are several months late. Of these four individuals, one has not had their investigation status updated since August 2002.	We recommend that CBP devote adequate resources to the completion of periodic reinvestigations and initial investigations that are due for all CBP personnel. Additionally, we recommend that CBP devote special attention to those individuals in critical sensitive positions requiring initial or periodic reinvestigations.	X		2
CBP-IT-09-62	We noted that the requirement to sign a rules of behavior is not implemented consistently. Out of 40 individuals with systems access across the country, ten individuals did not have a signed rules of behavior form on record. Additionally, 11 individuals signed the rules of behavior form months after the CBP Chief Information Officer (CIO's) requirement to sign the rules of behavior. These individuals have had access during fiscal year 2009.	We recommend that CBP implement a more consistent method of ensuring that all individuals with CBP systems access sign a rules of behavior form. We also recommend that methods be developed to ensure that individuals with access to any and all CBP systems have a rules of behavior form signed.	X		2

NFR #	Condition	+Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-63	We noted that is not configured to disable accounts after 45 days of inactivity for the full fiscal year, as required by CBP and DHS policy.	We recommend that CBP ensure that the Change Request to implement this control is completed, appropriately approved and implemented to disable accounts after 45 days of inactive as required by CBP and DHS policy.	X		2
CBP-IT-09-64	We determined that ISAs for all identified participating government agencies have not been documented as required by CBP and DHS policies.	We recommend that CBP develop a consistent and uniform naming scheme for all current and future ACS connections to facilitate the identification of all existing ACS connections as well as to facilitate in the reconciliation of existing ISAs. Finally, we recommend that once all ACS mission connections have been identified, that the appropriate ISAs are produced.	X		2
CBP-IT-09-65	We inspected access request documentation for 45 individuals who were granted ACE access during FY 2009. Initial access requests and approvals for 30 of these individuals could not be provided. Although confirmation that access is appropriate was provided for these 30 individuals, access approvals prior to the creation of the account were not maintained.	We recommend that CBP implement procedures to consistently document the access requests and approvals for any and all access creations and changes to ACE users.	X		2

NFR #	Condition	+Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-66	We 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. Additionally, We noted that one contractor who had access had separated from CBP but the account was not disabled until some time after they had separated.	We recommend that CBP investigate and implement a method to disable CBP accounts for separated employees and contractors upon their separation or before, as determined appropriate by security management and Human Resources.	X		2
CBP-IT-09-67	We inspected access request documentation for 45 individuals who had their access profiles modified during FY 2009. Access change requests and approvals for 14 of these individuals could not be provided. Although confirmation that the access is appropriate was provided for these 14 individuals, access approvals prior to the modification of the account were not maintained.	We recommend that CBP implement procedures to consistently document the access requests and approvals for any and all access creations and changes to user profiles.	X		2
CBP-IT-09-68	During our technical testing, patch and configuration management exceptions were identified on the . These conditions can be found in the table within the actual NFR.	During our technical testing, patch and configuration management exceptions were identified on the . The recommendations to address these conditions can be found in the table within the actual NFR.	X		2

NFR #	Condition	+Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-69	We inspected profile change reviews performed by CBP management for changes to SAP access profiles and noted that the profile review was ineffective. Specifically, We noted that only access deletes were tested in the review. These deletes remove an individual's access and do not increase an individual's access. Additions of new users and modification to user ID's (change/addition of profiles) were not part of the selected access changes that were reviewed. The review only consisted of deleted accounts and did not review any new accounts that had been added during the review period.	We recommend that the review of these access change logs is implemented on a periodic basis by an independent reviewer and that CBP modify their procedures to ensure that all types of access changes (adds, deletes and modifications) are reviewed to ensure that appropriate requests and approvals were documented.	X		2
CBP-IT-09-70	We noted that a memo was issued by the Component Chief Information Security Officer (CISO) to limit temporary/emergency access to to no more than four times per month. We noted that the policy was adjusted to restrict access to 25 times per user, per role, over a six month period. Taking into account this new control, We noted that during FY 2009, there was one individual who was granted access to a temporary/emergency role 43 times over a six month period.	We recommend that procedures be formalized around the process for granting temporary and emergency access to developers to ensure that access to these sensitive roles is restricted appropriately. Specifically, we recommend that CBP ensure controls are in place to confirm a user is authorized to be granted the role and that the individual had not been granted that role more than authorized by the Component CISO over a certain period of time.	X		2

NFR #	Condition	+Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-71	We noted that out of a selected 25 instances in which emergency access was granted to users, four individuals did not have Chief Information Security Officer (CISO) approval for their emergency access. Additionally, we noted that there was one instance in which the emergency access was granted in error without authorization and three instances where the improper form was used to request emergency/temporary access.	We recommend that CBP continue to implement processes to appropriately restrict and authorize access to temporary and emergency roles within .	X		2
CBP-IT-09-72	We noted that is not currently configured to restrict access to least privilege for performing job functionality as required by CBP policy.	We recommend that the Security Team continue to work with the Office of Finance to identify incompatible roles and that procedures are developed as part of the access control process to ensure that these role combinations are not granted to users.	X		2

NFR #	Condition	+Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-09-73	We inspected access documentation for three National SCOs created in FY 2009 and 37 Field SCOs created in FY 2009 and noted the following exceptions: • Two of the three National SCOs were not authorized and their roles were added by mistake. • One National SCO was approved through a manual recertification and initial authorization request and/or approval could not be provided. • 36 of the 37 Field SCO's initial authorization and approval could not provided. Instead, a recertification was provided, though the recertification did not note who performed the recertification and what authorization they had to perform the recertification.	We recommend that CBP develop and implement procedures to restrict access to the Field and National SCO roles and require documented authorization requests and approval for each person requiring access to the administrative capabilities.	X		2
CBP-IT-09-74	Multiple incidents of unprotected CBP information systems and data were found as a result of physical security walkthroughs. Additionally, passwords were obtained from two CBP employees through social engineering techniques.	We recommend that CBP review their information system security awareness programs to ensure that individuals are adequately instructed and reminded of their roles in the protection of both electronic and physical CBP data and hardware. Additionally, CBP employees and contractors should be made especially aware of the need to protect personally identifiable information as well as information marked "For Official Use Only."	X		2

Department of Homeland Security
FY2009 Information Technology - Notice of Findings and Recommendations – Detail

- **Federal Emergency Management Agency**

Department of Homeland Security
FY2009 Information Technology
Notification of Findings and Recommendations – Detail

Federal Emergency Management Agency

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-02	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

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-03	The process outlined for the Core Integrated Financial Management Information System (FMIS) recertification that initiated on January 12, 2009, required that a new FEMA Form 20-24 be approved and submitted to the Financial Systems Section (FSS) for all current IFMIS users, and also required revocation of any accounts that could not be validated. However, we noted that the requirement to revoke access is not documented in the *Office of the Chief Financial Officer (OCFO) Procedures for Granting Access to IFMIS* or FEMA Instruction 2200.7, *IFMIS User Access Policy and Procedures*. We reviewed access authorization documentation for a selection of 40 active Core IFMIS user accounts, noted that two accounts did not have a FEMA Form 20-24 completed after January 12, 2009, and concluded that the accounts were not appropriately recertified and validated as belonging to current users. Additionally, access for the two accounts was not revoked, per the process described in the memorandum.	• Revise applicable FEMA policies and procedures to require that any accounts which are not positively verified during the periodic review of IFMIS accounts for recertification are revoked until a new approved FEMA Form 20-24 is received by FSS personnel. • Dedicate resources to ensure that consistent application of FEMA policies/procedures and DHS policy is performed by revoking access for all IFMIS application accounts not validated through submission of a new FEMA Form 20-24 as part of the periodic account review.		X	3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-06	During the FY 2009 follow-up testwork, we noted that FEMA has obtained and distributed a reference guide that documents the purpose of Core IFMIS system security functions and their associated permissions and configuration options. However, the guide does not include policies and procedures addressing process requirements for adding, deleting, and modifying Core IFMIS system security functions. We also determined that no additional policies and procedures have been developed by FEMA or the IT developer of IFMIS that establish a process for implementing change controls for the maintenance of system security functions and their associated privileges. FEMA management represented to us that access to the security menu is limited, individuals with access to the menu do not use their privileges to delete, create, or modify functions, and changes are made to Core IFMIS system security functions through the standard change control process. However, we noted there are no controls in place to restrict and/or monitor the use of these privileges to ensure that system security functions are not modified, created, or deleted. Based on our testwork, we concluded that a formalized process for modifying specific Core IFMIS system security functions to ensure that appropriate privileges are created, documented, approved, and monitored does not exist.	Develop and implement policies and procedures documenting the process of adding, deleting, and modifying Core IFMIS system security functions to ensure that the proper controls are in place for modifying user account privileges. Additionally, these policies and procedures should include requirements over the monitoring of the usage of function modification privileges, configuration changes implemented for Core IFMIS system security functions, and requirements over updating system documentation for changes in the system security functions.		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-12	The standard operating procedure (SOP) for recertification of NEMIS positions has not been finalized and implemented to require a semi-annual review of all user roles within the NEMIS Access Control System (NACS), including privileges related to access to specific NEMIS applications and modules. Furthermore, we determined that FEMA Enterprise Operations staff completed development of the technical infrastructure within NACS to support the recertification effort at the end of FY 2008. However, we determined that the FY 2008 recertification of NEMIS/NACS roles was not completed and FEMA initiated but did not complete the FY 2009 recertification that was scheduled for completion by April 30, 2009.	• Dedicate resources to complete the on-going review of NEMIS user access for FY 2009 and perform subsequent reviews, as required by DHS policy. • Finalize and fully implement formal procedures for conducting the NEMIS recertification process and retaining auditable records, in accordance with DHS policy.		X	3
FEMA-IT-09-13	During FY 2009, we performed test work over security controls in place for Core IFMIS, NEMIS, and the FEMA iPass/virtual private network (VPN) remote access system, including follow-up testing on the prior year finding. Through comparison of active Core IFMIS, NEMIS, and iPass/VPN remote access accounts against a list of FEMA employees that had separated from employment since October 1, 2008 and determined that 1 Core IFMIS account, 62 NEMIS accounts, and 28 iPass/VPN accounts remained active and unlocked after the account holder's separation from FEMA. Additionally,	• Evaluate and, if appropriate, revise existing procedures over removal of separated user access to IT systems to identify weaknesses that contribute to untimely removal of separated individuals from the information systems. • Ensure that procedures and processes 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.		X	3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	of the 28 active iPass/VPN accounts, we determined that 11 also had at least one active NACS role, indicating active remote access privileges to both the FEMA network and NEMIS.				
FEMA-IT-09-17	During the FY 2009 follow-up testwork, we noted that FEMA has a SOP that outlines the controls intended to address the risk associated with the Core IFMIS developers having the ability to migrate changes to the Core IFMIS production environment. The SOP, in particular, requires the locking and unlocking of the *ifmiscm* account during the implementation of software changes into production by system administrators. However, we determined that no formal procedures or processes are documented for performing reviews to verify that only authorized changes to the *ifmiscm* directory and sub-directories are implemented into production by the developers. Additionally, we determined that although informal reviews of the directories were performed during the fiscal year, they were not routinely completed, and documented evidence of the reviews performed was not retained.	Implement compensating controls to address the risk associated with the segregation of duties weakness related to developers making changes to the production environment. Specifically, FEMA should develop and implement policies and procedures for conducting periodic reviews to verify that only authorized changes are made to the Core IFMIS production directories and subdirectories by developers using the *ifmiscm* account. Additionally, the policies and procedures should include requirements for retention of auditable evidence of the reviews that are performed.		X	2
FEMA-IT-09-19	FEMA Enterprise Operations personnel informed us that the *SOP, Monitoring Sensitive Access to NEMIS,* was developed to outline the process for monitoring sensitive access to the NEMIS operating system. Based upon our review of the	• Revise the *SOP, Monitoring Sensitive Access to NEMIS,* to ensure that it states that the scope of the procedures includes all servers defined in up-to-date system documentation as supporting NEMIS		X	3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	SOP, we noted that a list of NEMIS servers that are considered to be within the scope of the SOP are listed, but that specific hosts and server designations are not clearly defined. In particular, approximately 30 separate IT components are described and certain servers supporting web-facing applications for registration, applicant inquiry, and assistance processing are listed. However, based on additional testwork and corroborative inquiry of NEMIS personnel, we determined that at least 170 operating system servers for NEMIS are not comprehensively included in the scope of the SOP. Additionally, FEMA informed us that outlined procedures for conducting the required reviews of audit trails every three days and retaining evidence for at least a year have not been implemented and the NEMIS operating system activity is not currently being logged or monitored. Additionally, we noted that no application or tool is currently in place to support the audit logging function on the NEMIS Linux server. Consequently, we concluded that FEMA has partially addressed the prior year recommendation by including review and retention requirements in the SOP for monitoring NEMIS activity. However, the SOP has not been implemented on the operating system software supporting NEMIS and does not include all	system software within system boundaries for the financial applications and modules. • Acquire and deploy appropriate tools on system software and operating systems supporting the NEMIS financial applications 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.			

