Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the FY 2008 DHS Financial Statement 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-09-50

April 2009

Office of Inspector General

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

Homeland Security

April 6, 2009

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 (IT) management letter for the FY 2008 DHS financial statement audit as of September 30, 2008. It contains observations and recommendations related to information technology internal control that were not required to be reported in the financial statement audit report (OIG-09-09, November 2008) 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 2008 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated December 5, 2008, and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control or make conclusions 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 this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner

Richard L. Skinner
Inspector General

KPMG LLP
2001 M Street, NW
Washington, DC 20036

December 5, 2008

Inspector General
U.S. Department of Homeland Security

Chief Information Officer
U.S. Department of Homeland Security

Chief Financial Officer
U.S. Department of Homeland Security

Ladies and Gentlemen:

We were engaged to audit the accompanying consolidated balance sheet of the U.S. Department of Homeland Security (DHS) as of September 30, 2008, and the related statement of custodial activity for the year then ended (referred to herein as "financial statements"). We were not engaged to audit the statements of net cost, changes in net position, and budgetary resources for the year ending September 30, 2008 (referred to herein as "other financial statements"). Because of matters discussed in our *Independent Auditors' Report*, dated November 14, 2008, the scope of our work was not sufficient to enable us to express, and we did not express, an opinion on the financial statements.

In connection with our fiscal year (FY) 2008 engagement, we considered 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 in order to determine our procedures. We limited our internal control testing to those controls necessary to achieve the objectives described in *Government Auditing Standards* and Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements*. We did not test all internal controls relevant to operating objectives as broadly defined by the *Federal Managers' Financial Integrity Act of 1982* (FMFIA). The objective of our engagement was not to provide an opinion on the effectiveness of DHS' internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of DHS' internal control over financial reporting. Further, other matters involving internal control over financial reporting 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, 2008, and the related statement of custodial activity for the year then ended, and had we been engaged to audit the other FY 2008 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 misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects DHS' ability to initiate, authorize, record, process, or report financial data reliably in accordance with U.S. generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of DHS' financial statements that is more than inconsequential will not be prevented or detected by DHS' internal control over financial reporting. A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control.

During our audit, we noted certain matters involving internal control and other operational matters with respect to financial systems Information Technology (IT) general and application controls. Collectively, we consider these IT control weaknesses to collectively contribute to a material weakness regarding IT for the FY 2008 audit of the DHS consolidated financial statements.

The material weakness described above is presented in our *Independent Auditors' Report*, dated November 14, 2008. This letter represents the separate restricted distribution report mentioned in that report.

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 is 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 information technology infrastructure within the scope of the FY 2008 DHS financial statement audit in Appendix A; a description of each internal control finding in Appendix B; and the current status of the prior year NFRs in Appendix C. Our comments related to financial management and reporting internal controls have been presented in a separate letter to the Office of Inspector General and the DHS Chief Financial Officer dated December 5, 2008.

This report is intended solely for the information and use of DHS management, DHS Office of Inspector General, OMB, U.S. Government Accountability Office, and the U.S. Congress, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

Page

APPENDICES

Department of Homeland Security

Information Technology Management Letter
September 30, 2008

OBJECTIVE, SCOPE AND APPROACH

We were engaged to perform an audit of Department of Homeland Security (DHS) Information Technology (IT) general controls in support of the fiscal year (FY) 2008 DHS balance sheet and statement of custodial activity audit engagement. The overall objective of our engagement was to evaluate the effectiveness of IT general controls of DHS' financial processing environment and related IT infrastructure as necessary to support the engagement. The Federal Information System Controls Audit Manual (FISCAM), issued by the Government Accountability Office (GAO), formed the basis of our audit. The scope of the IT general controls assessment is described in Appendix A.

FISCAM was designed to inform financial auditors about IT controls and related audit concerns to assist them in planning their audit work and to integrate the work of auditors with other aspects of the financial audit. FISCAM also provides guidance to IT auditors when considering the scope and extent of review that generally should be performed when evaluating general controls and the IT environment of a federal agency. FISCAM defines the following six control functions to be essential to the effective operation of the general IT controls environment.

- *Entity-wide security program planning and management (EWS)* – Controls that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related security controls.
- *Access control (AC)* – Controls that limit and/or monitor access to computer resources (data, programs, equipment, and facilities) to protect against unauthorized modification, loss, and disclosure.
- *Application software development and change control (ASDCC)* – Controls that help to prevent the implementation of unauthorized programs or modifications to existing programs.
- *System software controls (SS)* – Controls that limit and monitor access to powerful program that operate computer hardware and secure applications supported by the system.
- *Segregation of duties (SD)* – Controls that constitute policies, procedures, and an organizational structure to prevent one individual from controlling key aspects of computer-related operations, thus deterring unauthorized actions or access to assets or records.
- *Service continuity (SC)* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

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

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

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

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2008, DHS components took significant steps to improve their financial system security and address prior year IT control weaknesses, which resulted in the closure of more than 40% of our prior year IT control findings. Additionally, some DHS components reduced the severity of the weaknesses when compared to findings reporting in the prior year. However, during FY 2008, we continued to identify IT general control weaknesses. The most significant weaknesses from a financial statement audit perspective include: 1) excessive unauthorized access to key DHS financial applications; 2) application change control processes that are inappropriate, not fully defined, followed, or effective; 3) service continuity issues impacting DHS' ability to ensure that DHS financial data is available when needed. Collectively, the IT control weaknesses 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 weaknesses 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 information technology findings were combined into one material weakness regarding Information Technology for the FY 2008 audit of the DHS consolidated financial statements.

The FISCAM IT general control areas that continue to present a risk to financial systems data integrity include:

1. Excessive access to key DHS financial applications, including; weaknesses in access documentation and approval, disabling account access upon termination, instances of inadequate or weak passwords, workstations, servers, or network devices were configured without necessary inactivity time-outs and up-to-date anti-virus software.

2. Application change control processes that are inappropriate, not fully defined, followed, or effective, including instances where database scripts are not properly documented or monitored; instances where changes made to the system were not always properly approved, tested, documented or performed through System Change Requests (SCRs), instances where policies and procedures regarding change controls were not in place to prevent users from having concurrent access to the development, test, and production environments of the system, or for restricting access to application system software and system support files, and policies and procedures surrounding the system development life cycle (SDLC) process have not been documented or finalized.

3. Service continuity issues impacting DHS' ability to ensure that DHS financial data is available when needed, including; instances where the Continuity of Operations Plan (COOP) does not include an accurate listing of critical information technology systems, did not have critical data files and an alternate processing facility documented, and was not adequately tested, and various weaknesses identified in alternate processing sites.

While the recommendations made by KPMG 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 CONTROL FINDINGS BY AUDIT AREA

Conditions: In FY 2008, the following IT and financial system control weaknesses were identified at DHS. Many of the issues identified during our FY 2008 engagement were also identified during FY 2007. The following IT and financial system control weaknesses result in IT being reported as contributing to a material weakness for financial system security.

1. Access controls – we noted:

   - One component does not maintain a centralized listing of contract personnel, including employment status. Additionally, non-disclosure agreements are not consistently signed by contractors.
   - Physical access authorization forms are not documented or maintained at one component. Additionally, procedures for granting access to the computer room are not documented. At another component, physical access authorizations are not consistently reviewed which resulted in excessive access to DHS servers.
   - Account management documentation was not updated when modifications were performed at one component. At three components, documentation of user access authorization was not maintained. Additionally, user account lists were not periodically reviewed for appropriateness, resulting in inappropriate authorizations and excessive user access privileges across seven DHS components.
   - System user roles and permissions are not documented at one component.
   - Access request forms are not being completed for all financial system users on a consistent basis at four components.
   - Excessive access existed within financial applications at two DHS components.
   - Emergency access was not appropriately restricted or was not approved by the Information System Security Manager (ISSM) at one component.
   - At one component, access review procedures for key financial applications do not include the review of all user accounts to ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked, and that privileges associated with each individual are still authorized and necessary.
   - Accounts were not disabled or removed promptly upon personnel termination at one DHS component. Procedures over the process of finalizing and implementing entity-wide processes for account terminations and related notifications are in draft and have not been implemented or communicated at two components.
   - Individuals were not required to sign rules of behavior or computer access agreements prior to gaining access to financial systems at two components.
   - Five DHS components had instances of inadequate or weak passwords that existed on key systems, servers and databases that house financial data. Additionally, one component was not

consistently remediating password vulnerabilities identified by scans in order to mitigate weak password configurations.

- Instances at three components where workstations or financial applications were configured with inadequate inactivity time-outs.
- Instances at four components where workstations, servers, or network devices were configured without necessary security patches, inadequate security configurations, or up-to-date anti-virus software.
- Procedures regarding the use of anti-virus software have not been finalized for one DHS component.
- At one component, a script which disables accounts after 30 days of inactivity was not functioning appropriately for the full fiscal year.
- Audit logs were not reviewed or evidence of audit log review is not retained at five DHS components. At two components, audit logs were not appropriately configured to capture security events. Additionally, at one component, audit logs of privileged database administrator actions are not enabled or reviewed.
- At one component, policy and procedures for review of audit logs are not documented.
- Media sanitation procedures do not reflect the current process in place at one component.
- Policy and procedures regarding implementation of Voice Over Internet Protocol (VOIP), wireless technologies, cryptographic tools, and sharing data with external parties are not finalized at one component.

2. Application software development and change controls – we noted:

   - At two components, procedures over approval, testing, and documentation requirements for database scripts remain in draft form. The testing, approval, and implementation documentation is not consistently documented for all scripts. In addition, the components do not monitor scripts run in the database through audit logging and has not developed a technical solution to monitor who accesses the database to run scripts or review what scripts are run. Analysis of the database scripts conducted by the components was incomplete and did not properly evaluate the financial statement impact of the scripts.
   - Change control policies and procedures are not fully documented and implemented at three DHS components.
   - Policies and procedures surrounding the SDLC process have not been documented or finalized for the Department and one component.
   - Emergency and non-emergency changes were made prior to management approval. Additionally, at five DHS components, instances where changes made to the system were not always documented or performed through SCRs, test plans, test results, approvals, or software modifications.
   - At two components, the contract with the support vendor did not include security configuration requirements that must be adhered to during the configuration management process.

- Policies and procedures over the authorization and use of mobile code technologies are in draft form for one DHS component.
- Excessive access to financial application program and support files at one component.

3. Service continuity – we noted:
    - The COOP does not include an accurate listing of critical information technology systems, did not have critical data files and an alternate processing facility documented, and was not adequately tested at one DHS component. Additionally, complete testing of a current and finalized Contingency Plan was not conducted for two components. At three components, the COOP and Business Continuity Plans were not updated to reflect results of testing.
    - The Contingency Plan is not distributed or stored at off-site locations for two components.
    - An alternate processing site is not operational for one DHS component. In another instance, the recovery facility was insufficient to fully and properly restore systems and conduct continuity testing.
    - Documented hardware maintenance procedures do not exist at one component.
    - Access to the backup facility is not appropriately secured from unauthorized access at one component.
    - Backup tapes are not tested on a quarterly basis at two components.