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	NEMIS operating system servers within its scope.				
FEMA-IT-09-22	During our FY2009 follow-up testwork, we noted that FEMA was unable to take corrective action to establish and implement an alternate processing site for the NEMIS application. Additionally, a current waiver over the lack of an alternate processing site did not exist. FEMA security personnel described compensating controls surrounding the contingency planning process. Specifically, FEMA management informed us that in FY 2009 the NEMIS Contingency Plan was partially tested through an annual table-top exercise to restore five of the NEMIS servers from backup tapes at the Mt. Weather Emergency Operations Center (MWEOC). Furthermore, FEMA management informed us that compensating controls were also provided through performance of full backups of critical NEMIS data on a regular basis and the transfer of these tapes to an offsite backup storage facility. However, during further testwork and analysis, we determined that there were weaknesses in the compensating controls described by FEMA management. In particular, we noted that while the contingency plan was tested, a full restore of all the of the NEMIS servers was not performed. Additionally, backup tapes for NEMIS are not fully tested on a periodic basis. (Please refer to NFRs FEMA-IT-	• 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 a waiver for approval in accordance with DHS policy regarding waivers, and ensure that compensating controls over the alternate processing site are effective and documentation of their effectiveness is maintained as auditable records.		X	3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	09-24 and FEMA-IT-09-25 for further information.)				
FEMA-IT-09-24	In FY 2009, we conducted follow up procedures to determine if FEMA had implemented corrective action for the prior year finding and determined that NEMIS backup tapes were not regularly tested during FY 2009.	Periodically test NEMIS backup tapes at a frequency that is in compliance with FEMA and DHS policy.		X	2
FEMA-IT-09-25	During our FY 2009 audit, we conducted follow up procedures and determined that full-scale testing of the NEMIS Contingency Plan, in accordance with DHS requirements for high impact availability systems, has not been conducted. FEMA provided us with the testing results of limited table top testing that was performed to test the local restoration for four of approximately 170 servers that comprise NEMIS. However, the DHS-approved waiver obtained in FY 2008 that listed table-top testing as a compensating control for FEMA's inability to fully test NEMIS, was expired. In FY 2009 we also determined that the existing NEMIS 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	• Update the NEMIS Contingency Plan so that it meets the requirements of DHS policy for high impact availability systems. Additionally, ensure that the plan comprehensively addresses the numerous sub-systems within NEMIS so that detailed information exists over the current system architecture, critical processing priorities, detailed SOPs for systems recovery and other required components in accordance with DHS guidance. • Conduct documented annual tests of the NEMIS Contingency Plan that address all critical phases of the plan and update the plan with lessons learned, as necessary and in accordance with DHS and NIST requirements. • If the NEMIS contingency plan cannot be tested in accordance with DHS guidance		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	names and information over the various modules of NEMIS, was not appropriately documented to reflect the current operating environment. • The contingency plan did not include detailed procedures necessary to fully restore the NEMIS application in the event of an emergency. • System/Application Recovery Priority Classification have not been defined. • Service Level Agreements and Memorandum of Understandings (MOU) were not included in the plan. • The Business Impact Analysis included in the contingency plan was completed in 2004 and not adequately documented.	for high impact availability systems, FEMA should develop, implement, and document effective compensating and mitigating controls.			
FEMA-IT-09-28	In FY 2009, we performed follow-up testwork over NEMIS non-emergency system changes that occurred under the process established during the time frame of October 1, 2008 to February 28, 2009 prior to the change in the NEMIS development contractors. Specifically, of the 25 NEMIS non-emergency application level System Change Requests (SCR) tested, we noted the following exceptions: • Seven of 25 SCRs did not obtain documented SCR approval prior to development; • 21 of 25 SCRs did not obtain documented Technical Development Laboratory (TDL) approval prior to implementation in the test environment;	We recommend that FEMA, in accordance with DHS and FEMA policy, ensure that when implementing the new NEMIS non-emergency change control process that all required approvals are obtained prior to development and implementation of changes into production. Additionally, FEMA should ensure that the appropriate testing is conducted and that the testing documentation is appropriately retained according to FEMA and DHS policy.		X	3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• Two of 25 SCRs did not obtain documented Technical Review Committee (TRC) approval prior to implementation into production; and • Eight of 25 SCRs did not have testing documentation to demonstrate that testing occurred.				
FEMA-IT-09-29	We tested a selection of three NEMIS emergency application level SCRs that occurred in the time frame of October 1, 2008 to February 28, 2009 before NEMIS configuration management responsibility was transitioned to the new contractor. Of the three SCRs tested, we noted that one was missing the required initial approval prior to moving the change into the TDL environment for testing.	We recommend that FEMA, in accordance with DHS and FEMA policy, ensure that when implementing the new NEMIS emergency change management process that all required approvals are obtained prior to development and implementation of changes into production. Additionally, FEMA should ensure that the appropriate testing is conducted and that the testing documentation is appropriately retained according to FEMA and DHS policy.		X	3
FEMA-IT-09-38	In FY 2009, we performed follow-up test work and determined that the NFIP contractor had documented system roles and had implemented capabilities for enforcing segregation of duties for users within the Traverse application currently. Also, as a mitigating control, the NFIP contractor reviews a User Log report generated by Traverse for each financial user's system access, which is reviewed and signed off on every month to ensure that the appropriate privileges are assigned. However, incompatible duties that must remain segregated when granting	Continuing with our prior year recommendation, NFIP should document Traverse duties that are incompatible and develop and implement policies and procedures for properly segregating incompatible duties within the system when granting and maintaining access.		X	1

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	and maintaining user access to the Traverse application have not been documented. We were also reviewed the *Traverse Standard Operating Procedure (SOP) for Financial Processes* and noted that it states that a Traverse user log is produced to show appropriate user access to perform accounting duties and usage of the Traverse accounting system. However, the SOP does not include policies and procedures regarding segregating incompatible duties within Traverse.				
FEMA-IT-09-39	The Traverse and TRRP Contingency Plan has not been tested, and a test of the system fail-over capability at the alternate processing site has not been conducted. Also, we did not receive the requested NFIP Certification & Accreditation (C&A) package that includes the Traverse and TRRP Contingency Plan and the test results. As a result, we determined that a current contingency plan for the TRRP and Traverse applications does not exist. At the time of our audit testwork, we were informed that due to delays in implementation of the new system of record, NFIP and the NFIP IT contractor had initiated efforts FEMA's Chief Information Security Officer (CISO) to recertify and accredit the NFIP legacy system and update and test the Traverse and TRRP Contingency Plan and NFIP Bureau and Statistical Agent Disaster Recovery and Continuity of Operations Plan.	• Complete the documentation and testing of the TRRP and Traverse Contingency Plan, to include all critical phases of the plan in accordance with DHS policy requirements for high impact systems. In addition, NFIP should conduct a test of the system fail-over capability at the alternate processing site and ensure that TRRP and Traverse processing is tested in accordance with DHS guidance. • Revise the NFIP Bureau and Statistical Agent Disaster Recovery and Continuity of Operations Plan to incorporate the Traverse and TRRP alternate processing facility and the TRRP critical data files in accordance with DHS guidance for high impact systems. Additionally, the revised plan should be tested and updated with lessons learned from the testing.		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Furthermore, the NFIP Bureau and Statistical Agent Disaster Recovery and Continuity of Operations Plan provided for auditor review does not incorporate the Traverse and TRRP alternate processing facility or TRRP critical data files.				
FEMA-IT-09-45	We determined that access for Core IFMIS Oracle database users was appropriately documented and authorized. Thus, this portion of the prior year recommendation, as it relates to the Core IFMIS database, is closed. Additionally, we reviewed a selection of 40 Core IFMIS Forms 20-24 (access request forms) for users who were either new IFMIS users during the fiscal year or whose access profile changed during the fiscal year outside of the recertification process. We determined that of the 40 active application users tested: • Two users did not have a completed Form 20-24 on file; • FEMA was unable to provide evidence that the initial account creation of ten accounts during FY 2009 were authorized; and • FEMA was unable to provide evidence that modifications to account privileges for ten accounts were authorized. FEMA management additionally informed us that recertification of IFMIS Oracle database accounts had not been performed during FY 2009. Consequently, we concluded that while certain	Review and revise the Office of the Chief Financial Officer's existing *Procedures for Granting Access to IFMIS* to require authorization of new and modified Core IFMIS user accounts by supervisors, program managers, and contracting officers' technical representatives (COTRs) in accordance with DHS guidance. The requirements should also include the retention of Core IFMIS access authorization documentation. • Develop and implement of policies and procedures over periodic recertification of all user access to the Core IFMIS Oracle database, and retain auditable records in accordance with DHS policies and procedures as evidence that recertifications are conducted and completed periodically. Additionally, if the Core IFMIS/G&T IFMIS merger is performed in FY 2010, ensure that a recertification of IFMIS Oracle accounts is performed prior to the merger.		X	3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	corrective actions to address weaknesses over Core IFMIS account management have been implemented, FEMA has not consistently maintained documentation for initial account creation or subsequent account modification for the application, and FEMA has not developed or implemented a process to recertify accounts on the IFMIS Oracle database.				
FEMA-IT-09-46	We determined that a MOU and Interconnection Sharing Agreement (ISA) was documented, accepted, and signed by FEMA and the Department of Treasury on April 22, 2009. Consequently, while the prior-year recommendation was addressed, the interconnection was operating without authority for a majority of the fiscal year and the NFR is re-issued.	No recommendation is required for this weakness that existed for the majority of FY 2009 because it was remedied on April 22, 2009 when the MOU and ISA were signed by FEMA and Treasury management.		X	1
FEMA-IT-09-48	During the FY 2009 audit, we were informed that internal vulnerability scans are conducted every month on the NEMIS systems. However, FEMA personnel informed us that identified vulnerabilities and related corrective actions are reported and tracked via emails and not documented in POA&Ms.	Complete planned corrective actions to develop and implement an SOP that outlines the process for formally reporting and tracking resolution of weaknesses identified during internal NEMIS vulnerability scans in accordance with DHS guidance.		X	3
FEMA-IT-09-50	During FY 2009 follow-up testwork, we obtained evidence that "superuser" activity reports for CORE IFMIS were appropriately reviewed by FSS personnel in accordance with FEMA and DHS policy. Consequently, this portion of our recommendation for prior year NFR FEMA-IT-	• Revise and implement policies and procedures that document requirements for configuring, retaining, and reviewing audit trails for the Core IFMIS application and database, in accordance with DHS policy. Additionally, ensure that all DHS		X	3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	08-50 is closed. However, FSS personnel informed us that failed database login attempts and activity performed by application users with the "superuser" role remain the only forms of activity logged and monitored for Core IFMIS. Other activity on the application and database required to be logged by DHS policy, including successful logins, access modifications, and changes to user profile, are not enabled within Core IFMIS. Additionally, we noted that a procedure does not exist to establish the process for reviewing and retaining evidence of these logs once the configurations are implemented. FEMA reported in the FY 2008 audit remediation plan that internal instructions describing the review process for these two reports were documented. We reviewed the *SOP, Monitoring of IFMIS Database Audit Logs*, and determined it addresses the process for reviewing the daily Oracle failed login report. However, documented instructions concerning the review of weekly "superuser" reports were not provided to us during the audit.	requirements are met through this process, including appropriate supervisory review and retention. • Implement configurations on the Core IFMIS application and database in accordance with DHS policy to ensure that audit logs sufficiently record required auditable events and activities.			
FEMA-IT-09-51	During our FY 2009 integrated test work, IT Enterprise Operations personnel informed us that the *SOP for Handling of Oracle Audit Logs* was implemented for the databases specified in the SOP and that evidence of audit log reviews are retained. However, we noted that weaknesses in NEMIS database audit controls still exist, as	Revise and enforce the *SOP for Handling of Oracle Audit Logs* to ensure that the procedures are developed and implemented in accordance with DHS guidance, to include: • All databases within the defined system boundaries that support		X	3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	follows: • During our inspection of the SOP, we noted that it requires the procedures to be performed for two specific NEMIS databases, the National Processing Service Center (NPSC) database and the Consolidated Master database. However, through additional testwork, we noted that NEMIS has at least 23 databases. Consequently, not all of the databases that comprise NEMIS are included within the scope of the SOP, and we were informed by IT Enterprise Operations personnel that no additional SOPs exist that address auditing logging for the remaining 21 databases. • The SOP has not been updated to require that successful logins, access modifications, highly privileged user account activity, and changes to user profiles are logged and reviewed. • On four of the NEMIS databases related to financial processing that we selected for testing, we determined that configurations are not fully enabled so that a review of audit trails and activity defined by DHS policy requirements can be completed. • Based on our review of audit log documentation, we noted that reviews of audit logs for NEMIS databases are performed by the database administrators (DBAs) who have been assigned	NEMIS financial applications and modules within the scope of the SOP; • Requirements for audit logging and retention of audit trails; • Periodic reviews of audit trails for NEMIS databases; and • Appropriate segregation of duties principles. Implement configurations on NEMIS databases in accordance with DHS policy over required auditable events and activities.			