4. Entity-wide security program planning and management – we noted:
    - Four components were not compliant with the requirements of the Federal Financial Management Improvement Act (FFMIA).
    - A formal agreement has not been established between the Department and their alternate processing site.
    - Interconnection Security Agreements (ISA) between two DHS components and external parties were not in place or not finalized.
    - A risk assessment for a major financial application at two components has not been completed and the associated System Security Plan (SSP) remains in draft form. At another component, the SSP is not accurate and up-to-date.
    - At one component, vulnerabilities identified from periodic scans are not reported and tracked via the Plan of Action and Milestones (POA&M) process.
    - Incident response procedures were not finalized and implemented at one component.
    - One component does not maintain a complete and up-to-date inventory listing of workstations.
    - Policies and procedures for system administrator responsibilities are not up-to-date for one component.

- Financial application users had not completed IT security awareness training at four components. Additionally, one of these components has not implemented role-based security awareness training.
- At two components, policies or procedures have not been implemented to require that a favorably adjudicated background investigation be completed for all contractor personnel.
- Background investigations for all civilian employees have not been completed and civilian position sensitivity designations have not been determined in accordance with DHS guidance at two components.
- Contractors and employees without completed background investigations retained access in DHS systems at one component.
- At one component, procedures surrounding the system used to track contractor personnel data have not been formally documented.
- Termination forms were not consistently completed and documented for separated employees and contractors at two components.

5. System software – we noted:

   - At two components, security patch management weaknesses exist on hosts supporting the key financial applications and general support systems.
   - Security configuration management weaknesses exist at three components on hosts supporting the key financial applications and the underlying general support systems.
   - At one component, procedures for identifying and installing patches are in draft and have not been implemented.
   - Monitoring and patch distribution software is not installed on all workstations at one component.
   - Policy and procedures for restricting access to system software have not been developed at one component.
   - System specific policies and procedures to review system software activity have not been developed at one component.
   - Evidence of system software audit log review is not retained at one DHS component.

6. Segregation of duties – we noted:

   - Segregation of duties policies have not been developed at one component.
   - Instances at two components where policies and procedures regarding change controls were not in place to prevent users from having concurrent access to the development, test, and production environments of the system, or for restricting access to application system software and system support files.
   - Evidence of the review of system programmer actions with access to production financial servers is not documented at one component.

- At one component, financial system users have the ability to create and approve payment vouchers.

Recommendations: We recommend that the DHS Office of Chief Information Officer (OCIO), in coordination with the DHS Office of Chief Financial Officer (OCFO), and the DHS component OCIOs and OCFOs make the following improvements to the Department's financial management systems:

1. For access controls:

   a) Develop and maintain a centralized listing of contract personnel and require all contractors to sign non-disclosure agreements;

   b) Develop and appropriately implement a physical access authorization process to ensure that physical access requests are completed and documented for all individuals prior to granting access to sensitive facilities;

   c) Develop and appropriately implement an access authorization process that ensures that a request is completed and documented for each individual prior to granting him/her access to a financial application or database;

   d) Document financial system user roles and permissions;

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

   f) Develop and implement procedures that will appropriately restrict the use of emergency or temporary access within DHS systems and that require documented supervisory approval from the ISSM confirming this access is needed;

   g) Implement a process to ensure that all accounts of terminated individuals from the system are immediately removed/end-dated/disabled upon their departure. This includes both terminated employees and contractors;

   h) Ensure that all individuals sign a rules of behavior or computer access agreement document prior to granting him/her access to a financial application or database;

   i) Enforce password controls that meet DHS' password requirements on all key financial systems. Conduct periodic vulnerability assessments, whereby systems are periodically reviewed for access controls not in compliance with DHS and Federal guidance and ensure that action is taken to remediate any security weaknesses identified;

   j) Enforce inactivity time-outs on all workstations and applications as required by DHS policy;

   k) Complete procedures regarding the use of anti-virus software. Develop procedures to regularly review and monitor workstations and servers to ensure that the most up-to-date patches, necessary security configurations, and virus protection software is installed;

   l) Ensure that all accounts that have been inactive for over 30 days are disabled as required by DHS policy;

   m) Develop and implement detailed procedures requiring the review of operating system and application logs for suspicious activity and conduct audit log reviews on a consistent and timely basis;

n) Develop and implement media sanitation procedures that are consistent with DHS policy and the current practices in place; and

o) Finalize and implement policy and procedures regarding VOIP, wireless technologies, cryptographic tools, and sharing data with external parties.

2. For application software development and change control:

a) Implement and better document a single, integrated script change control process that includes clear lines of authority to financial and IT management personnel, enforced responsibilities of all participants in the process, and documentation requirements. Additionally, continue efforts to complete an in-depth analysis of active scripts, with the following objectives: All changes to active scripts and new scripts should be subject to an appropriate software change control process to include testing, reviews, and approvals and all active scripts should be reviewed for impact on financial statement balances;

b) Implement a single, integrated change control process over the DHS components' financial systems with appropriate internal controls to include clear lines of authority to the components' financial management personnel and to enforce responsibilities of all participants in the process and documentation requirements. Further develop and enforce policies that require changes to the configuration of the system are approved and documented, and audit logs are activated and reviewed on a periodic basis;

c) Develop, document and implement a formalized SDLC process;

d) Ensure that all contracts with support vendors document all responsibilities and requirements of the change controls process;

e) Develop and implement formal policies and procedures for restricting access to DHS system software, and promulgate it to all needed personnel, to be in compliance with the DHS Sensitive System Policy Directive 4300A; and

f) Finalize and implement policies and procedures over the authorization and use of mobile code technologies.

3. For service continuity:

a) Update the COOP to document and prioritize an accurate listing of critical IT systems;

b) Perform testing of key service continuity capabilities, including contingency planning. Ensure that all contingency plans and related documentation are updated upon completion of testing;

c) Ensure that contingency plans and emergency documentation are distributed to the appropriate individuals and are stored off-site;

d) Ensure that alternate processing sites are made operational;

e) Document and implement hardware maintenance procedures;

f) Establish and implement a procedure for authorizing and maintaining a backup facility access list to ensure that only authorized individuals are granted access; and

g) Test backups at least quarterly.

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

    a) Develop and implement corrective action plans to address and remediate identified instances of non-compliance with FFMIA. Continue to improve and monitor component compliance with applicable DHS and Federal security requirements.

    b) Ensure that that formal agreements with service providers are established and finalized;

    c) Ensure that ISAs are documented and finalized between DHS components and all external parties;

    d) Finalize and implement the certification and accreditation package for all key financial systems in accordance with DHS and National Institute of Standards and Technology (NIST) guidance;

    e) Ensure that all vulnerabilities and weaknesses are reported and tracked via the POA&M process.

    f) Develop procedures to regularly review and monitor the workstations to ensure that monitoring software is installed on all machines;

    g) Ensure that new and existing workstations are accounted for in an appropriate fashion;

    h) Review of policies and procedures for security administrators to reflect the current operating environment;

    i) Ensure that IT security awareness training is completed by all personnel;

    j) Create and implement contractor background investigation policies and procedures in order to establish requirements and ensure compliance with the DHS Sensitive System Policy Directive 4300A. This includes the verification that all contracts include the appropriate position sensitivity designation requirements for contracted personnel;

    k) Perform initial background investigations and re-investigations for civilian employees in accordance with position sensitivity designations at no less than the Moderate level as required by DHS directives. In addition, conduct civilian background re-investigations every ten (10) years, as required by DHS directives;

    l) Finalize, communicate, and distribute procedures over contractor tracking. In addition, continuously monitor controls over the contractor tracking system to verify that contractor data within the system remains current and accurate; and

    m) Implement an automated process or system that will notify system owners of terminated contractor, military, and civilian personnel. Additionally, ensure that employee exit procedures are implemented for all separating personnel.

5. For system software:

    a) Implement a patch management and security configuration process, and enforce the requirement that systems are periodically tested by DHS components and the DHS Office of Chief Information Officer. Additionally, perform corrective actions on the specific patch and configuration weaknesses identified;

    b) Actively monitor the use of and changes related to operating systems and other sensitive utility software and hardware;

c) Develop and implement procedures for reviewing system software activity; and

d) Develop and implement policy and procedures for restricting access to system software.

6. For segregation of duties:

a) Develop and implement segregation of duties policies. Ensure that segregation of duties policies are enforced for all financial systems;

b) Develop and implement procedures to perform a periodic review of access to financial application software and support files to determine whether access is valid, consistent with job responsibilities, and according to the least privilege principle. Remove excessive access to the all DHS financial application software and support files; and

c) Monitor the activities of system programmers as well as the use of operating systems software and other sensitive utility software and hardware. Retain evidence of the reviews.

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

A contributing cause to the numerous repeated findings is that DHS lacks an effective agency-wide method of tracking the remediation progress made on findings at various components. In addition, while the components have made improvements in addressing the root cause of IT weaknesses, we found that focus is often placed on the tracking of response to audit recommendations, instead of on developing the most effective method of addressing the actual control weakness. When weaknesses in controls or processes are identified, the corrective actions address the symptom of the problem and do not the correct root cause which amounts to a temporary fix.

Further, insufficient testing of IT controls and testing of remediation activities by individual DHS components and by the DHS CIO limits DHS' ability to confirm that IT weaknesses are addressed. The most prevalent reason as to why these weaknesses are present is the lack of prioritization in taking the necessary actions to improve the IT control environment around the Department's financial management systems.

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

Criteria: The *Federal Information Security Management Act* (FISMA) passed as part of the *Electronic Government Act of 2002,* mandates that Federal entities maintain IT security programs in accordance with OMB and NIST guidance. OMB Circular No. A-130, *Management of Federal Information Resources,* and various NIST guidelines describe specific essential criteria for maintaining effective general IT controls. In addition OMB Circular No. A-127 prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems. 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: (1) to 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. In closing, for this year's IT audit we assessed the DHS component's compliance with the DHS Sensitive System Policy Directive 4300A.

APPLICATION CONTROL FINDINGS

Condition: In FY 2008, the following IT application control weakness was identified at DHS. This application control weakness, in combination with the IT and financial system control weaknesses detailed above result in IT being reported as contributing to a material weakness for financial system security.

Four (4) contractors and an additional user account used by contractors had super user access privileges within the core financial system at one component. Based on notification of this weakness, component management responded by removing the access as of September 24, 2008.

Recommendation: No recommendation was issued as the weakness was remediated by the component upon notification.

MANAGEMENT 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 2008 DHS Financial Statement Audit Engagement

Department of Homeland Security
Information Technology Management Letter
September 30, 2008

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

Locations of Audit: ICE Headquarters (HQ) in Washington, D.C [redacted]

Key Systems Subject to Audit:

[redacted] – ICE owns and operates [redacted]. ICE performs accounting services for other DHS components, such as the United States Citizen and Immigration Services, Management Directorate, Science and Technology Directorate, and US-Visit, using [redacted] per the shared services agreement these agencies have with ICE. [redacted] is a commercial off-the-shelf financial reporting system that was fully implemented in fiscal year (FY) 2003. [redacted] is the official system of record and is built in [redacted]. It includes the core system used by accountants, [redacted] that is used by standard users, and a [redacted] payroll interface. [redacted] supports all USCIS/ICE core financial processing and uses a Standard General Ledger (SGL) for the accounting of agency financial transactions.

Locations of Audit: USCIS HQ in Washington, D.C [redacted]

Key Systems Subject to Audit:

- [redacted] – The ICE component owns and operates [redacted]. ICE performs the financial reporting function for USCIS, using [redacted] per the shared services agreement with USCIS. [redacted] is a commercial off-the-shelf financial reporting system that was fully implemented in FY 2003. [redacted] is the official system of record and is built in [redacted]. It includes the core system used by accountants, [redacted], which is used by average users, and a National Finance Center payroll interface. [redacted] supports all USCIS core financial processing. [redacted] uses a SGL for the accounting of agency financial transactions.

- [redacted] - [redacted] provides USCIS with a decentralized [redacted] based system that supports the requirements of the Direct Mail Phase I and II, Immigration Act of 1990 (IMMACT 90, Pub. L. No. 101-649) and USCIS forms improvement projects. The [redacted] is located at each of the service centers [redacted]. The main purpose of [redacted] is to enter and track immigration applications.

- [redacted] - The purpose of [redacted] is to track and manage naturalization applications. [redacted] resides on multiple platforms, including a [redacted]. [redacted] data is centrally stored within one [redacted] Software is developed and maintained in the [redacted] relational database and [redacted] environments.

Locations of Audit: Coast Guard HQ in Washington, DC [redacted].

Key Systems Subject to Audit:

- [redacted] – [redacted] is the core accounting system that records financial transactions and generates financial statements for the Coast Guard. [redacted] is hosted at [redacted] the Coast Guard's primary data center. It is a customized version of [redacted].

- [redacted] – The [redacted] 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. [redacted] is interconnected with the [redacted].

- [redacted] - [redacted] is the document image processing system, which is integrated with an [redacted] [redacted] allows electronic data and scanned paper documents to be imaged and processed for data verification, reconciliation and payment. [redacted] utilizes [redacted] to scan documents and to view the images of scanned documents and to render images of electronic data received.

[redacted] [redacted] is a commercial product used to reconcile payment information retrieved from the United States Department of the Treasury. [redacted] reconciles items that Treasury has paid for Coast Guard, with items [redacted] has paid to Treasury. This system is hosted on a [redacted]

- [redacted] - [redacted] is a Microsoft Access Database and is maintained at [redacted] and information from [redacted] is uploaded to this instance monthly. After reconciliation, [redacted] information is uploaded into [redacted]

- [redacted] - [redacted] is a mainframe application used for paying Coast Guard active and reserve personnel's payroll.

- [redacted] - [redacted] is the system of record and all functionality, data entry, and processing of payroll events is conducted exclusively in [redacted].

[redacted] [redacted] – Formerly named the [redacted] is hosted at [redacted] [redacted] is the primary financial application for the [redacted]

- [redacted] - [redacted], is a web-based application designed to automate the management of Coast Guard's vessel logistics by supporting the following functions: configuration, maintenance, supply and finance.

- [redacted] - [redacted] is hosted at the Coast Guard's [redacted] and provides core information about the USCG shore facility assets and facility engineering. The application tracks activities and assists in the management of the [redacted] Program and the [redacted] Program.

Locations of Audit: The [redacted] in [redacted] and the [redacted]

Key Systems Subject to Audit:

- [redacted] - [redacted] is CBP's financial management system that consists of a 'core' system, which supports primary financial accounting and reporting processes, and a number of additional subsystems for specific operational and administrative management functions. [redacted] is a client/server-based financial management system that was implemented beginning in FY 2004 to ultimately replace the [redacted] [redacted]-based financial system using a phased approach.

- [redacted] – [redacted] is a collection of business process mainframe-based systems used by CBP to track, control, and process all commercial goods, conveyances and private aircraft entering the U.S. territory for the purpose of collecting import duties, fees, and taxes owed to the Federal government. Key application software within [redacted] includes systems for data input/output, entry and entry summary, and collection of revenue.

[redacted] - [redacted] is the commercial trade processing system being developed by CBP to facilitate trade while strengthening border security. [redacted] is being deployed in phases, with a final full deployment scheduled for FY 2010. As [redacted] is partially implemented now and processes a significant amount of revenue for CBP, [redacted] was included in a limited scope in the FY 2008 financial statement audit. The [redacted] [redacted] [redacted]

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

Key Systems Subject to Audit:

- [redacted] – The system of record for the DHS consolidated financial statements is [redacted] The DHS components update [redacted] on a monthly basis with data extracted from their core financial management systems. [redacted] subjects component financial data to a series of validation and edit checks before it becomes part of the system of record. Data cannot be modified directly in [redacted] but must be resubmitted as an input file.

- [redacted] – [redacted] interfaces with [redacted] and is used for the consolidation of the financial data and the preparation of the DHS financial statements. [redacted] is also administered by Treasury.

  The [redacted] and [redacted] applications reside on the Department of Treasury's network and are administered by Treasury. Treasury is responsible for the administration of the [redacted] and the [redacted]. The DHS Office of Financial Management is responsible for the administration of DHS user accounts within the [redacted].

Location of Audit: FLETC HQ in [redacted]

Key Systems Subject to Audit:

- [redacted] - FLETC's core financial management system that processes financial documents generated by various FLETC divisions in support of procurement, payroll, budget and accounting activities. All financial, procurement and budgeting transactions where the FLETC is involved are processed by [redacted]

[redacted] FLETC's procurement management system, which is used for the tracking of procurement activities at various FLETC locations. [redacted] is a system used to input requisitions for the acquisition of goods and services. [redacted] purpose is to process contractual documents generated by FLETC in support of procurement activities. The system resides on an [redacted] and the front-end of the system is integrated with [redacted]

Department of Homeland Security
Information Technology Management Letter
September 30, 2008

Locations of Audit: FEMA HQ in Washington, D.C., [redacted]

Key Systems Subject to Audit:

- [redacted] – [redacted] is the key financial reporting system, and has several feeder subsystems (budget, procurement, accounting, and other administrative processes and reporting).

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

- [redacted] - The [redacted] application acts as a central repository of all data submitted by the Write Your Own (WYO) companies. [redacted] also supports the WYO program, primarily by ensuring the quality of financial data submitted by the WYO companies to [redacted] is [redacted] that runs on the [redacted] mainframe logical partition in [redacted].

- [redacted] - The general ledger application used by [redacted] to generate the [redacted] financial statements. [redacted] is a client-server application that runs on a [redacted] server in [redacted] which is secured in the local area network room. The [redacted] client is installed on the desktop computers of the [redacted] Bureau of Financial Statistical Control group members.

- [redacted] - [redacted] is a web based application which was developed by Digital Systems Group specifically for FEMA grants. [redacted] allows grantees access to their grant funds as well as upload [redacted] online. Draw down transaction information from [redacted] is interfaced with [redacted] then interfaces with Treasury to transfer payment information to Treasury, resulting in a disbursement of funds to the grantee.

Locations of Audit: TSA HQ in Washington, D.C. [redacted]

Key Systems Subject to Audit:

- [redacted] – [redacted] is the core accounting system that records financial transactions and generates financial statements for the Coast Guard. [redacted] is hosted at the [redacted] in [redacted]. [redacted] interfaces with [redacted] Additionally, [redacted] fixed asset module for property management is interconnected to the [redacted] [redacted] that is hosted at [redacted]

- [redacted] – The [redacted] application used to create and post obligations to the core accounting system. It allows users to enter funding, create purchase requests, issue procurement documents, perform system administration responsibilities, and reconcile weekly program element status reports. [redacted] is interconnected with the [redacted] and [redacted] [redacted] and is located at the [redacted] [redacted]

- [redacted] is a customized third party commercial off the shelf product used for [redacted] [redacted] property management. [redacted] interacts directly with the fixed asset module in [redacted] Additionally, [redacted] is interconnected to the [redacted]

<u>Locations of Audit:</u> DHS HQ [redacted] The DHS-CIO is responsible for setting security and control related policy and guidance for the department. If any issues were identified during the audit that resulted in the DHS-CIO being the responsible party, an NFR was issued directly to them.

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

Appendix B

FY2008 Notices of IT Findings and Recommendations - Detail by DHS Organizational Element

<u>Notices of Findings and Recommendation – Definition of Risk Ratings:</u>

The Notices of Findings and Recommendations (NFR) were risk ranked as High, Medium, and Low based upon the potential impact that each weakness could have on the DHS component's IT general control environment and the integrity of the financial data residing on the DHS component's financial systems, and the pervasiveness of the weakness. The risk ratings are intended only to assist management in prioritizing corrective actions, considering the potential benefit of the corrective action to strengthen the IT general control environment and/or the integrity of the DHS consolidated financial statements. Correction of some higher risk findings may help mitigate the severity of lower risk findings, and possibly function as a compensating control. In addition, analysis was conducted collectively on all NFRs to assess connections between individual NFRs, which when joined together could lead to a control weakness occurring with more likelihood and/or higher impact potential. The risk ratings, used in this context, are not defined by *Government Auditing Standards*, issued by the Comptroller General of the United States, or the American Institute of Certified Public Accountants (AICPA) Professional Standards, and do not necessarily correlate to a significant deficiency, as defined by the AICPA Professional Standards and reported in our *Independent Auditors' Report* on the DHS consolidated financial statements, dated November 14, 2008.

<u>High Risk</u>: A control weakness that is more serious in nature affecting a broader range of financial IT systems, or having a more significant impact on the IT general control environment and /or the integrity of the financial statements as a whole.

<u>Medium Risk</u>: A control weakness that is less severe in nature, but in conjunction with other IT general control weaknesses identified, may have a significant impact on the IT general control environment and / or the integrity of the financial statements as a whole.

<u>Low Risk</u>: A control weakness minimal in impact to the IT general control environment and / or the integrity of the financial statements.

The risk ratings included in this report are intended solely to assist management in prioritizing its corrective actions.