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	administrator privileges to administer the databases. Thus, we determined that database audit log review duties are not appropriately segregated from DBA duties.				
FEMA-IT-09-52	In FY 2009, we performed follow-up testwork and were informed that FEMA is currently in the process of updating the NEMIS patch management policy and that the finalized policy had not been implemented. However, FEMA could not provide us with a copy of the requested draft policy that was reported as under development for our review. Based on additional inquiry, we also determined that the timeframe for implementing patches on FEMA systems has not been established, in accordance with DHS guidance.	We recommend that FEMA dedicate the appropriate resources to complete efforts to document, finalize, and implement comprehensive patch management policies and procedures for NEMIS, in accordance with DHS policy. Additionally, FEMA should ensure that these procedures include requirements for responding to DHS Security Operations Center (SOC) and DHS Computer Security Incident Response Center (CSIRC) notifications to ensure compliance with the timely implementation of required patches.		X	3
FEMA-IT-09-53	During our FY 2009 audit, we reviewed FEMA's Remediation Plan and we noted that FEMA management had reported that corrective action to update the *NEMIS SSP* had been fully implemented. We obtained the *NEMIS SSP* dated February 16, 2009 for our review and noted that the plan had been revised since our prior year audit. However, upon further inspection, we determined that the current plan does not fully document the system's boundaries, define all of the NEMIS subsystems and major applications, nor establish security responsibilities for the various system components.	Ensure that *NEMIS SSP* is updated in accordance with DHS policy so that the system's boundaries, components, and responsibilities surrounding the various subsystems and major applications of NEMIS are accurately and comprehensively documented in the plan.		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-54	In FY 2009, KPMG performed testwork over Traverse configuration management. Upon inspection of the *System Change Control Procedures*, that address Traverse configuration management, we noted that the procedures outline steps for controlling changes during the change control process for Traverse. However, the procedures do not include comprehensive configuration management guidance that addresses the following elements required by FEMA and DHS policy: • configuration identification • configuration control • version control • configuration status accounting • configuration audits • Establishing a Change Control Board (CCB) or TRC for evaluating changes prior to production.	We recommend that NFIP management ensure the implementation of an updated version of the current Traverse configuration management procedures that comprehensively addresses FEMA and DHS requirements.		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-56	Based on observations conducted with FSS and G&T IFMIS database personnel, we identified the following weaknesses in database security controls: • A manual review of inactive G&T IFMIS database accounts is performed on a monthly basis to disable accounts which have not been used in the past 90 days. However, since IFMIS is categorized as a high impact system, reviews are required to identify accounts that have been inactive for 45 days. • Emergency and temporary access to the G&T IFMIS database, including access for contractor development personnel, is approved by the FSS Chief and/or their staff, not by the FEMA CISO/Information System Security Manager (ISSM) or a designee, as required by DHS policy.	• Revise the formal process for reviewing and disabling inactive G&T IFMIS Oracle database user accounts to adhere to DHS policy over disabling inactive accounts on high impact systems. • Configure all G&T IFMIS Oracle database user accounts to adhere to DHS policy for passwords and authenticator controls. • Establish a formal process for granting emergency and temporary IFMIS G&T database access that includes segregation of duties considerations and appropriate approval from FEMA management in accordance with DHS policy.	X		3
FEMA-IT-09-57	Based on observations conducted with FSS and G&T IFMIS database personnel, we determined that Oracle database audit trails are not configured to capture any activity, including failed login attempts or administrator-level actions.	• Configure the G&T IFMIS databases to log events and retain audit records in accordance with DHS policy; and • Develop and implement policies and procedures surrounding the requirements for G&T IFMIS database audit logging to include the periodic review of database audit logs in accordance with DHS policy.			3
FEMA-IT-09-58	Based on collaborative inquiry with FSS and application and database administrators, we concluded that a management review to validate the appropriateness of G&T application and	• Establish a formalized process for the recertification of the G&T IFMIS application and database accounts or include G&T IFMIS in the scope of the	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Oracle database user accounts has not been formally implemented or performed by FSS this fiscal year. Additionally, FSS management further informed us that no recertification of accounts was conducted when the application was acquired and brought online at FEMA in FY 2007 and has not been conducted since.	formalized processes for the recertification of Core IFMIS application and database accounts. Additionally, ensure that the established processes are developed and implemented in accordance with DHS guidance. • Conduct an immediate recertification of user account access on the G&T IFMIS application and Oracle database to validate the continued appropriateness of access as being commensurate with job responsibilities.			
FEMA-IT-09-59	In FY 2009, we performed test work over the G&T "ifmiscm" account, to determine the controls in place for the migration of changes into production. The "ifmiscm" account is 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 are also responsible for migrating application code changes into the production environment using the "ifmiscm" account. Additionally, when we inspected the account, the G&T "ifmiscm" account was not locked on May 15, 2009, which allowed the contractor unrestricted access to the production environment. We were further informed by FEMA personnel that access to that account is not limited or monitored on a periodic basis.	• Limit the contracted developers' access to the G&T IFMIS production environment to "read only" and segregate the responsibility for deploying application code changes into production from the contractor to an independent control group. • If business need requires that the segregation of duties cannot be immediately implemented, FEMA should document policies and procedures to mitigate the risk associated with the segregation of duties weakness noted in accordance with DHS guidance.	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-60	During our testwork, we concluded that the "Legacy NFIP IT System" C&A pertaining to the Traverse application, TRRP application, and NFIP LAN expired on October 4, 2008. Consequently, the legacy system has since been operating without a current Authorization to Operate (ATO). Furthermore, we were not provided the requested NFIP C&A package consisting of the following artifacts: • FIPS 199 Categorization • Privacy Impact Assessment • E-Authentication • Risk Assessment • SSP • Contingency Plan • Security Test and Evaluation • Contingency Plan Testing • Security Assessment Report • ATO • Annual NIST SP 800-53-based Self-Assessments	We recommend that NFIP immediately work with FEMA's CISO to complete the recertification and accreditation of the NFIP legacy system in accordance with applicable DHS policies and Federal guidance.	X		2
FEMA-IT-09-61	The G&T instance of IFMIS was brought online at FEMA in FY 2007 after acquisition from the Department of Justice. However, we determined that a C&A of the system had not been performed, and the system has not received an ATO. Specifically, the following C&A elements have not been completed, documented, or approved for G&T IFMIS and will not be for the	• Formally designate an ISSO and DAA for G&T IFMIS. • Immediately work with FEMA's Information Security Office to certify and accredit the G&T IFMIS instance in accordance with applicable DHS policies and Federal guidance. If FEMA	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	remainder of the fiscal year: • FIPS 199 categorization • Privacy Impact Assessment • E-Authentication • Risk Assessment • SSP • Contingency Plan • Security Test and Evaluation • Contingency Plan Testing • Security Assessment Report • ATO • Annual NIST SP 800-53-based Self-Assessments In addition, we determined that at the time of our test procedures, neither an ISSO nor a DAA had been formally designated for the G&T instance of IFMIS by FEMA management.	management makes a business decision to conduct a C&A of IFMIS after the merger and not over the existing G&T IFMIS instance, as a mitigating control, FEMA should immediately conduct an assessment of key controls to identify security weaknesses and determine the operational risks related to IFMIS G&T. The weaknesses identified should be documented with plans for accelerated remediation efforts or related risks should be formally accepted by FEMA in accordance with DHS guidance.			
FEMA-IT-09-62	We reviewed the *VPN Rules of Behavior for Users Behind Corporate Firewalls*, dated December 5, 2002, and noted that individual VPN access request forms are required to be completed, approved by managers, and submitted to the National Help Desk, Enterprise Service Desk (ESD). However, we noted that the requirements do not include approval by the system owner or a designated representative, as required by DHS policy. We reviewed a blank VPN Access Request Form and noted that an approval block titled "For	• Revise and implement policies and procedures for documenting, reviewing, and approving individual VPN user accounts for employees of external entities requiring access to the FEMA network via VPN access and ensure that sufficient resources are dedicated to appropriately authorizing accounts on behalf of the system owner or a designee, according to FEMA and DHS policy. • Develop and implement policies and procedures in accordance with DHS	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	FEMA Office of Cyber Security (OCS) Use Only" is included and that the form states that all VPN requests must be approved by the FEMA OCS. We reviewed a selection of 25 completed forms for active VPN user accounts and determined that, while the forms were approved by the requestor's manager or supervisor, none of the forms had an approval noted by OCS or an appropriate designated representative of the system owner. Additionally, we were informed by FEMA IT security personnel that OCS, as referred to in the Rules of Behavior and the request form, 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. Additionally, we were informed that 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. VPN accounts are managed within the FEMA LAN, specifically the Active Directory environment, and subsequently added to the Cisco Access Control Server (ACS) that permits VPN access. However, through test work conducted over the FEMA LAN, we determined that a recertification of network user accounts is not performed.	policy to perform a periodic recertification of all VPN user access and retain auditable records as evidence that recertifications are conducted and completed periodically.			

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-63	We noted the following weaknesses in the process for authorizing remote VPN access to external organizations, including state emergency management agencies and FEMA contractors: • 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. Additionally, we noted that the current process in place for granting remote access to the FEMA network through VPN is not in compliance with FEMA, DHS, and NIST guidance. Specifically, we noted the following weaknesses: • Access for state emergency management agencies and FEMA contractors to load the VPN client onto state or contractor owned equipment to connect to the FEMA LAN is approved by the SOC. However, DHS policy requires that any non-DHS equipment	• 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, FEMA should 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 Component CISO/ISSM to connect to non-DHS equipment. • Draft and formalize ISAs, MOUs, and MOAs delineating security responsibilities by FEMA and external organizations when connecting through non-DHS equipment to the FEMA network via VPN access. 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. • Ensure that agreements related to VPN access are reviewed and recertified on a	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	connecting to a DHS network must be authorized by the Component CISO/ISSM. • Two-factor authentication is not used for VPN access, as required by DHS policy. • 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 the Inter-Agency VPN Agreements have not been documented and that this requirement is inconsistent with DHS policy, which requires ISAs or Memoranda of Understanding/Memoranda of Agreement (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 site surveys were outdated, did not contain the level of technical granularity describing the external network security controls required to appropriately approve a connection to the	periodic basis, specifically, when a major system change occurs or every three years, in accordance with DHS policy. • Implement and require two-factor authentication for all remote access to the FEMA network, including VPN and all other tools used for remote access, in accordance with DHS policy and FIPS 140-2.			