Department of Homeland Security
FY2008 Information Technology
Notification of Findings and Recommendations – Detail

- **United States Citizenship and Immigration Services**

Department of Homeland Security
United States Citizenship and Immigration Services
FY2008 Information Technology
Notification of Findings and Recommendations – Detail

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
USCIS-IT-08-01	The [redacted] has not defined or documented the appropriate user permissions for the various roles granted to [redacted]	Define and document the various [redacted] roles and their associated user permissions.		**X**	**Medium**
USCIS-IT-08-02	[redacted] does not perform periodic [redacted] user access reviews to ensure that users' level of access remains appropriate.	• Annually review and approve the list of employees stating the appropriate level of access for each [redacted] employee with access to [redacted] • Annually review the list of [redacted] system and database administrators as well as review and approve the access level list; and • Ensure necessary adjustments in [redacted] account access levels are accomplished based on the input.		**X**	**Medium**
USCIS-IT-08-03	Management at the CIS HQ and the Service Centers [redacted]) has not completed or inadequately completed access forms for [redacted] and Citizenship and Immigration Services [redacted] system users.	Establish and enforce procedures for the completion and maintenance of user access forms for [redacted]		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
USCIS-IT-08-04	The [redacted] has not defined or documented the appropriate user permissions for the various roles granted to [redacted]	Define and document the various [redacted] roles and their associated user permissions.		**X**	**Low**
USCIS-IT-08-06	Access to USCIS server cage is not reviewed to determine whether access is appropriate and authorized, and USCIS does not provide oversight of the services the [redacted] is to provide.	• Establish and implement a procedure for authorizing and maintaining a current cage (server room) access list. • Establish and implement emergency exit and re-entry procedures. In addition, develop a process that assures all resources with access to the USCIS resources adhere to the policy and procedure.	**X**		**Medium**
USCIS-IT-08-07	Documented media sanitation procedures do not reflect the current processes at USCIS.	We recommend that USCIS update their policies and procedures to reflect their current media sanitization operation.	**X**		**Medium**
USCIS-IT-08-08	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**		**Medium**

Department of Homeland Security
FY2008 Information Technology
Notification of Findings and Recommendations – Detail

- **Immigration and Customs Enforcement**

Department of Homeland Security
FY2008 Information Technology
Notification of Findings and Recommendations – Detail

Immigration and Customs Enforcement

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
ICE-IT-08-04	During our FY 2008 follow-up, we noted the following: • [redacted] authorizes user access for [redacted] for several DHS components; however, they lack a process to document, maintain or monitor user access forms from all components that use [redacted] • Procedures for periodically recertifying and reviewing privileged [redacted] accounts were not established until June 2008.	• Develop and implement a written policy discussing the standard process for requesting, authorizing, and granting [redacted] access for all users. This policy should include users and system administrators at the various Bureaus that ICE supports, as well as ICE system administrators and users. This written policy should outline the responsibilities of the system administrators, to include the procedures for maintaining the access request forms for all users, and ICE's responsibility to periodically monitor all system administrators to ensure they are following the appropriate procedures. • Enhance procedures for annually recertifying [redacted] administrator accounts to ensure that the recertification procedures are executed properly.	X		Medium
ICE-IT-08-09	[redacted] contingency plan was not distributed to the offsite locations designated to support ICE in case of an emergency.	No recommendation will be offered as this issue was corrected upon notification.	X		Low
ICE-IT-08-10	[redacted] backup facility access is not appropriately secured from unauthorized access.	We recommend ICE develop procedures to periodically review the backup facility [redacted], and update it accordingly.	X		Low

Department of Homeland Security
FY2008 Information Technology
Notification of Findings and Recommendations – Detail

- **Customs and Border Protection**

Department of Homeland Security
FY2008 Information Technology
Notification of Findings and Recommendations – Detail

Customs and Border Protection

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-02	We noted that significant progress has been made at addressing this persistent finding. We noted that a full listing of connections to [redacted] has been developed and is maintained. However, we also noted that there are active connections to [redacted] that still do not have a documented [redacted] in place. Work is progressing within CBP to address the missing [redacted] but as of testing, we noted that not all connections had a documented [redacted]	We believe that work should continue to review and maintain a listing of active connections with the [redacted] and account for each connection with a documented [redacted]		**X**	**Medium**
CBP-IT-08-03	CBP does not maintain a centralized listing of contract personnel, including employment status. Currently, CBP only maintains contractor information for OIT contractors. While this is a majority of CBP contractors, it does not include all CBP contractors. Additionally, as a result of additional test work we noted data validity issues in the [redacted].	We recommend that CBP continue work on the [redacted] to ensure that all CBP contractors are included in the database and that the data for each contractor is complete and accurate.		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-08	We noted the following issues in regards to Security Audit Logs for [redacted] • A solution has been implemented to track and monitor security and audit related activity but has not been operational for the entire FY 2008. • There is a configuration weakness for capturing security and audit related activity in the [redacted] application. The configuration has changed on multiple occurrences in regards to tracking activity for the 'Logon to Account' field in FY 2008. • There is no defined method to generate and review security audit logs for security violations for the [redacted]	We recommend that CBP properly configure the application to capture appropriate data per DHS policy. We further recommend that a method for generating and reviewing security audit logs be developed for [redacted] according to CBP and DHS policy, to detect potential security events.		**X**	**Low**
CBP-IT-08-09	We noted that during FY 2008, CBP implemented a script to disable accounts after 30 days of inactivity. However, we noted that the script was not functioning appropriately for the full fiscal year and was fixed during the third quarter of FY 2008.	We recommend that CBP ensure that the updated script runs regularly on the system to disable user accounts after the DHS-specified period of inactivity.		**X**	**Low**
CBP-IT-08-12	As noted in FY 2007, we noted that [redacted] is not installed on all workstations for the majority of the fiscal year. Specifically, we noted that as of 3/31/2008, 4,751 workstations out of 50.282 accounted for workstations do not have [redacted] installed.	We recommend that CBP develop procedures to regularly review and monitor the workstations that have [redacted] installed and perform inquiries to determine why identified workstations do not have [redacted] installed.		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-13	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.	We recommend that CBP work with administrators across the country to ensure that new and existing workstations are added to a CBP [redacted] domain to allow for all workstations to be accounted for in an appropriate fashion.		X	**Medium**
CBP-IT-08-16	We noted that the [redacted] has been adjusted to limit active temporary and/or emergency access to 24 hours after the request. We noted, however, that the table is still being used and that administrator or supervisory approval is not required each time temporary or emergency access is activated and that ISSM approval is not required, as required in DHS policy.	• Develop and implement procedures that will appropriately restrict the use of emergency or temporary access within [redacted] and that requires documented supervisory approval from the ISSM confirming this access is needed. • Perform regular recertifications of the emergency access table to ensure persons with the capability to request temporary or emergency access need to remain on the emergency access table.		X	**Medium**
CBP-IT-08-18	We noted there are currently no procedures in place for the completion of semi-annual recertifications of [redacted] accounts. We also notes that a recertification of [redacted] [redacted] accounts is not performed on a semi-annual basis.	• Develop formal procedures for recertifying [redacted] [redacted] accounts and access to shared data. • Perform regular recertifications of [redacted] [redacted] accounts and access to shared data as required by developed procedures.		X	**Medium**
CBP-IT-08-21	We noted that when changes to a user's access are performed in [redacted] the log of these events is not regularly reviewed by personnel independent from those individuals that made the changes. We further noted that logs from March 2008 through July 2008 have not been reviewed by the [redacted] ISSO/Independent Reviewer.	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 [redacted] security audit logs.		X	**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-26	We noted that out of 25 dates, 6 [redacted] security violation report reviews were not provided.	We recommend that CBP follow DHS policy and maintain documented evidence of review for [redacted] for the duration outlined in DHS policy.		**X**	**Low**
CBP-IT-08-27	We noted that authorizations are not being maintained for personnel that have administrator access to [redacted]. Additionally, we noted in FY 2008 that access requests for new [redacted] administrator accounts are requested and approved verbally.	• Develop and implement procedures to restrict access [redacted] administrative capabilities, and • Require documented authorization requests and approval for each person requiring access to [redacted] administrative capabilities.		**X**	**Medium**
CBP-IT-08-28	We noted that procedures have been developed to require access request forms for any new account created for the [redacted] However, we noted that access request forms were not available for review for 3 accounts created by [redacted] administrators during FY 2008.	We recommend that CBP continue efforts to develop a method for tracking and consolidating access request forms for the [redacted] and continue to implement the procedures developed to control [redacted] account creation.		**X**	**Medium**
CBP-IT-08-29	We noted that procedures are in place for the completion of the termination forms for separating government employees. We noted, however, that the forms are not completed consistently, with employee and/or supervisor signature missing from seven of the 25 separated employees selected.	We recommend that CBP require managers to consistently complete the CBP-241 forms that are required as set forth in CBP directives and policy.		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-34	We noted that [redacted], the system used to enforce virus protection policies, was not installed on all CBP [redacted] on [redacted]. We noted that as of 8/11/2008, 0.25% of all workstations on [redacted] did not appear on the [redacted]. In addition to this, we could not conclude on whether all CBP workstations have antivirus protection, as those workstations that are not on [redacted] are not communicating with [redacted].	We recommend that CBP develop procedures to regularly review and monitor the workstations that have antivirus protection installed and perform inquiries to determine why identified workstations do not have the protection installed and updated.		**X**	**Low**
CBP-IT-08-35	During our technical testing, configuration management exceptions were identified on [redacted] [redacted] and hosts supporting the [redacted] and [redacted] applications.	Implement the corrective actions for the recommendations listed within the NFR.		**X**	**High**
CBP-IT-08-36	During our technical testing, patch management exceptions were identified on hosts supporting the [redacted] and the [redacted] and [redacted] applications.	Implement the corrective actions for the recommendations listed within the NFR.		**X**	**High**
CBP-IT-08-37	We noted that formal procedures do not exist for [redacted] review process. We further noted that informal procedures are used by the network security specialist to inspect the [redacted] for suspicious activity and to document the review.	We recommend that CBP create formal procedures to document the [redacted] security violation review process.	**X**		**Low**
CBP-IT-08-38	We noted that formal procedures do not exist for the review process of [redacted] audit and [redacted] [redacted]. We further noted that informal procedures are used by the [redacted] [redacted] to inspect logs for suspicious and unusual activity and to document the review.	We recommend that CBP create formal procedures to document the review process for [redacted] audit and [redacted].	**X**		**Low**
CBP-IT-08-39	We noted that the 'special characters' requirement under password complexity is not set.	We recommend that CBP follow DHS policy and improve password complexity by including special characters for the [redacted] application.	**X**		**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-40	We noted that access authorizations for emergency and temporary access to [redacted] are not approved by [redacted].	• Adjust CBP-level and [redacted]-level policies to require the ISSM to approve the emergency and temporary access authorizations prior to access being granted, and • Require documented supervisory approval from the ISSM each time a user requires emergency access abilities.	X		**Low**
CBP-IT-08-41	We noted that a Customs Directive was provided as separation procedures for contractors and the 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. Additionally, we noted that [redacted] contractor separation forms are not completed consistently for separating CBP contractors. Specifically, we noted that all forms for selected separated contractors were completed; however, 6 of the selected 25 separated contractors' forms were completed between one and several months after the individual separated from CBP.	• Review the current directive, document an up-to-date review of this document and make modifications as needed based on the new operating environment for CBP as part of the Department of Homeland Security, and • Require the consistent and accurate completion of the [redacted] forms for all separating contractors.	X		**Medium**
CBP-IT-08-43	We noted that the most recent business continuity plan testing was incomplete. Specifically, we noted that not all systems were brought online as required since sufficient hardware was unavailable at the recovery facility to fully and properly perform the continuity testing.	We recommend that CBP allocate the appropriate hardware to [redacted] to allow for the system availability to fully test the business continuity plan to ensure that [redacted] has the capability to support CBP in the event that the [redacted] is rendered unavailable for production.	X		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-44	We noted that non-disclosure agreements are not consistently signed by contractors at CBP.	We recommend that CBP enforce DHS' requirement that a non-disclosure agreement be signed by all contractors in a moderate and high risk level position to ensure that they are aware of their responsibilities in protecting the confidentiality of DHS and CBP data.	**X**		**Low**
CBP-IT-08-45	We noted that the parameters for the [redacted] are not configured to collect appropriate data. We further noted that 3 out of the [redacted] do not produce any data in the log.	We recommend that CBP properly configure [redacted] audit and [redacted] to capture appropriate data for the [redacted] system.	**X**		**Low**
CBP-IT-08-46	We noted that a total of 10 specific logs were not available for the following dates: November 12, 2007, February 22, 2008, and March 7, 2008. For November 12, 2007, logs were not available for [redacted] For February 22, 2008, logs were not available for the [redacted] For March 7, 2008, logs were not available for [redacted] We further noted that all mainframe audit and [redacted] that went digital after April 1, 2008 were available for review.	We recommend that CBP maintain [redacted] audit and [redacted] per DHS policy.	**X**		**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-47	We noted that CBP does not currently require individuals to sign rules of behavior prior to gaining access to [redacted].	We recommend that CBP require all CBP personnel (employees and contractors) sign rules of behavior prior to being granted any system access. Additionally, for personnel that already have systems access, CBP should prioritize having these individuals sign rules of behavior to maintain their systems access.	**X**		**Low**
CBP-IT-08-48	We noted the following weaknesses for the [redacted] procedures below: • Procedures do not define how often the [redacted] security audit logs are reviewed, • Procedures do not describe the documented evidence of review process, [redacted] Security Violation Log Report that is created by the [redacted] ISSO/Independent Reviewer, • Procedures do not define the sampling methodology that is used to select [redacted] daily security logs, and • Procedures were not effective for the entire FY 2008 (October 1, 2007 – September 30, 2008).	We recommend that CBP create detailed procedures that document the review process for [redacted] security audit logs that includes the documented evidence of review.	**X**		**Low**
CBP-IT-08-49	We noted that the initial password granted to new [redacted] accounts was not in compliance with DHS requirements.	We recommend that CBP update the [redacted] Security Administrator Handbook to require a strong password that is in compliance with DHS and CBP password policies to be set as the initial password for all new [redacted] accounts.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-50	CBP has no method of tracking completion of security awareness training for CBP employees and contractors. Individuals from the program team responsible for security awareness training do not have the ability to identify those individuals who have not completed security awareness training. Therefore, CBP can not ensure all personnel have completed this training.	We recommend that CBP develop a method for determining individuals who have and have not completed security awareness so that they can actively work towards 100% compliance with the DHS requirement that all individuals with systems access complete annual security awareness training.	**X**		**Low**
CBP-IT-08-51	We noted through inquiry with the [redacted] that documented hardware maintenance procedures do not exist.	We recommend that CBP document their [redacted] hardware maintenance procedures to ensure a consistent application of maintenance methodologies for the [redacted] environment.	**X**		**Low**
CBP-IT-08-52	We determined that the CBP workstation policy for screensavers is not appropriately implemented. Specifically, we noted that the configuration of a password-protected screensaver can be modified by the user, allowing that user to remove the password requirement and disable the screensaver completely.	We recommend that CBP determine a method for appropriately applying CBP and DHS policy requiring automatically-activated, password-protected screensavers after a period of inactivity.	**X**		**Low**
CBP-IT-08-53	The [redacted] Security Administrators Handbook is out of date and has inaccurate statements of CBP and DHS policies. Specifically, we noted: • Out-of-date references to US Customs Service, • References to out-of-date Customs (now CBP) policies and procedures (1400-05a), • Requirement that [redacted] initial passwords are set to a weak password string, and • Statement that [redacted] does not allow special characters in passwords.	We recommend that a full review of the [redacted] Security Administrators Handbook be performed and updates be made to the document to reflect the current operating environment. This review should be fully documented and the Handbook should be updated to include a change log as evidence of the updates made.	**X**		**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-08-54	We noted the following weaknesses in [redacted] access control procedures: • A regular (at least semi-annual) recertification of all [redacted] portal accounts is not performed, • Formal procedures are not documented for the creation of [redacted] portal accounts, and • [redacted] is not configured to disable accounts after 45 days of inactivity on the system.	We recommend that CBP document and implemented policies and procedures for [redacted] access control.	**X**		**Medium**
CBP-IT-08-55	We noted that 2 accounts created during FY 2008 did not have appropriate access authorization forms maintained by the Metro Area [redacted] administrators. We further noted that multiple administrators on the [redacted] had accounts created by other groups than the Metro Area [redacted] Support Team.	We recommend that CBP limit the organization that can create [redacted] accounts, administrator accounts and require any accounts be created by a single organization.	**X**		**Medium**