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	FEMA LAN, and were not independently verified for accuracy by FEMA. Additionally, we determined that 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 multiple connecting networks listed in single ISAs with external entities is not being evaluated by the FEMA SOC to ensure the security requirements are appropriately implemented.				
FEMA-IT-09-64	The Core IFMIS database is not configured to retain a history of account passwords in order to prevent reuse. However, DHS guidance requires passwords to be configured so that users cannot reuse the last eight passwords.	• Configure the Core IFMIS Oracle database to enforce DHS policy requirements regarding the reuse of user passwords. • Develop and implement procedures to ensure that those with systems administration and security responsibilities over the Core IFMIS database environment are made aware of DHS, FEMA and Federal system security requirements and guidance and are properly trained in those requirements and guidance.	X		2
FEMA-IT-09-65	We determined that of 40 access request forms (Form 20-24) for active G&T IFMIS application users selected:	We recommend that FEMA review and revise the Office of the Chief Financial Officer's existing *Procedures for Granting Access to IFMIS* to specifically require the authorization	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• FEMA was unable to provide documented evidence that the initial account creation of 11 accounts in FY2009 were authorized; and • FEMA was unable to provide documented evidence that modifications to account privileges for 11 accounts were authorized. Additionally, we requested for review a selection of eight G&T IFMIS Oracle Database User Access Control Forms for G&T IFMIS Oracle database users whose accounts were created during the fiscal year. We determined that of the eight users selected, two did not have documented evidence that the accounts were authorized or appropriately approved prior to creation.	of new and modified G&T IFMIS user accounts by supervisors, program managers, and/or contracting officers' technical representatives for the G&T IFMIS application and database in accordance with DHS guidance. The requirements should also include retention guidance for G&T IFMIS access authorization documentation.			
FEMA-IT-09-66	Based on observations conducted with IT Enterprise Operations database personnel over the four databases selected for test work that process NEMIS financial data, we determined that DBA account passwords are not required to be "strong passwords." Specifically: • No minimum password length is enforced. • Password complexity is not required so that passwords include a combination of upper/lowercase letters, numbers, and special characters. • Reuse of previous passwords is not prohibited. • Passwords are not configured to expire and forced to be changed after a predetermined	• Configure all NEMIS Oracle databases to enforce the DHS policy for passwords and authenticator control requirements, including expiration, reuse, and length and complexity. • Develop and implement procedures to ensure that those with systems administration and security responsibilities over the NEMIS database environment are made aware of DHS, FEMA and Federal requirements and guidance and are properly trained in those requirements and guidance.	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	length of time.				
FEMA-IT-09-67	Based on observations conducted over the FEMA domain policy and an end-user workstation, we determined that workstations are configured to activate a password-protected screensaver after 15 minutes of inactivity, rather than the five minute inactivity threshold required by DHS policy.	Implement the plan to configure the FEMA LAN domain security policy to automatically activate a password-protected screensaver on end-user workstations after five minutes of inactivity, consistent with DHS policy.	X		2
FEMA-IT-09-68	We determined that a C&A of PARS was not performed and the system had not received an ATO. Specifically, no evidence exists to support that the required C&A elements have been completed, documented, or approved for PARS. In addition, we determined that at the time of our test procedures, neither an ISSO nor a DAA had been formally designated by FEMA management for PARS.	• Formally designate an ISSO and DAA for PARS. • Immediately work with FEMA's Chief Information Security Office to certify and accredit PARS in accordance with applicable DHS policies and Federal guidance.	X		3
FEMA-IT-09-69	Upon inspection of the *NFIP Technical Services Department Production Systems Control Unit Procedures*, that addresses TRRP configuration management, we noted that the procedures outline steps for controlling changes during the change control process for TRRP. However, the procedures do not include a comprehensive configuration management guidance that addresses the required elements for a comprehensive configuration management plan in accordance with FEMA and DHS policy.	Ensure implementation of an updated version of the current TRRP configuration management procedures that comprehensively addresses FEMA and DHS requirements. The updated procedures should require initial approvals of OSRs and establish a process for obtaining CCB and TRC approvals prior to implementing changes into production, in accordance with DHS policies and procedures.	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Furthermore, we performed testwork over initial approval, testing, and implementation of a selection of 25 TRRP changes made in FY 2009 and noted the following exceptions: • 16 out of the 25 changes did not obtain initial OSR approvals prior to developing the change. ▪ All 25 changes did not obtain TRC or CCB approval for production implementation approval.				
FEMA-IT-09-70	We were informed by the NFIP contractors, that no patch management policy and procedures exist for the Windows operating system which supports the Traverse application and the NFIP LAN. Additionally, we determined that while NFIP has documented the *Traverse System Software Procedures* which outline the process to initiate, approve, test, and implement operating system upgrades into production, the procedures do not specifically address patch management. Furthermore, the procedures do not provide robust guidance for approving, installing, and testing patches, according to DHS requirements.	Document, finalize, and implement comprehensive patch management policies and procedures for the NFIP LAN and the Traverse operating system, in accordance with DHS policy. Additionally, NFIP should ensure that this procedure includes requirements for authorizing, testing, and approving patches to be implemented into production and responding to DHS SOC and DHS CSIRC notifications to ensure compliance with the timely implementation of required patches.	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-71	During our after-hours physical testing, we identified 42 written unprotected passwords, four external memory drives, two documents labeled as 'For Official Use Only (FOUO)', two badges, two instances of unsecured Personally Identifiable Information (PII), one instance of a written server name with an Internet Protocol (IP) address, and one unsecured laptop.	We recommend that appropriate FEMA management review the effectiveness of existing security awareness programs designed to protect electronic and physical data and ensure that individuals are adequately instructed and reminded of their roles in the protection of both electronic and physical FEMA data and hardware. Additionally, FEMA employees and contractors should be made aware of the need to protect PII, as well as information marked "FOUO."	X		2
FEMA-IT-09-72	Through discussions with FSS personnel, we determined that the description of mitigating and compensating controls noted in the approved DHS Waivers and Exceptions Request for Core IFMIS does not accurately reflect the operating environment for the Core IFMIS application and database. Specifically: • Successful database connections are not logged, as described. • Superuser activity is monitored at the application level. However, no other audit logs or records described in the request are reviewed. • The exception request states that "direct access to the IFMIS database is restricted to approximately 70 users, and is read-only in nature for the purposes of running ClearAccess report functions", however direct access to the database includes DBAs	• Submit a revised DHS Waivers and Exceptions Request Form that accurately reflects the mitigating and compensating controls in place on the Core IFMIS environment to justify exception from DHS policy concerning audit logging on the Core IFMIS database. • Ensure that future waiver and exception requests involve the input, review, and approval of system owners and administrators to provide adequate assurance that the documented risk mitigation strategies accurately reflect security controls in place. • Ensure that FEMA establishes a more formal communication process for providing approved waivers back to system owners so that any requirements	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	with read/write privileges in addition to ClearAccess read-only users. • Approval was granted by the DHS CISO with an added condition that FEMA periodically capture the audit records at a database level and compare them to the application logs to ensure that data is correct at the application level. However, the requirement had not been implemented at the time of our FY 2009 audit procedures. Consequently, we concluded that the request for an exception to DHS policy requirements related to audit logging for the Core IFMIS Oracle database was approved by the DHS CISO based on inconsistent or inaccurate information about the system environment and current controls in place to mitigate the risk of not implementing DHS policy. Additionally, the DHS CISO's condition for granting approval has not been met by FEMA.	for the implementation of additional controls are reviewed and executed appropriately and timely.			