Department of Homeland Security
FY2008 Information Technology
Notification of Findings and Recommendations – Detail

- **United States Coast Guard**

Department of Homeland Security
FY2008 Information Technology
Notification of Findings and Recommendations - Detail
United States Coast Guard

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CG-IT-08-01	The [redacted] [redacted] has not been updated to reflect the results of testing the [redacted], and the Business Continuity Plans (BCPs) for each division have not been finalized.	Update the [redacted] as the result of its testing and finalize the applicable supporting BCPs.		**X**	**Low**
CG-IT-08-06	During the first half of the fiscal year, the contract with the [redacted] [redacted] software vendor was still in place, and no corrective action had taken place related to the prior year recommendation. Therefore, the risk exists that the condition was present for the majority of the fiscal year (October 1, 2008 through April 1, 2008). However, due to the Coast Guard decision to terminate the contract with their software vendor and the Coast Guard Headquarters decision to suspend all [redacted]) and [redacted] the condition did not exist beyond the date of these 2 events.	• Enhance existing Configuration Management/Change Management policies and procedures to explicitly address security configurations and software patches (e.g., those associated with system/application "builds", service packs, and maintenance releases) to better ensure compliance with DHS requirements and NIST guidance. • Communicate with and educate affected staff regarding these improved policies and procedures. • Develop, communicate, and implement procedures to periodically review system changes and system baselines.		**X**	**High**
CG-IT-08-07	We determined that [redacted] has not implemented the following password requirements: • Passwords shall contain special characters • Passwords shall not contain any dictionary word • Passwords shall not contain any proper noun or the name of any person, pet, child, or fictional character • Passwords shall not contain any employee serial	• Continue with the plans to upgrade the [redacted] operating system in order to enforce password complexity requirements to meet the DHS Sensitive System Policy Directive 4300A. • Continue to implement mitigating controls to reduce the risk of unauthorized individuals		**X**	**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	number, Social Security number, birth date, phone number, or any information that could be readily guessed about the creator of the password • Passwords shall not contain any simple pattern of letters or numbers, such as "qwerty" or "xyz123" • Passwords shall not be any word, noun, or name spelled backwards or appended with a single digit or with a two-digit "year" string, such as 98xyz123 • Passwords shall not be the same as the User ID While compensating controls were implemented to reduce the risk of unauthorized access, they unto themselves do not remove the potential risk from occurring.	gaining access to the system. • Educate all employees and contractors of the DHS Sensitive System Policy Directive 4300A password requirements so they can set their passwords in accordance with policy despite the systems inability to enforce them.			
CG-IT-08-10	Coast Guard Headquarters has developed but not yet implemented policies and procedures to require that a favorably adjudicated background investigation be completed for all contractor personnel.	Create and implement contractor background investigation policies and procedures in order to establish requirements and ensure compliance with the DHS Sensitive System Policy Directive 4300A. This includes the verification that all contracts issued by the Coast Guard include the appropriate Coast Guard position sensitivity designation requirements for contracted personnel.		X	High
CG-IT-08-14	Coast Guard headquarters has not finalized the Role-Based Training for USCG Information Assurance Professionals Commandant Instruction, which will require all Coast Guard members, employees, and contractors with significant IT security responsibilities to receive initial specialized training and annual refresher training thereafter. The online [redacted] ([redacted] which will track compliance, will not be implemented until the Role-Based Training is implemented.	• Continue efforts to finalize and implement the Role-Based Training for USCG Information Assurance Professionals Commandant Instruction which would require personnel with significant information security responsibilities to complete specialized role-based training on an annual basis. • Develop and deploy this specialized role-based training throughout the Coast Guard. • Implement the use of the [redacted] in order to		X	Medium