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-73	Based on observations conducted with FEMA IT security personnel and IFMIS UNIX system administrators, we determined that the "root" account access 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 local access to the root account is not locked down. Additionally, FEMA has not enforced the use of the switch user command, "sudo," which requires system administrators to login with their userID and switch over to the root account to ensure who is accessing the account is logged and authorized. Additionally, we determined that system logs and reports of administrator activity, including the "sudo" log, which monitors actions performed by administrators while acting as the "root" account, were not reviewed by FEMA management personnel independent of the system administration staff.	• FEMA should develop and implement policies and procedures over the monitoring of system administrator and highly-privileged account activity in the Core and G&T IFMIS UNIX environments, in accordance with FEMA and DHS policy. • Implement technical controls to restrict access to the "root" account through the use of "sudo" to ensure that explicitly authorized individuals only have access to the account. • Ensure that system logs and records of administrator activity, including "sudo" activity related to the "root" account, are retained and reviewed by IT security management independent of the system administration team.	X		3
FEMA-IT-09-74	FEMA's systems inventory does not include all financial systems. Specifically, G&T FMIS and PARS were not included in the inventory provided to us during the audit by FEMA and neither system is being tracked via the Trusted Agent Federal Information Security Management Act.	Update the FEMA system inventory to include the G&T instance of IFMIS, as well as PARS. FEMA should comply with DHS policy and consistently follow procedures for updating and monitoring their FISMA system inventory to ensure that all new and current systems are accounted for with complete and accurate information, in accordance with NIST and DHS policy.	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-75	During the audit, we determined that review of access to the NFIP data center is performed on an ad-hoc basis. However, there are no policies or procedures that require periodic and documented re-certification of data center access at a defined frequency.	Document defined and repeatable procedures for the review of physical access to the NFIP data center in accordance with DHS and NIST guidance. These procedures should, at a minimum, define the frequency of this review and what documentation should be maintained as evidence of that review.	X		1
FEMA-IT-09-76	Based on testwork performed and inquiries conducted with FSS and Core IFMIS database personnel, we determined that emergency and temporary access to the database, including access for contractor development personnel, is approved by the FSS Chief and/or their staff, rather than by the FEMA Chief Information Security Officer (CISO)/Information System Security Manager (ISSM) or a designee, as required by DHS policy. Additionally, we determined that the Core IFMIS Oracle database access granted to contracted development personnel to implement database changes to Core IFMIS conflicts with segregation of duties principles.	Establish a formal process for granting emergency and temporary Core IFMIS database access that includes segregation of duties considerations and appropriate approval from FEMA management in accordance with DHS policy.	X		3
FEMA-IT-09-77	FEMA 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	We recommend 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. The processes should include, but are not limited to, formal	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	communication and decision-making of FEMA OCFO, OCIO, and NFIP management.	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 Acquisition Decision Events at each SELC phase, and integration of IT security considerations throughout all project phases.			
FEMA-IT-09-78	Based on our testwork, we concluded that NEMIS configuration management is not adequately 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 new development contract have not been documented and approved by FEMA management, in accordance with DHS and FEMA policy. • Once the new systems development contractor delivers developed changes to FEMA, FEMA does not monitor and track NEMIS SCRs throughout the configuration management lifecycle, from initial approval through implementation into the production	• Document and implement a comprehensive configuration management plan for NEMIS which clearly defines the roles and responsibilities for FEMA and contractor personnel managing the development of non-emergency and emergency system changes, in compliance with DHS and FEMA requirements. • Ensure that NEMIS non-emergency and emergency system changes are tracked, controlled, properly documented, and managed by FEMA personnel throughout the lifecycle of the configuration management process in accordance with DHS and FEMA guidance and policies.	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	environment. Instead, FEMA only tracks and collects documentation for SCRs from Project Managers at the final approval stage when the request is received by the TRC.				
FEMA-IT-09-79	Based on observations conducted over the FEMA LAN and the Microsoft Windows Active Directory (AD) environment, we concluded that the following weaknesses exist: • The FEMA LAN domain security policy does not enforce password requirements in accordance with DHS policy. • Policies and procedures over the authorization of FEMA LAN accounts, independent of NACS approval process outlined in the *Non-User Specific, Shared, Other Group Type Accounts SOP*, have not been finalized or implemented. Additionally, we determined that initial access authorizations for a selection of AD accounts were not authorized. • A periodic recertification of FEMA LAN access accounts is not currently performed to ensure that access is still necessary and appropriate for each individual. • We compared a listing of active FEMA LAN/AD accounts against a list of FEMA employee separations that had occurred since October 1, 2008. Based on our test work, we determined that 36 accounts remained active and unlocked after the account holder's separation from FEMA.	• Configure the FEMA LAN and AD account policies to require strong passwords, in accordance with DHS policy. • Finalize and fully implement the *Non-User Specific, Shared, Other Group Type Accounts SOP*. Specifically, FEMA should ensure that policies and procedures over the granting and managing of access for group/shared/service and administrator-level user accounts not authorized through NACS are documented and implemented consistently. Additionally, policies and procedures should ensure that, in accordance with DHS policy, a clear business need is established and documented justifying the creation and use of these types of accounts. • Develop and implement a formal process for performing a periodic recertification of user access to the FEMA LAN which defines requirements and addresses users not accounted for during the planned recertification of NEMIS application access.	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		• Evaluate and, if appropriate, revise existing procedures over removal of separated user access to ensure that all separated users on the FEMA LAN are removed in a timely manner. Ensure that procedures and processes are implemented consistently to remove network accounts for all separated users immediately upon notification of separation, in accordance with FEMA, DHS, and NIST guidance.			
FEMA-IT-09-80	NFIP has not developed and implemented formal procedures that outline the process for conducting internal scans for the NFIP LAN and for assessing, reporting, and correcting identified weaknesses. We also determined that remediation of vulnerabilities identified during internal scans of the NFIP LAN is not formally tracked and monitored through the Plan of Actions and Milestones (POA&M) Process in accordance with DHS policy. While the NFIP contractor conducts internal vulnerability scans of the NFIP LAN on a monthly basis, scanning of select workstations are presently excluded.	• Develop and implement formal procedures that outline the internal scan processes and requirements. These procedures should include, at a minimum, the process for assessing, reporting, and correcting weaknesses identified during scans. Additionally, ensure that the scope of vulnerability scans conducted include all workstations on the NFIP LAN. • With the involvement of both FEMA management and NFIP contractors, implement procedures for formally tracking and monitoring the remediation of vulnerabilities identified during the internal scans of the NFIP LAN through FEMA's POA&M process.	X		2
FEMA-IT-09-81	FEMA does not have approved and finalized procedures that establish formal requirements, processes, and responsibilities for performing regular vulnerability scans of Core and G&T	• Establish and formalize FEMA policies and procedures over the requirements, processes, and responsibilities for performing periodic vulnerability scans	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	IFMIS. FEMA also provided us with documented evidence of a G&T IFMIS internal vulnerability scan that was performed on July 17, 2009. However, we noted that the scan was scheduled and performed after our initial request for audit documentation. Additionally, FEMA was unable to provide us with any evidence that prior scans of G&T IFMIS had been performed or scheduled since the system was brought online in FY 2007.	for Core and G&T IFMIS instances, in accordance with DHS guidance. • Ensure that vulnerability assessment scans are performed for G&T IFMIS and that weaknesses identified are formally reported and tracked for remediation through the DHS POA&M process, as required by DHS guidance.			
FEMA-IT-09-82	Upon inspection of the FEMA SOP for installing UNIX patches to the Core and G&T IFMIS instances, we noted that it does not outline the process for defining a timeline for implementing non-emergency and emergency patches or for authorizing, testing, and approving patches for implementation, in accordance with DHS guidance. Furthermore, FEMA IT personnel informed us that documented test results of UNIX patches are not retained by IT personnel after testing is completed.	Document, finalize, and implement comprehensive patch management policies and procedures for Core and G&T IFMIS, in accordance with DHS policy. Policies and procedures should include requirements for responding to DHS SOC and DHS Computer Security Incident Response Center notifications to ensure the timely implementation of required patches and retention of testing documentation.	X		2
FEMA-IT-09-83	We were informed by FEMA IT System Integrations that NEMIS' program directories for the TDL environment, where all User Acceptance Testing (UAT) occurs, and the NEMIS production environment where the code changes are implemented, are located on one server. Upon review of the processes for restricting access to these directories, we noted the	• Develop and implement a formalized a process and procedures for restricting and monitoring access over the NEMIS production 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	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	following weakness: • Of the fifteen individuals with access to the server, three accounts belonged to development personnel who have write, read, execute, and modify access to all of the server's directories, which allow unrestricted access to both the production and development environments for NEMIS. • FEMA does not lock down the code in their server directory environment, giving all accounts unrestricted access to the NEMIS TDL and production environment after the code has been approved for implementation. 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 of not locking down the directories.	the monitoring of NEMIS system directories to ensure that no changes have occurred after the approval of NEMIS system changes has occurred. • Limit the developers' access to the NEMIS production directories to "read only" and segregate the responsibility for delivering application code changes into the NEMIS directory server from the contractor to an independent control group. If business need requires that the segregation of duties cannot be immediately implemented, FEMA should document policies and procedures to compensate for the risk associated with the segregation of duties weakness noted, in accordance with DHS guidance.			
FEMA-IT-09-84	Based on testwork performed, we identified the following weaknesses in PARS database security controls: • 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 are not required and/or enforced in accordance with DHS requirements. • Database audit logs are not configured to	• Perform documented periodic reviews of PARS database accounts and disable inactive accounts, in accordance with DHS policy. • Configure PARS database accounts to adhere to DHS policy for passwords and authenticator controls, including expiration, reuse, and complexity. • Configure the PARS databases to log events and conduct documented reviews	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	capture auditable events, including failed login attempts and administrator-level actions. • A periodic recertification of PARS database access accounts is not currently performed to ensure that access is still necessary and appropriate for each individual. FEMA could not provide evidence that initial PARS database granted to one of four users was appropriately authorized and the individual was inappropriately approved for emergency database access by the FSS Chief, rather than the FEMACISO/ISSO/ISSM or designee, as required by DHS policy.	of audit logs, in accordance with FEMA and DHS policy. • Further define and implement a formal process that documents requirements for configuring, retaining, and reviewing audit trails for the PARS database in accordance with FEMA and DHS policy. Additionally, ensure that all DHS requirements are met through this process, including appropriate supervisory review and retention. • 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.			
FEMA-IT-09-85	Based on observations conducted with the NFIP IT contractor, we determined that while TRRP system passwords were configured to enforce password complexity using alphabetic, numeric, and special characters, the configurations did not limit the use of dictionary words. Additionally, the password configuration did not prevent the password from being any word, noun, or name spelled backwards or appended with a single digit or with a two-digit "year" string, in accordance with DHS guidance.	No recommendation is required for this weakness that existed for the majority of FY 2009 because it was remedied prior to the end of the audit when the TRRP password settings were reconfigured to enforce complexity requirements that exceed DHS requirements.	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-09-86	We noted that the 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. Additionally, we determined that 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, establish a separate account for the third party vendor's use to implement Traverse changes and limit use of the account so that's its activated on an as needed basis. • Establish and implement a formal process for monitoring and verifying configuration changes made by the vendor in the Traverse environment, in accordance with DHS policy. Additionally, ensure that these procedures include requirements for documentation retention.	X		2
FEMA-IT-09-87	Procedures for management of FEMA IT security incidents have not been developed, approved, and implemented, in accordance with FEMA and DHS requirements. Additionally, our unannounced FY 2009 vulnerability assessment scanning activity was not detected and appropriately reported by FEMA IT personnel in accordance with DHS and	• Develop, approve, and implement an SOP for managing security incidents that clearly outlines roles and responsibilities required to maintain a continuous incident response capability, as required by DHS and FEMA policy. • Provide training to all personnel with incident response roles and	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	FEMA policy.	responsibilities.			
FEMA-IT-09-88	During our FY 2009 audit testwork, we noted that NFIP had not formally established a process for authorizing, documenting the approval and business need for service accounts, and recertifying service accounts on the TRRP system. As a result, authorization forms were not on file for all service accounts and recertifications of access are only conducted for user accounts.	• Revise the TRRP access control policies and procedures to ensure that the creation of service accounts are appropriately authorized and that a clear business need is established and documented justifying the creation and use of these types of account in accordance with DHS policy. • Ensure that policies and procedures over TRRP access authorization include a formalized process for the recertification of service accounts on an annual basis in accordance with DHS policy.	X		2
FEMA-IT-09-89	FEMA did not adequately conducted suitability investigations for FEMA federal employees in accordance with DHS requirements and position designations associated with employees with elevated system privileges did not have appropriate position sensitivity designations. We also determined that formal procedures were not developed or implemented for conducting suitability screenings of contractors accessing DHS IT systems. Additionally, suitability	• Further define and refine processes to ensure that background investigations for all types of federal employees are performed in accordance with DHS directives. • Reevaluate and assign the correct position sensitivity levels to federal employees with access to DHS information systems in accordance with DHS policy.	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	investigations were not appropriately conducted for contractors with access to multiple FEMA information systems holding sensitive IT security positions and the contractors did not have position sensitivity designations.	• 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 contracting personnel in accordance with DHS policy. • Ensure that all systems owners formally and correctly define the appropriate suitability designation for contracting personnel needing access to their information systems in accordance with DHS policy. Additionally, ensure that position sensitivity designations distinguish between various levels of access and require the contractor to have their suitability investigation completed prior to being granted access.			
FEMA-IT-09-90	We determined that FEMA has certified the FEMA Switch Network (FSN)-2 switch network which is comprised of various FEMA LANs across the regions and each LAN is classified as a subsystem of the switch network. During our review of the C&A package, we noted that the MD National Processing Service Center (NPSC) is considered to be a sub-system to the overarching GSS FSN-2 and that the primary servers for NEMIS, Core IFMIS, and G&T IFMIS financial applications reside on this portion of the LAN. However, the document states that no current accreditation or certification	• Formally designate an ISSO and DAA for the MD NPSC. • Immediately conduct an assessment of key controls that help ensure confidentiality and availability of data for security weaknesses and determine the operational risk related to MD NPSC LAN supporting FEMA financial applications. Weaknesses identified should be documented with plans for accelerated remediation efforts or related risks should be formally accepted by	X		3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	letters could be found for that subsystem during the certification and accreditation of the FSN-2 package. Specifically, there is no evidence in the package that the required C&A elements have been completed/updated, documented, or approved for MD NPSC in accordance with DHS guidance. We further noted that the C&A package states that C&A activities are to be completed for the MD NPSC subsystem at a separate time and that no security roles were defined for the MD NPSC within the C&A. We inquired with FEMA Information Technology (IT) Security and management to determine the status for the MD NPSC C&A package and were not provided with any additional information as to the status of the C&A package. Additionally, upon further review of the C&A package, we noted that both the MD NPSC and the regional LANs are within scope of this review as NEMIS has servers at multiple regional sites. Furthermore, we determined that management had not adequately completed the C&A package over FSN-2 according to DHS policy.	FEMA. • Review and revise the FSN-2 C&A package to reflect the current GSS environment in accordance with DHS and Federal Guidance. Additionally, ensure that the C&A Package has been completed to include the required artifacts, addresses the security controls for the various subsystems and assigns and updates the appropriate security roles for each subsystem.			
FEMA-IT-09-91	FEMA does not have a formal process for adequately tracking FEMA contractors throughout the on-boarding, termination, and transfer processes. Furthermore, we noted that the process established for notifying the FEMA OCIO of changes in contractor's status, so that	Document and implement procedures, according to DHS guidelines and requirements, that track the on-boarding, transfer and separation of contractors. Ensure that the policies and procedures include:	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	accounts can be disabled/removed or account profiles can be appropriately modified in the required timeframe, is not effective or comprehensive. Specifically, there are no formal requirements for COTRs to notify the OCIO of separating contractors.	• The assignment of roles and responsibilities to appropriate FEMA management and stakeholders. • Steps for notifying the FEMA OCIO that a contractor is separating or transferring so that the contractor will have their systems access removed or modified in a timely manner, in accordance with DHS policies. • Regularly distribute a listing of terminated contract personnel to information system administrators so they can remove user access timely.			

Department of Homeland Security
FY2009 Information Technology - Notice of Findings and Recommendations – Detail

- **Federal Law Enforcement Training Center**

Department of Homeland Security
FY2009 Information Technology
Notification of Findings and Recommendations – Detail

Federal Law Enforcement and Training Center

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
FLETC-IT-09-03	We determined that SOP 4250, which has been in effect for the entire fiscal year, was last updated on May 12, 2009 and that FLETC has developed a manual control for the installation of system software for Momentum. Specifically, logs of file changes to the Momentum UNIX servers are reviewed monthly. Therefore, this condition of the prior weakness has been partially corrected. We also determined that FLETC is still in the process of implementing the Security Information Management System (SIM) to compile audited events of Oracle and other system software for review by FLETC personnel. FLETC management has confirmed that logs of Oracle are not being reviewed to identify potential anomalies or incidents. Due to the lack of audit logging procedures around system software for Momentum, this NFR will be reissued.	We recommend that FLETC enable audit logging over all Momentum system software and ensure that logs are maintained and proactively reviewed by management.		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
FLETC-IT-09-04	We determined that FLETC has implemented DHS's System Engineering Lifecycle (formally called SDLC) into their business processes, and that it is promulgated to personnel involved in the change management process. However, we determined that implementation did not occur until April 2009. As a result, we will be reissuing this NFR with no recommendation since the condition has existed for a majority of the fiscal year.	As FLETC has effectively put into place procedures over the implementation of DHS' SELC effective April 2009, no recommendation will be offered.		X	2
FLETC-IT-09-26	During the internal vulnerability assessment efforts of FLETC's Glynco Administrative Network (GAN), Financial Accounting and Budgeting System (FABS), and Student Information System (SIS) systems we identified several High/ Medium Risk vulnerabilities, related to Configuration Management and Password Management. We confirmed that security configuration management weaknesses (i.e., default configuration settings, role and group policies, password policy, and user account management) continue to exist on hosts supporting FLETC. The conditions are exploitable as an insider without specific knowledge of the operation of the system or the applications hosted on that system. These conditions can be found in the table within the actual NFR.	Implement the corrective actions for the recommendations listed within the NFR.		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
FLETC-IT-09-31	We determined that in January 2009, FLETC implemented a Standard Operating Procedure (SOP) #60 titled, Monthly Review of Security and Approval logs, which requires management review and sign off. However, FLETC was unable to provide documentation supporting the management review of approval logs for April, May, June, and July. In addition, FLETC was unable to provide evidence of management review of the security violation logs for June and July.	We recommend that FLETC, enforce their own policies and procedures for the maintenance and periodic review of audit logs for Momentum.		X	2
FLETC-IT-09-33	We determined that logs of auditable events in the LAN are not being reviewed to identify potential anomalies or incidents. FLETC is in the process of implementing SIM with the capabilities to manage logged auditable events for review by personnel. We determined that, while the SIM is being implemented, FLETC does not have an alternative procedure for the review of these logs.	We recommend that FLETC establishes and implements procedures to document and review logs of auditable events in the LAN.	X		2
FLETC-IT-09-34	We determined that access control weaknesses existed over the Momentum access authorizations for user profiles created or modified during the fiscal year. Specifically, we learned that profile creation and modification is not tracked and a listing of events could not be provided.	We recommend that FLETC activate the logs for tracking the addition of new users and profile changes to Momentum.	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
FLETC-IT-09-35	We noted several weaknesses with logical access controls related to GAN: • The GAN is configured to prohibit password resuse for 6 generations, which does not meet the DHS standard of eight password generations. • The GAN is configured to reset the account failed logon counter after 60 minutes, which does not meet the DHS standard of 24 hours. • Several user IDs were identified having excessive access. • Supporting documentation for new user authorizations to the GAN could only be provided for ten users out of 25 sampled. • Fourteen separated employees still had an active user account to the GAN. • Formalized procedures are not in place for periodic reviews over GAN users.	We recommend that FLETC Management: • Establish a process to ensure the GAN is configured to meet minimum DHS password configuration requirements. • Remove all generic/shared accounts and conduct period reviews of the user access lists to ensure compliance. • Establish and enforce procedures for the completion and maintenance of user access forms for the GAN. • Enforce procedures for the removal of transferred/terminated users within the GAN upon their separation from FLETC. • Establish and implement policies and procedures for recertification of GAN user privileges.	X		2
FLETC-IT-09-36	During our after hours physical testing, we identified 84 passwords, four For Official Use Only Violations , seven unsecured ID badges/keys, 83 Personally Identifiable Information violations, six unsecured laptops, two unsecured external drives, 12 unsecured credit cards, and four users logged into a system	We recommend that FLETC management implement processes to: • Ensure that users are trained and aware of safeguarding login credentials, locking network sessions to DHS systems, and locking any sensitive information, media containing sensitive information, or data	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	without an active screen saver set.	not suitable for public dissemination in secure locations when not in use. • Effectively limit access to DHS buildings, rooms, work areas, spaces, and structures housing IT systems, equipment, and data to authorized personnel.			
FLETC-IT-09-37	During the FY 2009 financial statement audit, we noted several weaknesses with the logical access controls for the SIS. Specifically, we determined the following: • SIS is configured to have a password history of two passwords stored that does not meet the DHS 4300A requirement of eight remembered passwords. • SIS is configured to have a minimum password age of five days that does not meet DHS 4300A requirements of seven days. • SIS is not configured to reset the account failed logon counter, which does not meet the DHS 4300A requirement of a reset every 24 hours. • Users were not locked out until after 6 invalid attempts to access the application. • SIS system administrators share the 'root' username and password to perform administrative responsibilities. • A sample of audit logs that track changes to system data could not be provided. • Invalid user access attempts were not tracked	We recommend that FLETC management: • Establish a process to ensure the SIS is configured to meet minimum DHS password configuration requirements. • Adjust system configuration settings to lock out users after three invalid logon attempts as designated by DHS policies. • Remove all generic/shared accounts and conduct periodic reviews of the user access lists to ensure compliance. • Retain audit trail records in accordance with DHS policies in order to support potential incidents within the system, and for review of user privileges. • Activate tracking for the addition of new users to SIS.	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	and monitored until March 2009. Since this weakness was corrected during the fiscal year, no recommendation will be offered. • 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.				
FLETC-IT-09-38	We determined that weak access controls exist over Momentum's system software. Specifically, we noted that the password configuration settings for Linux, which supports Momentum, is set to allow a user to attempt to logon six times before the account is locked out.	We recommend that management establish a process to ensure FLETC systems are configured to meet minimum DHS logical access configuration requirements.	X		2