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		track and verify specialized role-based training requirements compliance.			
CG-IT-08-15	Until August 2008, configuration management weaknesses continue to exist on hosts supporting the [redacted] Database. Note: Due to the nature of this testing, see the tables in the NFR for the specific conditions.	Through our test work, we determined that the prior year control weakness has been remediated prior to the fiscal year-end; therefore, no recommendation is required for this NFR.		X	**Low**
CG-IT-08-17	Although [redacted] has made significant process in remediation, we were unable to verify that [redacted] is consistently remediating the vulnerabilities identified by the [redacted] scans in order to make it an effective mitigating control for the [redacted] application.	Continue to use the currently implemented mitigating controls for those DHS password requirements that cannot be enforced by the system. Specifically, [redacted] should continue to routinely use the [redacted] scanner and remediate any identified password weakness vulnerabilities.		X	**Low**
CG-IT-08-22	Until August 15, 2008 when corrective actions were successfully implemented, password rules had not been appropriately configured for the [redacted] application. We noted that: • [redacted] does not require passwords to be a minimum of eight characters • [redacted] does not require a combination of alphabetic, numeric, and special characters; • [redacted] does not restrict dictionary words; • [redacted] does not restrict simple pattern passwords; • [redacted] does not restrict dictionary words spelled backwards • [redacted] does not restrict the use of proper names • [redacted] does not restrict the use of the employee's user ID	Through our test work, we determined that the prior year control weaknesses was remediated prior to the fiscal year-end, therefore, no recommendation is required for this NFR.		X	**Medium**
CG-IT-	Policies and procedures have not been developed and	• Develop procedures for the periodic review of		X	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
08-23	implemented for the manual periodic review of [redacted] audit logs. As a result, [redacted] audit logs are not periodically reviewed.	the manual [redacted] audit logs in accordance with DHS policy. • Ensure that an entity independent of the personnel administering the [redacted] application reviews system audit trails on a regular basis as part of a more comprehensive continuous monitoring program. • Ensure audit log files are configured, retained, and archived in compliance with DHS policy.			
CG-IT-08-25	• Procedures have been created and implemented for the quarterly review of developer and analyst roles. However the procedures do not include the review of all other [redacted] user accounts to ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked, and that privileges associated with each individual are still authorized and necessary. • 529 users have unlocked [redacted] database accounts with access to the [redacted]e. Therefore, the number of users with the [redacted] role has increased by 141 users from the 388 users noted during FY 2007. Additionally, a mapping [redacted] roles within the [redacted] application to the tables that can be updated within the [redacted] database has not been created. Therefore, we are unable to perform an analysis of the [redacted] roles and the associated tables that are affected to determine whether access is appropriately restricted. • The password configurations for the [redacted] and [redacted] profiles will not be updated to be	• Develop and implement procedures to require a periodic review of all [redacted] accounts and their associated privileges. These 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. • Continue to reduce the number of tables that can be updated to ensure that each user has a business need to update each table. • Document a mapping between the [redacted] flow roles and the associated database tables that are affected. • Continue with plans to complete the [redacted] upgrade and configure the [redacted] password requirements to be in compliance with DHS guidance.		X	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	in compliance with DHS guidance until after the [redacted] [redacted] [redacted] upgrade. Since no improvements have been made in regards to the [redacted] password configuration, we determined that the password configurations continue to not meet the following DHS requirement of having a user password contain at least one special character.				
CG-IT-08-27	Progress was made during FY 2008, but weaknesses still exist. Specifically, we noted that: • [redacted] access request forms are documented and approved; • [redacted] user accounts are revalidated annually; and • [redacted] access is revoked in a timely manner for employees or contractors that have left Coast Guard or are re-assigned to other duties.	• Establish and enforce procedures to ensure [redacted] access request forms are documented, approved, and provided to [redacted] prior to establishing a [redacted] user account. • Continue to develop and implement policy and procedures for re-validating [redacted] user accounts in order to meet the requirements of the DHS Sensitive System Policy Directive 4300A. • Establish and enforce procedures to ensure [redacted] access is revoked for employees or contractors who leave the Coast Guard or are reassigned to other duties in order to meet the requirements of the DHS Sensitive System Policy Directive 4300A.		X	Medium
CG-IT-08-31	Coast Guard's controls over the scripting process remain ineffective. Weaknesses were noted in controls over script implementation, approvals and testing, as well as active script modification. In addition, Coast Guard has not maintained or developed a population of scripts run since the inception of [redacted] in 2003 nor has it performed a historical analysis of script impact on the cumulative	In order for management to assert to any financial statement line items, Coast Guard should: • Continue to design, document, implement, and demonstrate the effectiveness of internal controls associated with the active (current and future) scripts. • Identify and evaluate the historical scripts (all		X	High

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	balances in permanent accounts of the financial statements. Specifically: • Coast Guard lacks a formal process to distinguish between the module lead approvers for script approval requests; • The Procedures for [redacted] do not specifically state the testing and documentation requirements for blanket approval scripts and this policy remains in draft form; • Coast Guard does not monitor scripts run in the database through audit logging and has not developed a technical solution to monitor who accesses the database through [redacted] Navigator to run scripts or review what scripts are run; • The [redacted] does not consistently include all testing, approval, and implementation documentation for all scripts; and • Coast Guard has not completed [redacted] documentation for all scripts executed since their implementation.	those implemented prior to those identified in recommendation 1 above) to determine the financial statement impact on cumulative balances in permanent accounts; and develop and maintain supporting procedures related to each script. With respect to procedures already in place, Coast Guard should: • Continue to update script policies and procedures to include clear guidance over module lead approvers, testing and documentation requirements, monitoring/audit log reviews, and blanket approval requirements • Finalize and implement policies and procedures governing the script change control process including completing records within the [redacted] for <u>all</u> executed scripts and ensuring that all scripts are tested in an appropriate test environment prior to being put into production. Regarding the actual scripts themselves, Coast Guard should: • Determine the root causes and specific detailed actions necessary to correct the conditions that resulted in scripts, for the total population of scripts run at [redacted] in order to develop system upgrades that would eliminate the use of some of the scripts.			

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		● Continue efforts to complete an in-depth analysis of active scripts, with the following objectives: ○ All changes to active scripts and new scripts should be subject to an appropriate software change control process to include testing, reviews, and approvals. ○ All active scripts should be reviewed for impact on financial statement balances.			
CG-IT-08-32	Although Coast Guard Headquarters has mandated the use of [redacted] to maintain and track contracted personnel data, procedures surrounding this process have not been formally documented. As a result, we were unable to determine the effectiveness of the controls in place for contractor tracking.	● Finalize the procedure documentation and communicate/distribute the procedures ● Continuously monitor controls over [redacted] to verify that contractor data within the system remains current and accurate.		X	Medium
CG-IT-08-33	Coast Guard does not consistently notify system owners that individuals are terminating from the Coast Guard so that system accounts can be updated timely.	● Implement an automated process/system that will notify system owners of terminated contractor, military, and civilian personnel. ● Finalize and implement entity management policies and procedures for verifying that terminated user accounts have been successfully removed.		X	Medium
CG-IT-08-34	All [redacted] [redacted] are not being appropriately reviewed and approved by management prior to development/deployment. In addition, [redacted] developers and testers are not updating information in the [redacted] tool in a timely manner.	● Reconfigure the [redacted] tool to not allow the automatic approval of [redacted] [redacted] upon creation. ● Enforce established change control policies and procedures by reviewing and approving: a) all software change requests prior to developing the changes; b) test results; and c) all tested developed changes prior to		X	Medium

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		deploying the changes into the production environment. • Ensure that the [redacted] development and test staff adheres to the policies and procedures for updating software change control information within the [redacted] tool.			
CG-IT-08-35	We noted that control weaknesses still exist within the design of [redacted]s Configuration Management policies and procedures for [redacted] and [redacted] as well as the operating effectiveness of those controls. Our test work over the design of the change controls covered both periods of the change control environment; however, our testing of operating effectiveness covered only the period of start of the fiscal year through March 2008, since there were no changes made to [redacted] and [redacted] from April through the remainder of the fiscal year.	• [redacted]: develop, implement, communicate, and enforce procedures regarding how changes are to be controlled, documented, tracked, and reviewed as these changes progress through testing and into production. • Coast Guard Headquarters: develop, implement, communicate, and enforce procedures regarding how change control documentation will be maintained, reviewed, and validated in accordance with the DHS Sensitive System Policy Directive 4300A.		X	High
CG-IT-08-36	Configuration management weaknesses continue to exist on hosts supporting the [redacted] and [redacted] and the underlying [redacted] [redacted] [redacted] Note: Due to the nature of this testing, see the tables in the NFR for the specific conditions.	• Implement the corrective actions for the recommendations listed within the NFR. • Continue to implement polices and procedures to ensure that the tested and deployed software builds include required software patches and have current, correct, and compliant security configuration settings.		X	Medium
CG-IT-08-37	Security patch management weaknesses continue to exist on hosts supporting the [redacted] and [redacted] and [redacted] Note: Due to the nature of this testing, see the tables in the NFR for the specific conditions.	• Implement the corrective actions for the recommendations listed within the NFR. • Continue to implement polices and procedures to ensure that the tested and deployed software builds include required software patches and have current, correct, and compliant security		X	Medium

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		configuration settings.			
CG-IT-08-40	Although Coast Guard Headquarters is in the process of completing background investigations for all civilian employees, this has not been completed. Additionally, Coast Guard has set its position sensitivity designations to Low for the majority of its employees. However, DHS requires position sensitivity designations no less than Moderate which equates to [redacted]. Therefore, we determined that the conditions noted in prior year NFR CG-IT-07-40 have not been remediated.	• Perform initial background investigations and re-investigations for civilian employees in accordance with position sensitivity designations at no less than the Moderate level as required by DHS directives; and • Conduct civilian background re-investigations every ten (10) years, as required by DHS directives, to ensure that each employee has a favorably adjudicated and valid [redacted].		X	**Medium**
CG-IT-08-41	[redacted] has not completed the risk assessment for the [redacted] and the [redacted] is still in draft form.	Finalize and implement [redacted] Package for the [redacted] in accordance with DHS and NIST guidance.		X	**Low**
CG-IT-08-42	During prior financial statement audits dating back to FY 2003, we noted that implementation and oversight of the Coast Guard's information security policy and procedures was fragmented among the organizations responsible for operating various applications/systems. In FY 2008, significant improvements have been made in some areas, however, improvements are still warranted at the Coast Guard data centers/locations that operate and process key Coast Guard financial information. Improvements are needed especially in the areas of change control and to a lesser extent access to data and programs. These two key areas were the subject of significant findings identified and recommendations that were made during the audit. 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).	• Continue to implement, improve, and monitor compliance with DHS, Coast Guard, and Federal security policies and procedures in the areas of Change Controls • Continue to improve and monitor compliance with DHS, Coast Guard, and Federal security policies and procedures in the areas of: - Access Controls - Entity-wide Security Planning - Service Continuity - Segregation of Duties - System Software - Application Controls • Develop and implement corrective action plans to address and remediate the NFRs issued during the FY 2008 audit. These corrective action plans should be developed		X	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		from the perspective of the identified root cause of the weakness. In addition, the IT NFRs should not be assessed as individual issues to fix, but instead, should be assessed collectively based upon the area where the weakness was identified. This approach would enable a corrective action that would be more holistic in nature, thereby leading to a more efficient and effective process of fixing the controls that are not operating effectively.			
CG-IT-08-43	During our testwork over [redacted] access accounts, we noted that controls over user account authorizations were not operating effectively, and controls over user account reviews were not operating effectively.	• Implement and document the [redacted] user access review procedures to include all [redacted] access privileges and include supervisors in each review. • Update procedures to ensure that a documented and approved access authorization request is completed for each individual prior to granting him/her access to the [redacted] applications or databases.	X		**Medium**

Department of Homeland Security
FY2008 Information Technology
Notification of Findings and Recommendations - Detail

- **Federal Emergency Management Agency**

Department of Homeland Security
FY2008 Information Technology
Notification of Findings and Recommendations - Detail

Federal Emergency Management Agency

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-08-02	The [redacted] application database instance is [redacted] and the [redacted] application database instance is [redacted]. Specifically, servers were identified with password and auditing configuration weaknesses.	FEMA should implement the corrective actions listed in the NFR for each technical control weakness identified.		X	High
FEMA-IT-08-03	[redacted] accounts did not complete a new FEMA Form 20-24 in response to the recertification process	Ensure that the OCFO Procedures for Granting Access to [redacted] are consistently followed by continuing to perform and document a review of all [redacted] accounts in accordance with DHS policy, including supervisor verification of all access privileges granted through the submission of a new FEMA Form 20-24 by all federal employees and contractors.		X	High
FEMA-IT-08-06	We noted that FEMA has made a management decision not to develop policies and procedures over the modification of [redacted] account functions until the new [redacted] system upgrade occurs. We noted that FEMA has reported in the Plan of Action and Milestones that they expect to address corrective action for this weakness in FY 2010. As a result, a formalized process does not exist to guide [redacted] staff in the modification of the system to ensure that appropriate privileges are created,	We recommend that FEMA develop and implement policies and procedures documenting the process of adding, deleting, and modifying [redacted] system functions to ensure that the proper controls are in place for modifying user account privileges.		X	Low

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	documented, and approved for a specific function.				
FEMA-IT-08-12	FEMA informed us that the automated manager certification process has not yet begun. Therefore, the FY 2008 recertification has not been completed and the risk of unauthorized users accessing [redacted] was present for a majority of the fiscal year.	• Dedicate resources to complete the review of [redacted] user access for FY 2008 and conduct subsequent annual reviews of [redacted] user access by performing the management certification process in accordance with FEMA and DHS policies and procedures. • Fully implement the policies and procedures in place for the [redacted] recertification process and retain auditable records, in accordance with DHS Policy, that provide evidence that recertifications are conducted and completed periodically with timeliness.		X	**Medium**
FEMA-IT-08-13	We were informed that terminated [redacted] users are to have the "[redacted]" role applied to their account profile prior to being removed from the application, which overrides all existing roles and deactivates any existing privileges within the application although the individual can still log into the account. However, FEMA Instruction 2200.7 specifies that personnel separating from FEMA shall have all [redacted] access privileges cancelled and their user account removed. Consequently, although the risk is mitigated by the limited access rights on the accounts with the "[redacted] privilege, those six accounts demonstrate that the policies and procedures surrounding the [redacted] terminated user process are not consistently applied and the accounts have not been	Ensure that policies and procedures over removal of separated user access to [redacted] and [redacted] are consistently followed by removing accounts for any separated users immediately upon notification of separation according to FEMA, DHS and NIST guidance.		X	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	removed. Additionally, four (4) out of the ten (10) accounts remained on the [redacted] system with an active status.				
FEMA-IT-08-17	There is no documented evidence to support that monitoring of the “[redacted] directory and sub-directories is occurring.	We recommend that FEMA establish a process within existing procedures for retaining documented evidence that the “[redacted] directory and sub-directories are being monitored to verify that only authorized changes are implemented into production.		**X**	**Medium**
FEMA-IT-08-19	While FEMA informed us that system software activity is logged, we were unable to obtain evidence that the audit logs were reviewed on a periodic basis.	We recommend that FEMA’s process for monitoring sensitive access and suspicious activity on [redacted] system software include retention of evidence that audit records are proactively reviewed.		**X**	**Medium**
FEMA-IT-08-22	Per inspection of the POA&M, we noted that corrective action was initiated by FEMA to implement an alternate processing facility for [redacted] but that the alternate site has not been established. Due to the magnitude of the project scope, implementation of an alternate processing site will not be achieved within twelve (12) months. Consistent with DHS policy for corrective actions that cannot be implemented within twelve (12) months, a DHS IT Security Program Waiver (number WR-2008-012) was approved by the DHS [redacted] in March 2008 to provide FEMA with additional time to plan and develop an effective alternate processing site for	• Complete on-going efforts to fully establish and implement an alternate processing site for the [redacted] system according to the DHS Sensitive System Policy Directive 4300A. • Ensure that redundant servers are created at the alternate processing site for the [redacted] servers located at the [redacted] during implementation of the center as the alternate processing site. • Update the existing waiver, as required, in accordance with effective DHS policy regarding waivers and ensure that compensating controls described in the waiver		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	[redacted] Per DHS policy, the waiver must be reviewed, updated, and re-approved by the appropriate management officials every six (6) months. As required by DHS policy, the approved waiver describes the mitigating efforts, management's acceptance of the associated residual risk, and a plan for attaining compliance with DHS policy. The waiver also documents the compensating controls to mitigate risk until the alternate processing site is implemented. The compensating controls are to be derived by conducting annual table-top exercises and ensuring that regular backups of critical [redacted] data and offsite backup storage are performed. However, a fully successful table top test of [redacted] has not been conducted for FY 2008. The waiver granted provides an extension of time to implement corrective action, but the associated risk still remains.	are effective and documentation of their effectiveness is maintained as auditable records.			
FEMA-IT-08-23	[redacted] system administrators conducted ad hoc backup tape restores for system users and performed a full database restore in March 2008 during a server upgrade. However, there was no evidence that quarterly testing was conducted or that FEMA has a formalized process to test backup tapes more frequently than annually.	We recommend that FEMA develop and implement procedures to periodically test the [redacted] backups in accordance with the DHS Sensitive System Policy Directive 4300A.		**X**	**Low**
FEMA IT-08-	We noted that the tape restore schedule requires quarterly testing of backup tapes	We recommend that FEMA periodically test [redacted] backups on a quarterly basis in compliance		**X**	**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
24	beginning no earlier than FY 2009. Additionally, we determined that the [redacted] Contingency Plan was not tested and consequently a full [redacted] backup tape restore did not occur in FY 2008. Rather, [redacted] system administrators conducted ad hoc backup tape restores at the request of system users during the fiscal year.	with FEMA and DHS policy.			
FEMA-IT-08-25	Due to the magnitude of the project scope to establish a "real-time" alternate processing site for [redacted] FEMA was unable to implement corrective actions to fully remediate the prior year finding within twelve (12) months. Consistent with DHS policy for findings that cannot be remediated within twelve (12) months, a DHS IT Security Program Waiver (number WR-2008-012) was approved by the DHS Chief Information Security Officer in March 2008 to provide FEMA with additional time to plan and develop an effective alternate processing site for [redacted] Per DHS policy, the waiver must be reviewed, updated, and re-approved by the appropriate management officials every six (6) months. The waiver identifies that until the alternate processing site is implemented and full scale testing can be conducted, compensating controls will be implemented by conducting annual table-	• Continue to dedicate resources towards completing on-going corrective actions to implement a "real-time" alternate processing site for [redacted] • Update the existing waiver, as required, in accordance with effective DHS policy regarding waivers and ensure that compensating controls described in the waiver are effective and documentation of their effectiveness is maintained as auditable records. • In the event that an updated waiver is denied or when the alternate processing site is established, conduct documented annual tests of the [redacted] contingency plan that address all critical phases of the plan. • Update the [redacted] contingency plan based on the lessons learned from table top or full-scale		X	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	top exercises. Additionally, at the close of our audit test work, we determined that annual table top testing had not been conducted and documented. We determined that the most recently conducted table top review of [redacted] contingency plan occurred on July 21, 2007 and was conducted for processes, procedures, and scenarios identified in the contingency plan dated June 29, 2007. We noted that the documented results of the July 2007 test stated that FEMA was unable to successfully complete steps that were planned to be conducted during the Recovery Procedure Activation phase due to material weaknesses and deficiencies cited in the Recovery procedures.	testing results, as necessary.			
FEMA-IT-08-28	During our FY 2008 follow up test work, we tested a selection of 40 [redacted] non-emergency application level [redacted] that had occurred since October 1, 2007. Of the 40 [redacted] tested, we noted the following exceptions: • 29 [redacted] did not have testing documentation attached to the [redacted] • 36 [redacted] did not obtain Technical Development Laboratory (TDL) approval; and • 32 [redacted] did not obtain Technical Review Committee (TRC) approval	We recommend that FEMA, in accordance with DHS and FEMA policy, ensure that [redacted] non-emergency application level changes obtain all required approvals prior to implementation into production and that testing documentation is appropriately retained.		X	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-08-29	We noted that TRC approvals for [redacted] application level emergency changes did not consistently follow FEMA and DHS guidance. Specifically, we determined that of 25 emergency [redacted] changes selected for testing: • 22 changes did not have documented TRC approval; • 4 did not gain [redacted] approval prior to implementation into production; • 16 did not gain TDL approval; and • 6 did not have related testing documentation attached.	We recommend that FEMA, in accordance with DHS and FEMA policy, ensure that [redacted] application level emergency changes obtain all required approvals prior to implementation into production and that testing documentation is appropriately retained.		X	**Medium**
FEMA-IT-08-38	We were referred to Section 2.2.1 of the [redacted] [redacted] Administrative Manual as guidance on segregating incompatible duties. Based on our review of the manual, we noted that it does not include policies and procedures regarding segregating incompatible duties within [redacted]. Additionally, while we noted that system roles and responsibilities have been documented, [redacted] duties are incompatible are not documented. As a result, prior year NFR FEMA-IT-07-38 is re-issued.	We recommend that [redacted] document [redacted] duties that are incompatible and develop and implement policies and procedures for properly segregating incompatible duties within the system.		X	**Medium**
FEMA-IT-08-39	During our test work, we noted that a planned update and subsequent testing of the [redacted] Contingency Plan was not conducted and that system fail over capability at the alternate processing site had not been tested. Additionally, the NFIP	• Update and test the [redacted] Contingency Plan, covering all critical phases of the plan in accordance with DHS policy. In addition, NFIP should conduct a test of the system fail-over capability at the alternate processing site. • Revise the Disaster Recovery and Continuity		X	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Disaster Recovery and COOP was not updated to include the [redacted] [redacted] alternate processing facility or [redacted] critical data files and restoration priorities.	of Operation Plan to incorporate the [redacted] and [redacted] alternate processing facility and the [redacted] critical data files, as well as update the plans with lessons learned from the testing.			
FEMA-IT-08-45	[redacted] User Access is not Managed in Accordance with Account Management Procedures	• In support of the OCFO Procedures for Granting Access to [redacted] continue to ensure the process for granting or modifying access is monitored and that changes made to user profiles outside of the recertification process are documented and authorized by supervisors, program managers, and COTRs. • Ensure that the [redacted] Database User Access Instruction is implemented consistently by requiring that all existing and new [redacted] users complete a current [redacted] [redacted] User Access Form. • Complete the development and implementation of policies and procedures over periodic recertification of all user access to the [redacted] [redacted] database, and retain auditable records in accordance with DHS polices and procedures as evidence that recertifications are conducted and completed periodically with timeliness.	X		High
FEMA-IT-08-46	The existing MOU with the Department of Treasury expired in October 2007.	We recommend that FEMA complete the review, reauthorization, and re-issuance of a current [redacted] and [redacted] between the Treasury [redacted] and FEMA.	X		Low
FEMA-IT-08-47	Based upon our review, we determined that the [redacted] between FEMA and [redacted] expired in July 2007 and has not been reauthorized and reissued, as required by DHS policy.	Complete the reauthorization and reissuance of a renewed [redacted] between FEMA [redacted] and ensure that the [redacted] is subsequently reviewed, updated as necessary, and reissued timely, as required by DHS policy and/or the terms of the agreement.	X		Low