Department of Homeland Security
FY2009 Information Technology - Notice of Findings and Recommendations – Detail

- **Immigration and Customs Enforcement**

Department of Homeland Security
FY2009 Information Technology
Notification of Findings and Recommendations – Detail

Immigration and Customs Enforcement

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
ICE-IT-09-11	We accessed ICE facilities located at the Tech World Building on 800 K Street and the PCN Tower on 500 and 12th Street without the use of DHS issued credentials. Moreover, we overtly presented non-government issued identification to building security and was then granted physical access to the facilities.	We recommend that ICE train physical security personnel to recognize DHS issued identification or credentials and detect non-conforming credentials.	X		2
ICE-IT-09-12	Ineffective/non-compliant account lockout counter settings During the FY09 audit, KPMG inquired of ICE OCIO personnel about ADEX account settings, reviewed the account lockout settings, and inspected ICE's logical access polices and found that the account lockout settings for ADEX was not compliant with DHS policy. DHS policy requires that the system is to lock user accounts after three consecutive invalid login attempts within a 24 hour period. However, within ADEX, the number of invalid attempts to access the system resets to zero after 30 minutes if up to two invalid access attempts are made. Therefore, several attempts can initiated as long as the user waits 30 minutes before attempting again.	The Enterprise Operations Division of the OCIO adjusted the lockout settings after they were informed by us of the discrepancy. No recommendation given.	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
ICE-IT-09-13	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.	We recommend that ICE update the FFMS password configuration settings to be in compliance with DHS 4300A policies.	X		2
ICE-IT-09-14	We identified that the ADEX user recertification process is not designed appropriately. Specifically, we noted a lack of formal policy and procedure for managing the periodic review of ADEX general user access. In addition, the informal process contingent upon personnel's annual completion of the Information Assurance Awareness Training (IAAT) as a mitigating control for ensuring a review of users' access on a periodic basis is insufficient.	We recommend that ICE management establish and implement policies and procedures for recertification of ADEX user privileges. This process should include a method to document user recertification and a process to maintain evidence of the reviews.	X		2
ICE-IT-09-15	We 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, we identified 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.	We recommend that ICE management establish and implement policies and procedures for recertification of FFMS user privileges. This process should include a method to document user recertification and a process to maintain evidence of the reviews.	X		2
ICE-IT-09-16	We determined that weaknesses exist over ADEX access. Specifically, we found that 14 users, which were separated from ICE, still had active ADEX accounts that were not removed upon their termination/transfer.	We recommend ICE management develop processes for the removal of transferred/terminated users within ADEX upon their separation.	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
ICE-IT-09-17	We 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 that were in violation of FFMS segregation of duties policies.	We recommend that ICE enforce policies and procedures to ensure that assigned roles and responsibilities are commensurate with personnel job functions.	X		2
ICE-IT-09-18	We identified that background reinvestigations are not conducted in a timely manner. We performed an inspection of a sample of ICE personnel requiring reinvestigations during the fiscal year and of the 25 ICE employees sampled, evidence of background reinvestigations during FY 2009 could not be provided for 16 contractors.	We recommend ICE management periodically review personnel files to confirm background reinvestigations have been completed in accordance with DHS standards.	X		2
ICE-IT-09-19	We performed an inspection of a sample of personnel that had terminated/transferred from their employment with ICE during the fiscal year. We 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.	We recommend ICE management adhere to exit clearance procedures and require personnel to follow them in the event of transfer/termination.	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
ICE-IT-09-20	We determined that ICE lacks policies and procedures requiring completion of a training program by personnel in IT security positions.	We recommend that ICE management implement mandatory requirements for IT security personnel to complete training consistent with their job function duties.	X		2
ICE-IT-09-21	During the internal vulnerability assessment efforts of ICE's network servers and systems we identified several High/ Medium Risk vulnerabilities, related to configuration management. We determined that security configuration management weaknesses (i.e., missing security patches and incorrect configuration settings) exist on hosts supporting the ICE.	In addition to addressing the specific vulnerabilities identified in the condition, ICE should: • Redistribute procedures and train employees on continuously monitoring and mitigating vulnerabilities. In addition, we recommend that ICE periodically monitor the existence of unnecessary services and protocols running on their servers and network devices, in addition to deploying patches. • Perform vulnerability assessments and penetration tests on all offices of the ICE, from a centrally managed location with a standardized reporting mechanism that allows for trending, on a regularly scheduled basis in accordance with NIST guidance. • Develop a more thorough approach to track and mitigate configuration management vulnerabilities identified during monthly scans. ICE should monitor the vulnerability reports for necessary or required configuration changes to their environment. • Develop a process to verify that systems identified with "HIGH/MEDUIM Risk" configuration vulnerabilities do not	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
		appear on subsequent monthly vulnerability scan reports, unless they are verified and documented as a false-positive. All risks identified during the monthly scans should be mitigated immediately, and not be allowed to remain dormant.			
ICE-IT-09-22	During our after hours physical testing, we identified 26 passwords, four For Official Use Only Violations , two unsecured ID badges/keys, 15 Personally Identifiable Information violations, two server names/IP addresses, three unsecured laptops, six unsecured external drives, one unsecured credit card, and two users logged into a system without an active screen saver set.	KPMG recommends that ICE management implement processes to: • Ensure that users are trained and aware of safeguarding login credentials, locking network sessions to DHS systems, and locking any sensitive information, media containing sensitive information, or data not suitable for public dissemination in secure locations when not in use. • Effectively limit access to DHS buildings, rooms, work areas, spaces, and structures housing IT systems, equipment, and data to authorized personnel.	X		2
ICE-IT-09-23	We identified that the IT security awareness training requirements are not enforced. Of the population of staff that had not taken the training by the ICE deadline of 6/1/09, we determined that three employees still maintained system access. Additionally, procedures are not in place to disable user accounts and access privileges if annual training is not completed.	We recommend ICE management to: • Remove system access for personnel that are not in compliance with training requirements. • Document procedures regarding the disabling of user accounts and access privileges in accordance with DHS policies for employees not in compliance.	X		2

Department of Homeland Security
FY2009 Information Technology - Notice of Findings and Recommendations – Detail

- **Office of Chief Information Security Officer**

Department of Homeland Security
FY2009 Information Technology
Notification of Findings and Recommendations – Detail

Office of Chief Information Security Officer

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
OCIO-IT-09-03	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		1

Department of Homeland Security
FY2009 Information Technology - Notice of Findings and Recommendations – Detail

- **Office of Financial Management**

Department of Homeland Security
FY2009 Information Technology
Notification of Findings and Recommendations – Detail

Office of Financial Management

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CONS-IT-09-13	We identified that while weekly DHSTIER Oracle activity audit reports (including the OBJECT, USER, and PRIVILEGE listings) are generated and retained, evidence of RMTO security management reviews of reports is not retained.	We recommend that the RMTO Audit Log Review Policy/Procedures be revised to require that DHSTIER Oracle activity audit reports are retained with evidence that they have been reviewed by management in accordance with DHS 4300A requirements.	X		1
CONS-IT-09-14	We noted that the following password configurations for the DHSNET domain, which controls access to the CFO Vision application, are not in compliance with DHS 4300A requirements: • Password History is configured to remember the previous six (6) passwords rather than eight (8) as required by policy; and • Automatic Session Termination is configured to lock workstations after fifteen (15) minutes of inactivity rather than five (5) as required by policy. Upon informing OFM management of this issue, DHS took corrective action and partially remedied the condition by modifying the DHSNET domain policy to remember the	We recommended that DHSNET domain password settings be configured to be aligned with DHS 4300A requirements concerning automatic session termination.	X		1

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	previous twenty-four (24) passwords. However, the account lockout duration remains at 15 minutes.				
CONS-IT-09-15	DHS IT personnel informed us that prior to August 2009 a formal process was not documented or implemented for authorizing, testing, and deploying Windows operating system patches and emergency operating system patches on the servers which support the DHSTIER and CFO Vision applications. However, we were informed that since August 2009, DHS has implemented the Infrastructure Change Control Board (ICCB) Change Management Handbook as the formal requirement followed to document an initial change request form, maintain test results, and obtain Infrastructure Change Control Board (ICCB) approval prior to deploying operating system patches. Therefore, we concluded that a formal change management process for operating system patches was not present for the majority of the fiscal year.	We recommend that DHS continue to obtain and document approvals and test results in accordance with DHS policies and requirements for non-emergency and emergency operating system patches for DHSTIER and CFO Vision.	X		1
CONS-IT-09-16	We noted that policies and procedures requiring a periodic review of physical access privileges to the NCCIPS Stennis Data Center (SDC), which houses the physical infrastructure for DHSTIER and CFO Vision, have not been documented nor implemented since DHS operations at NCCIPS began on October 1, 2008.	We recommend that DHS develop and implement policies and procedures for performing a periodic review of physical access privileges to the DHS Stennis Data Center facility, to include retention of evidence that reviews were performed and approved by appropriate management.	X		1

Department of Homeland Security
FY2009 Information Technology - Notice of Findings and Recommendations – Detail

- **Transportation Security Administration**

Department of Homeland Security
FY2009 Information Technology
Notification of Findings and Recommendations – Detail

Transportation Security Administration

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-09-20	We were unable to obtain six of the eight Employee Exit Clearance Forms and one of the three Separating Non-Screener Employee and Contractor IT Certificates sampled.	• Complete workgroup efforts to establish clear ownership and corrective action plans for the conditions noted. • Complete and maintain all forms during the exit process, as required by the Employee Exit Clearance procedures for employees and contractors. • Verify that a computer access agreement is acknowledged by all TSA employees and contractors, as required by the IT Security Policy Handbook, and that evidence of this acknowledgement is maintained.		X	1
TSA-IT-09-23	Deficiencies continued to exist over the script configuration management process. Specifically, Deficiencies were noted in the areas of approvals, testing, monitoring, maintaining documentation, and audit logging. • Coast Guard lacks a formal process to distinguish between the module lead approvers for script approval requests. • Coast Guard Finance Center (FINCEN) analysts may run scripts without seeking further approval from the	Continue making improvements to implement and better document an integrated script configuration management process that includes enforced responsibilities of all participants in the process, and the continued development of documentation requirements. We recommend that the Coast Guard should: • Continue to design, document, implement, and enforce the effectiveness of internal controls associated with the active (current and future) scripts.		X	3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Functional Supervisors for approved recurring scripts. • Testing requirements are inconsistently followed for the testing of the Recurring Approval scripts and retaining evidence of testing. • No reconciliation between the scripts run and the changes made to the database tables is being performed to monitor the script activities using this report as it is too difficult to accurately and effectively reconcile the scripts to the audit log table changes. • The Script Tracking System does not consistently include all testing, approval, and implementation documentation for all scripts. • Variations in the way the Production Review Process (PRP) Approval Forms are populated and completed exist for fields such as financial impact, test strategy and baseline determinations. • Proper approval is not consistently obtained and documented prior to the running of each script. In addition, we noted the following deficiencies related to TSA monitoring controls over the Coast Guard IT script process:	With respect to procedures already in place, Coast Guard should: • Update / Develop procedures and implement technical controls in the Core Accounting System (CAS) and Financial Procurement Desktop (FPD) databases to ensure that the appropriate monitoring and review of script activities is performed and documented. • Continue to update script policies and procedures to include clear requirements and more detailed guidance over requesting recurring scripts, testing and documentation requirements, monitoring/audit log reviews, and blanket approval requirements. Additionally, ensure that the policies and procedures include detailed guidance over the requirements for the testing of scripts and associated test plans to ensure that the appropriate financial impact of the script is evaluated, reviewed by the appropriate personnel, tested in an appropriate test environment prior to being put into production, and documented prior to execution. • Further develop and implement policies and procedures governing the script change control process to ensure that all script records			

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• TSA management receives a weekly script report as well as a Validation of Monthly Recurring Scripts from FINCEN. However, we were informed that TSA was still requesting modifications to the script reports and had asked FINCEN to go back into Change Management Script System (CMSS) to populate missing information so that further analysis could be conducted. Additionally, during test work, we noted that for eight PRP forms, the financial impact determination did not match the CMSS script record field. • TSA management is still in the process of identifying the appropriate subject matter experts in each area and have not formalized the roles and responsibilities surrounding this process. • TSA policies and procedures developed by require that the TSA subject matter experts utilize the financial impact guidance set forth by FINCEN management in the PRP Staff Instruction. However, upon inspection of the PRP Instruction we determined that this guidance does not adequately include detailed criteria to determine financial impact. • Once the financial impact is assessed	within the Change Management Script System are accurate and complete.			

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	and approved by FINCEN for the parent blanket approved recurring script, the testing of the script is not subsequently reviewed by an individual with financial reporting knowledge for child scripts that are run in production to ensure that financial impact is correct before the script is placed in production. • TSA is not asked to review and approve all scripts with a financial impact – thus a Coast Guard approver may approve a script that TSA is not in agreement with, or even aware of.				
TSA-IT-09-28	During our after-hours physical security testing, we identified four passwords located on employee workstations.	Review security awareness programs designed to protect financial data to help ensure that individuals are adequately instructed and reminded of their roles in the protection of both electronic and physical TSA financial data and hardware that supports financial data.	X		1
TSA-IT-09-29	Controls over the TSA quarterly access reviews for CAS and FPD user accounts have not been effectively implemented to ensure that TSA users who no longer require system access are removed in a timely manner.	Develop and effectively implement quarterly review policies and procedures that include follow-up measures that will be enforced to ensure that users identified through these reviews are maintaining unnecessary access have their accounts end dated in a timely manner.	X		1

Department of Homeland Security
FY2009 Information Technology
Notification of Findings and Recommendations – Detail

- **United States Citizen and Immigration Services**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CIS-IT-09-01	We inspected the National Benefits Center (NBC) CLAIMS 3 LAN user role/responsibilities documentation and determined that the system settings and assigned user roles within the system do not accurately reflect documented user responsibilities.	Continue to define and document the various CLAIMS 3 LAN roles and their associated responsibilities for the remaining service centers.		X	2
CIS-IT-09-02	NBC does not perform periodic CLAIMS 3 LAN user access reviews to ensure that users' level of access remains appropriate and there are no procedures established for performing periodic reviews.	Establish and implement policies and procedures for handling, reviewing, and retention of Claims 3 LAN user account request forms.		X	2
CIS-IT-09-03	Management at the USCIS Headquarters (HQ) and the Service Center, Vermont has not completed or inadequately documented access forms for CLAIMS 3 LAN and CLAIMS 4, system users.	Establish and enforce procedures for the completion and maintenance of user access forms for CLAIMS 3LAN and CLAIMS 4 for all the service centers.		X	2
CIS-IT-09-04	The USCIS HQ has not maintained or documented a selection of system administrator's access authorization forms.	Conduct and document annual reviews of all users with Active Directory system administrator access.		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CIS-IT-09-06	The biometric facial recognition scanner allowed unauthorized personnel access to USCIS server room, and procedures regarding removal, authorization, and logging of USCIS backup media are not in place for the Technology Engineering Consolidation Center (TECC).	• Establish and implement backup media retention and rotation policies. • Establish and implement emergency exit and re-entry procedures. • Develop a process that assures all resources with access to the USCIS resources adhere to the policy and procedure. • Implement stronger physical access controls over the server cage door to prevent further unauthorized access		X	2
CIS-IT-09-07	USCIS has not finalized a policy that outlines the process for developing forms for labeling and tracking the disposition process or provided clear instructions for conducting media wipes or purges of data.	Update and finalized their policies and procedures to reflect their current media sanitization operation.		X	2
CIS-IT-09-08	USCIS does not recertify its system administrator accounts on an annual basis.	Management should establish a more timely process to perform a periodic review of user accounts ensuring proper authorization and training.		X	2
CIS-IT-09-09	CLAIMS 3 LAN password re-use and length configurations does not meet DHS standards. CLAIMS 3 LAN generic user accounts was not timely removed because of a lack of user account recertification.	• Establish a process to ensure that USCIS systems are configured to meet minimum DHS password configurations and requirements. • Remove all generic accounts to CLAIMS 3 LAN production systems and perform periodic reviews of the user access list to ensure compliance.	X		2
CIS-IT-09-10	CLAIMS 4 LAN password configuration settings does not meet DHS4300A password standards.	We recommend that USCIS establish a process to ensure CLAIMS 4 LAN is configured to meet DHS4300A password configuration standards.	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CIS-IT-09-11	We identified that an inadequate background investigation was performed and documented for one new hire personnel from a sample of 25.	We recommend that USCIS management periodically review personnel files to confirm background investigations have been completed in accordance with DHS standards.	X		2
CIS-IT-09-12	We inspected a sample of personnel that had terminated/transferred from their employment with USCIS. Of the 28 terminated/transferred USCIS personnel sampled, evidence of compliance with exit clearance procedures could not be provided for 19 employees.	We recommend that USCIS management adhere to exit clearance procedures and require personnel to follow them in an event of transfer/termination.	X		2
CIS-IT-09-13	Vermont Service Center (VSC) has ineffective safeguards exist over the computer room in the Office of Information Technology (OIT). VSC procedures regarding the removal, authorization and logging of backup media are not in place. VSC procedures for ensuring accuracy and completeness over visitor logs are not enforced.	• Establish and implement procedures for maintaining and authorizing the OIT's computer room access list. • Establish and implement backup media retention and rotation policies. • Enforce completeness and accuracy over visitor information in logs.	X		2
CIS-IT-09-14	During our testing of access controls for FFMS, in our sample of 25 active users, we noted one user's access was excessive, based on the access approved by their present supervisor. We learned that this user's profile was changed as the user relocated to a different service center. However, when the profile change was requested, the FFMS administrator did not remove all previous access nor assure that the access rights were current and authorized. As a result, the user had excessive privileges for her role and responsibilities. We also noted that the USCIS SOP did not reflect this procedure though we learned through inquiry that the FFMS administrators are required to remove all prior	We recommend that USCIS establish and enforce policies and procedures that ensure that roles and responsibilities are commensurate with their job function.	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	access when performing a profile change. As a result of our test work, USCIS responded by removing the excessive access to reflect the user's role and responsibilities. In addition, USCIS updated their SOP to require all previous access to be confirmed and removed prior to granting new access roles.				
CIS-IT-09-15	We identified a lack of audit logging policies over the application and server logs for the CLAIMS 3 and CLAIMS 4 LAN system.	We recommend that USCIS establish and enforce policies and procedures for maintenance and review of audit logging.	X		2
CIS-IT-09-16	We identified weaknesses within physical access controls for CLAIMS 4 LAN over lack of procedures for recertifying user access, lack of evidence of least privilege and segregation of duties controls, and untimely removal of terminated personnel accounts.	• Establish and implement policies and procedures for the handling, periodically reviewing, and retaining CLAIMS 4 LAN user account request forms. • Define and document policies and procedures for identifying and approving CLAIMS 4 user roles/profiles to include the user's responsibilities. In addition, the policies and procedures should address and implement segregation of duties procedures. • Develop policies and procedures for the removal of transferred/terminated users within CLAIMS 4 upon their separation from USCIS.	X		2
CIS-IT-09-17	We identified weaknesses within monthly trainings of USCIS' ISSOs.	We recommend that USCIS management implement mandatory training requirements for IT security personnel to complete training consistent with their job function duties.	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CIS-IT-09-18	We determined that weaknesses exist related to CLAIMS3 LAN access. Specifically, we identified 21 users which were separated from USCIS and still retained access to the CLAIM3 LAN.	We recommend that USCIS management develop and implement policies and procedures for the removal of separated users within CLAIMS 3 LAN upon their separation.	X		2
CIS-IT-09-19	We tested a sample of personnel that were required to complete annual Computer Security Awareness Training during the fiscal year. Of the thirty (30) personnel sampled, evidence of compliance could not be provided for two employees. Additionally, procedures are not in place to disable user accounts and access privileges if annual training is not completed on a timely basis.	• Establish and implement requirements for personnel to complete Computer Security Awareness Training annually. • Develop a process to disable user accounts and access privileges in accordance with DHS policies for employees not in compliance.	X		2

Appendix C

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

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

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
CBP-IT-08-02	Interconnection Security Agreements (ISAs)	X	
CBP-IT-08-03			09-03
CBP-IT-08-08	Audit Logs	X	
CBP-IT-08-09	Disabling of Inactive Accounts on	X	
CBP-IT-08-12	Installations		09-12
CBP-IT-08-13	Complete List of CBP Workstations		09-13
CBP-IT-08-16	Excessive Emergency Access	X	
CBP-IT-08-18	Recertification of Accounts	X	
CBP-IT-08-21	Review of Changes to Security Profiles in		09-21
CBP-IT-08-26	Review of Security Violation Logs	X	
CBP-IT-08-27	Administrator Access Authorization Weaknesses		09-27
CBP-IT-08-28	Access Policies and Procedures	X	
CBP-IT-08-29	Completion of CF-241 Forms for Terminated Employees		09-29
CBP-IT-08-34	Installation of Virus Protection		09-34
CBP-IT-08-35	Configuration Management	X	
CBP-IT-08-36	Patch Management	X	
CBP-IT-08-37	Security Violation Review Process	X	
CBP-IT-08-38	Process for Reviewing Audit and Logs	X	
CBP-IT-08-39	Password Configuration Weakness in	X	
CBP-IT-08-40	ISSM Approval of Emergency and Temporary Access Authorizations	X	
CBP-IT-08-41	Weaknesses in the Process of Separating CBP Contractors		09-41
CBP-IT-08-42	Formal Agreement Not in Place for CBP's Use of as Business Continuity Facility	X	
CBP-IT-08-43	Inadequate Resources at for Business Continuity Testing	X	
CBP-IT-08-44	Completion of Non Disclosure Agreements for CBP Contractors		09-44
CBP-IT-08-45	Log Configuration Weakness for System		09-45
CBP-IT-08-46	Review of Logs	X	
CBP-IT-08-47	Rules of Behavior are Not Signed Before Gaining Systems Access	X	
CBP-IT-08-48	Lack of Effective Access Change Log Review Procedures		09-48
CBP-IT-08-49	Weak Initial Passwords Granted for New Accounts in	X	
CBP-IT-08-50	Inadequate Tracking of Security Awareness Training Completion	X	
CBP-IT-08-51	No Hardware Maintenance Procedures	X	
CBP-IT-08-52	Screensavers are Not Appropriately Configured on the	X	
CBP-IT-08-53	Out of Date and Inaccurate Security Administrator Procedures	X	
CBP-IT-08-54	Access Control Weaknesses	X	
CBP-IT-08-55	Accounts Created by Unauthorized Parties	X	
CG-IT-08-01	FINCEN Service Continuity Weakness	X	
CG-IT-08-06	Security Configuration Management Policy and Procedures Weakness	X	
CG-IT-08-07	RACF/JUMPS Password Configuration Needs Strengthening	X	

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
CG-IT-08-10	Contractor Background Investigation Weakness		09-10
CG-IT-08-14	Weaknesses in Specialized Role-based Training for Individuals with Significant Security Responsibilities		09-14
CG-IT-08-17	Checkfree Password Configuration Needs Strengthening	X	
CG-IT-08-23	SAM Audit Log Review Weakness		09-23
CG-IT-08-25	WINS Access Controls Need Strengthening		09-25
CG-IT-08-27	SAM Account Management Weakness	X	
CG-IT-08-31	Weaknesses in Controls Over the Scripting Process		09-31
CG-IT-08-32	Lack of a Documented Contractor Tracking Mechanism		09-32
CG-IT-08-33	Lack of a Consistent Contractor, Civilian, and Military Account Termination Process for Coast Guard Systems		09-33
CG-IT-08-34	WINS Change Control Weakness		09-34
CG-IT-08-35	CAS and FPD Change Control Weakness	X	
CG-IT-08-36	Vulnerability Assessment Weakness – Configuration Management	X	
CG-IT-08-37	Vulnerability Assessment Weakness – Patch Management	X	
CG-IT-08-40	Civilian Background Investigation Weakness		09-40
CG-IT-08-41	Weakness in the CAS C&A Package	X	
CG-IT-08-42	Non-Compliance with FFMIA – Information Technology		09-42
CG-IT-08-43	Access Authorization and Recertification Weaknesses within the User Management System (UMS)		09-43
CIS-IT-08-01	Lack of Definition and Documentation of Access Roles at the National Benefits Center for CLAIMS 3 LAN		09-01
CIS-IT-08-02	Periodic CLAIMS 3 LAN User Access Reviews are not Performed at the NBC		09-02
CIS-IT-08-03	Incomplete or Inadequate Access Request Forms for CLAIMS 3 LAN, CLAIMS 4, and CISCOR System Users at Headquarters and the Service Centers		09-03
CIS-IT-08-04	Ineffective Controls for Restricting Security Software Exist		09-04
CIS-IT-08-06	Weak Data Center Access Controls		09-06
CIS-IT-08-07	Equipment and Media Policies and Procedures are not Current		09-07
CIS-IT-08-08	Weak Access Controls for Security Software Exist		09-08
CONS-IT-08-07	Lack of Individual Accountability for DBA Accounts	X	
CONS-IT-08-11	Lack of Sufficient Evidence of TIER Change Control Testing	X	
CONS-IT-08-12	Evidence of Approvals and Testing for the CFO Vision 4.3 Upgrade Not Documented	X	
FEMA-IT-08-02	Configuration Management Weaknesses on IFMIS, NEMIS, and Key Support Servers		09-02
FEMA-IT-08-03	Weaknesses Exist over Recertification of Access to the IFMIS		09-03
FEMA-IT-08-06	Documentation Supporting the IFMIS User Functions Does Not Exist		09-06
FEMA-IT-08-12	NEMIS Access Controls Need Improvement		09-12
FEMA-IT-08-13	Employee Termination Process for Removing System Access		09-13

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
	Should be More Proactive		
FEMA-IT-08-17	System Programmers Have the Ability to Migrate Code into the IFMIS Production Environment		09-17
FEMA-IT-08-19	Monitoring of FEMIS System Software Needs Improvement		09-19
FEMA-IT-08-22	Alternate Processing Site for NEMIS Has Not Been Established		09-22
FEMA-IT-08-23	IFMIS Backup Tapes are not Tested in Accordance with DHS Requirements	X	
FEMA IT-08-24	NEMIS Backups are not Tested in Accordance with Policy		09-24
FEMA-IT-08-25	NEMIS Contingency Plan is not Tested		09-25
FEMA-IT-08-28	NEMIS Configuration Management Process for Non-Emergency Changes Needs Improvement		09-28
FEMA-IT-08-29	NEMIS Emergency Change Process Needs Improvement		09-29
FEMA-IT-08-38	Segregation of Duties Not Enforced for Traverse		09-38
FEMA-IT-08-39	Traverse Contingency Plan Not Tested and NFIP Disaster Recovery and CCOP Needs Improvement		09-39
FEMA-IT-08-45	IFMIS User Access is not Managed in Accordance with Account Management Procedures		09-45
FEMA-IT-08-46	IFMIS System Interconnections Agreements have not been Reauthorized		09-46
FEMA-IT-08-47	NEMIS System Interconnections Agreements have not been Reauthorized	X	
FEMA-IT-08-48	Corrective Action over NEMIS Vulnerabilities is Not Formally Documented		09-48
FEMA-IT-08-49	Anti-Virus Settings on User's Workstation were not Configured Properly	X	
FEMA-IT-08-50	Weaknesses Exist over IFMIS Application and Database Audit Logging		09-50
FEMA-IT-08-51	NEMIS Oracle Audit Logging is not Sufficient		09-51
FEMA-IT-08-52	Existing NEMIS Patch Management Guidance Needs to be Implemented		09-52
FEMA-IT-08-53	The NEMIS System Security Plan has not been Fully Updated in Accordance with DHS Policy		09-53
FEMA-IT-08-54	Traverse Application Management Needs Improvement		09-54
FEMA-IT-08-55	TRRP Change Management Needs Improvement	X	
FLETC-IT-08-01	Momentum Configuration Management Needs Improvement	X	
FLETC-IT-08-02	Procurement Desktop Configuration Management Needs Improvement	X	
FLETC-IT-08-03	Installation of Momentum System Software is not Logged or Reviewed		09-03
FLETC-IT-08-04	The SDLC for Momentum is not Finalized		09-04
FLETC-IT-08-05	Momentum Backups are not Tested	X	
FLETC-IT-08-06	The Momentum Contingency Plan is not Complete	X	
FLETC-IT-08-07	Incidents are not Tracked in an Incident Response Management System	X	
FLETC-IT-08-08	Lack of Policies and Procedures over Incompatible Duties within	X	

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
	Procurement Desktop		
FLETC-IT-08-09	Telecom Room Access Controls Needs Improvement	X	
FLETC-IT-08-10	Momentum and Procurement Desktop Access Controls Need Improvement	X	
FLETC-IT-08-11	IT Security Awareness Training is in Draft Form	X	
FLETC-IT-08-12	Policies and Procedures over Mobile Code Technologies are not Developed	X	
FLETC-IT-08-13	Policies and Procedures for Review of Momentum Audit Logs are not Developed	X	
FLETC-IT-08-14	Policies and Procedures for Restricting Access to Momentum System Software are not Developed	X	
FLETC-IT-08-15	Policies and Procedures for Segregating Incompatible Duties in Momentum are not Developed	X	
FLETC-IT-08-16	Policies and Procedures over VoIP Technologies are not Developed	X	
FLETC-IT-08-17	Background Investigations for Contractors are not Consistently Performed	X	
FLETC-IT-08-18	Procurement Desktop Audit Logs Need Improvement	X	
FLETC-IT-08-20	Access to FLETC LAN is not Effectively Controlled	X	
FLETC-IT-08-21	FLETC Manual 4300: IT System Security Program and Policy is not Finalized	X	
FLETC-IT-08-22	Access Controls over Procurement Desktop are not Effective	X	
FLETC-IT-08-23	Lack of Procedures for Recertifying Procurement Desktop Users	X	
FLETC-IT-08-24	Momentum/Procurement Desktop Contingency Plan is not Maintained at the Alternate Processing Site	X	
FLETC-IT-08-25	Policies and Procedures over Anti-Virus Software for Servers and System Maintenance are not Finalized	X	
FLETC-IT-08-26	Configuration Management Weaknesses on the Procurement Desktop, Momentum, and GSS		09-26
FLETC-IT-08-27	Patch Management Weaknesses on Procurement Desktop and GSS	X	
FLETC-IT-08-29	Procurement Desktop Backups are not Tested	X	
FLETC-IT-08-30	Momentum Users are Granted Inappropriate Super User Access	X	
FLETC-IT-08-31	Momentum Security Violation Events are not Reviewed		09-31
FLETC-IT-08-32	Momentum Segregation of Duties Controls are not Effective	X	
ICE-IT-08-04	Weak ICE Network/ADEX Access Controls Exist	X	
ICE-IT-08-09	ICENet\ADEX Contingency Plan is not Stored at Offsite Locations	X	
ICE-IT-08-10	ICENet\ADEX Backup Facility Access is not Appropriately Secured from Unauthorized Access	X	
OCIO-IT-08-01	Formal Agreement Not in Place for CBP Use of the Stennis Data Center as a Business Continuity Facility	X	
OCIO-IT-08-02	DHS SDLC has not been Finalized	X	
TSA-IT-08-01	FINCEN Service Continuity Weakness	X	

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
TSA-IT-08-03	Security Configuration Management Policy and Procedures Weakness	X	
TSA-IT-08-05	Contractor Background Investigation Weakness	X	
TSA-IT-08-06	Weaknesses in Specialized Role-based Training for Individuals with Significant Security Responsibilities	X	
TSA-IT-08-13	Weakness in the CAS C&A Package	X	
TSA-IT-08-15	TSA IS Security Awareness Training Weakness	X	
TSA-IT-08-18	Vulnerability Assessment Weakness – Configuration Management	X	
TSA-IT-08-19	Vulnerability Assessment Weakness – Patch Management	X	
TSA-IT-08-20	Weaknesses over the TSA Computer Access Agreement and Termination Clearance Processes		09-20
TSA-IT-08-21	CAS, FPD, and Sunflower Change Control Policy and Procedures Weakness	X	
TSA-IT-08-22	CAS and FPD Change Control Weakness	X	
TSA-IT-08-23	Weaknesses in Controls Over the Scripting Process		09-23
TSA-IT-08-24	Civilian Background Investigation Weakness	X	
TSA-IT-08-26	Access Authorization and Recertification Weaknesses within the User Management System (UMS)	X	
TSA-IT-08-27	CAS and FPD Access Recertification Weakness	X	

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

Homeland Security

APR - 2 2010

MEMORANDUM FOR: Richard Skinner
Inspector General

FROM: Richard Spires
Chief Information Officer

Peggy Sherry
Acting Chief Financial Officer

Robert West
Chief Information Security Officer

SUBJECT: OIG Draft Audit Report - *Information Technology Management Letter for FY 2009 DHS Integrated Audit – For Official Use Only*

We have reviewed the Office of the Inspector General's (OIG) draft audit report, *Information Technology Management Letter (ITML) for FY 2009 DHS Integrated Audit*, dated December 9, 2009. We concur with the Financial Systems Security findings contained within your audit report.

The DHS Chief Information Officer (CIO) and Chief Financial Officer (CFO) have aligned the Federal Information Security Management Act (FISMA) framework with the internal control assessment process, governed by Office of Management and Budget (OMB), Circular A-123, *Management's Responsibility for Internal Control* across the Department to improve financial systems security at the Department. Major activities under this integrated approach include:

- Issued a final *Internal Control Playbook Management Assurance Process Guide Fiscal Year 2009* Addendum to the Information Technology General Controls (ITGC) Implementation Guide which provides guidance on DHS's approach to documenting and testing the design effectiveness of financial system ITGCs.
- Updated the CFO Designated Systems List for FY09 as a result of ITGC Systems Mapping performed in FY08. The list specifies the financial systems that require additional management accountability to ensure effective controls exist over financial reporting.
- Performed FY09 A-123 ITGC Assessments at the following Components – U.S. Citizenship and Immigration Services, Immigration and Customs Enforcement, Customs and Border Protection, Federal Law Enforcement Training Center, and U.S. Secret Service. The following details the A-123 ITGC Assessments for FY09:

- Performed walkthroughs with points of contact to discuss the process and procedures surrounding the CFO Designated Systems key controls.
- Updated Tests of Design, including review and status for corrective actions identified in FY08.
- Performed Tests of Operating Effectiveness for controls that are properly designed.
- Issued the FY09 DHS Secretary's Annual Assurance Statement based on FY09 test results.

Issued the FY 2010 DHS Information Security Performance Plan which includes the requirement to ensure key financial system security controls are tested annually. Updated DHS 4300A, Sensitive Systems Handbook, Attachment H: *POA&M Process Guide*, to include the CFO's role and responsibilities related to the POA&M process; and incorporated risk levels and risk ratings for financial systems to assist Components and DHS in better understanding the overall risk to information systems and data.

- Implemented tracking of A-123 ITGC weaknesses under the Weakness Remediation metric on the FISMA Scorecard.
- Provided root cause analysis training to DHS Components and assistance with addressing A-123 ITGC deficiencies in POA&Ms; provided POA&M training for 215 financial systems security professionals at eleven Components and DHS Headquarters.
- Improved tracking of all IT audit recommendations to ensure traceability to POA&Ms in TAF.
- Developed a POA&M Issues Metrics List to track financial systems deficiencies identified by the Components, DHS Headquarters, OIG Reports, and financial assessments to resolution.
- Updated Departmental Information Assurance tools, e.g., Risk Management System (RMS) and Trusted Agent FISMA (TAF) to monitor and track compliance with requirements for CFO Designated Systems.

Additionally, DHS plans to modify the scope of A-123 assessments for FY 2010 to perform verification and validation procedures to ensure POA&Ms address root causes of financial system security control deficiencies identified from the financial statement audits and FISMA annual assessments.

The DHS CIO and CFO remain fully committed to working together to secure DHS financial systems and continue to raise the standards for ITGCs 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.

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, Policy
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.