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-08-48	The vulnerabilities identified from the [redacted] scans are not reported and tracked via DHS' POA&M process.	We recommend that FEMA implement a process to ensure that weaknesses identified during vulnerability assessment scans of [redacted] are formally reported and that associated corrective actions are developed and tracked via DHS' POA&M process.	X		**Medium**
FEMA-IT-08-49	We noted that the software was improperly configured so that the user's ability to change the following settings had not been disabled: • [redacted] for automatically scanning system files for threats, known viruses, and worms on a continuous basis when Windows is started; • [redacted] for automatically scanning Outlook and/or Outlook Express messages for viruses. • [redacted] for automatically scanning incoming and outgoing Lotus Notes messages; and • [redacted] for scanning all incoming and outgoing e-mail messages other than Outlook and/or Outlook Express.	Action was taken to correct this weakness during the audit period. No further recommendation is required.	X		**Medium**
FEMA-IT-08-50	We performed test work over audit logging on the [redacted] application and Oracle database. Based upon inquiry and inspection of documentation, we determined that on a daily basis, an	We recommend that FEMA, in accordance with FEMA and DHS policy, continue to implement procedures over audit logging processes for the [redacted] application and database and retain evidence that audit records are proactively	X		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	automated report is generated and emailed to the Database Administrators (DBA) and FSS personnel for review. However, while this report is distributed for review by the DBAs and FSS staff, no evidence that the reviews are conducted is retained. Additionally, we noted that while FEMA Instruction 2200.7, [redacted] *User Access Instruction*, assigns the responsibility of conducting this weekly review to FSS, FEMA personnel do not formally document that the review is conducted.	reviewed. Specifically, the evidence should provide a record of review that at a minimum notes the identity of the individual that reviewed the log (e.g. initials), the date of review, and follow up actions taken, if required.			
FEMA-IT-08-51	We noted that the Standard Operating Procedure (SOP) does not comprehensively address requirements of FEMA Directive 140-1, FEMA Information Technology Security Policy. Specifically, the SOP does not require the monitoring of modifications to account tables and other highly-privileged and administrator-level activities. Additionally, we noted that the SOP requires database administrators to initial and retain printed logs as evidence that reviews are conducted as required. However, FEMA informed us that this portion of the SOP was not being performed.	We recommend that FEMA revise existing procedures for [redacted] audit logging to include a review of highly-privileged and administrator-level activities as required by FEMA and DHS policy and ensure implementation of all requirements, including retention of evidence of reviews of audit logs.	X		High
FEMA-IT-08-52	Finalization and implementation of the [redacted] SOP - FEMA [redacted]	We recommend that FEMA finalize and implement procedures that define the timeframe in which security patches should be installed.	X		Medium

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	[redacted] which specifies the timeframe for installing security patches, has been delayed due to organizational changes.				
FEMA-IT-08-53	Upon inspection of the [redacted] SSP that is a part of the [redacted] package; we noted that the server and host names listed in Appendix B of the SSP are not accurate. Specifically, the listing of system components is not comprehensive and portions of information, such as system owners, are not up to date.	We recommend that FEMA ensure that [redacted] SSP is updated in accordance with DHS policy so that current system components and system owners are comprehensively documented in the plan.	**X**		**Medium**
FEMA-IT-08-54	In FY 2008, we determined that NFIP had documented and implemented the [redacted]. During the audit, we determined that two (2) [redacted] changes had been implemented since October 1, 2007. We obtained change documentation for both changes and noted that testing documentation was not retained for these changes.	We recommend that NFIP ensure that testing documentation for [redacted] changes is documented and retained on file in accordance with DHS policy.	**X**		**Medium**
FEMA-IT-08-55	During our FY 2008 test work, we noted that NFIP documented and implemented the [redacted] Control Unit Procedures that provide guidance on implementing changes into the production environment. We selected for testing eight (8) [redacted] changes that had been implemented since October 1, 2007. Of the eight (8) tested, we identified that test results were not available for one (1) change.	We recommend that NFIP ensure that testing of all changes are documented and retained on file in accordance with DHS and NFIP requirements.	**X**		**Medium**

Department of Homeland Security
FY2008 Information Technology
Notification of Findings and Recommendations – Detail

- **Consolidated**

Department of Homeland Security
FY2008 Information Technology
Notification of Findings and Recommendations – Detail

Consolidated

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CONS-IT-08-07	Controls have not been implemented to detect and identify the actions taken with [redacted] [redacted] by non-database administration personnel Audit logs are only reviewed on an as needed basis by database administrators or personnel with database administrator access.	• Establish controls to detect and identify the actions taken with the [redacted] by non-database administration personnel. • Ensure that: ○ The [redacted] database supporting [redacted] is configured to capture all access attempts; ○ An individual independent of the personnel administering [redacted] is tasked with the responsibility for reviewing system audit trails on a regular basis. ○ The review of audit logs is documented to provide audit evidence of review. ○ The audit log files are retained and archived in accordance with DHS policy.		X	Medium
CONS-IT-08-11	We determined that Treasury has not sufficiently documented evidence of the completion of [redacted] application-level change management steps using the SCR process.	We recommend that the DHS OFM independently verify, on an ongoing basis, that Treasury performs adequate integration testing for all [redacted] changes and maintains documentation of testing as		X	Medium

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		audit evidence.			
CONS-IT-08-12	We noted that emergency changes procedures have been documented. However, we determined that OFM and Treasury did not properly document the necessary approvals and testing for one of six selected [redacted] changes.	• Maintain supporting documentation for each [redacted] change. At a minimum, the following documentation should be maintained for each change: change request, change request approval, evidence of testing, final approval. • Independently verify that Treasury is following the change control process as required and maintaining supporting documentation for each change.		**X**	**Low**

Department of Homeland Security
FY2008 Information Technology
Notification of Findings and Recommendations – Detail

- **OCIO**

Department of Homeland Security
FY2008 Information Technology
Notification of Findings and Recommendations – Detail

OCIO

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
OCIO-IT-08-01	There is no formal agreement in place between the DHS and the United States Navy (Navy) at [redacted] outlining DHS' and the Navy's responsibility for the services provided by the Navy at [redacted]	We recommend that the DHS OCIO ensure that DHS and the Navy document an Memorandum of Agreement/Memorandum of Understanding (MOA/MOU) outlining CBP's specific requirements for their business continuity facility and ensure that the agreement is complete, signed and up-to-date.	**X**		**Medium**
OCIO-IT-08-02	Through inquiry with OCIO personnel, we determined that the DHS [redacted] has not been finalized.	We recommend that the DHS OCIO finalize [redacted].	**X**		**Medium**

Department of Homeland Security
FY2008 Information Technology
Notification of Findings and Recommendations - Detail

- **Federal Law Enforcement and Training Center**

Department of Homeland Security
FY2008 Information Technology
Notification of Findings and Recommendations – Detail

Federal Law Enforcement and Training Center

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-08-01	FLETC finalized and approved the Financial Management System Configuration Management Standard Operating Procedures, which detail testing procedures. This prior year condition will be reissued as the weakness has been in place for the majority of the fiscal year. The access group, "[redacted]" has modify, read, execute, and write access to the [redacted] application program libraries. We determined that this gives all FLETC domain level users modify, read, execute, and write access to the [redacted] application program libraries.	We recommend that FLETC Ensure that access to the [redacted] program libraries is limited to only the Administrators group.		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-08-02	FLETC finalized and approved the Financial Management System Configuration Management Standard Operating Procedures, which detail testing procedures. This prior year condition will be reissued as the weakness has been in place for the majority of the fiscal year. Due to the decommissioning of the application, we learned that FLETC has not developed policies and procedures for [redacted] Desktop bug fixes and enhancements. This prior year condition will be reissued as the weakness has been in place for the majority of the fiscal year. All FLETC domain level users inappropriately have modify, read, execute, and write access to the [redacted]	- Continue with the projected plan for decommissioning the [redacted] application. Develop and implement policies and procedures over the configuration management process for Prism application level changes; - Ensure that access to the [redacted] program libraries is limited to only the Administrators group.		X	**Medium**
FLETC-IT-08-03	The installation of [redacted] system software is not currently logged or reviewed by FLETC management.	We recommend that FLETC, upon implementation of the [redacted] system, enable audit logging over the installation of [redacted] system software and ensure that logs are maintained and proactively reviewed by management.		X	**Medium**
FLETC-IT-08-04	The SDLC for [redacted] is currently in draft form.	1 Finalize and implement a SDLC methodology guide for [redacted], FLETC Directive and FLETC Manual. Ensure that security planning has been incorporated throughout the life cycle; 2 Ensure that the SDLC methodology is		X	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		promulgated to all personnel involved in the design, development, and implementation process of the SDLC methodology.			
FLETC-IT-08-05	We determined that FLETC has begun to implement corrective actions to address the prior year finding; however we learned that FLETC [redacted] server level and [redacted] database backups are not periodically tested. Additionally, we noted that procedures or a testing schedule are not in place for [redacted] level and [redacted] database backups.	Consistently apply the new CIO Backup SOP and periodically test the [redacted] server level and [redacted] database backups at least annually in compliance with the DHS Sensitive System Policy Directive 4300A.		X	**Medium**
FLETC-IT-08-06	The [redacted] contingency plan has not been fully tested. We determine that the recovery and resumption procedures were not tested during the table-top test of the [redacted] contingency plan.	• Perform corrective action over the [redacted] Contingency Plan test results and update the plan accordingly. • Perform a test over the [redacted] Contingency Plan, covering all critical phases of the plan, on an annual basis.		X	**Medium**
FLETC-IT-08-07	The FLETC Computer Security Operations Center and Computer Security Incident Response Capability SOP, is currently in draft form. Additionally, we noted that incidents are not tracked from inception to resolution in an incident response management system.	No recommendation will be offered as the condition was mitigated during the fiscal year		X	**Medium**
FLETC-IT-08-08	We noted that incompatible duties over [redacted] have been identified and that the [redacted] administrator is no longer a procurement approver. However, policies and procedures have not been developed to segregate incompatible duties.	Continue with the projected plan for decommissioning the [redacted] application.		X	**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-08-09	We determined that the procedures for granting access to the [redacted] had not been documented and no user authorization form is used and maintained for access requests. We noted that no documented procedures on re-entry into the facility after an emergency exist. FLETC also advised that all personnel on the [redacted] access listing and regular visitors to the [redacted] are provided fire suppression training. However, no supporting documentation was provided to support this effort.	• Document access procedures within the [redacted], including the use of a user authorization form; • Update the [redacted] to include access granting procedures as well as re-entry procedures, and; • Perform training for [redacted] staff and regular visitors over emergency procedures pertaining, but not limited to fire, water, and alarm procedures. Additionally, formalize this training by retaining documentation that all staff has completed the training.		X	Low

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-08-10	We found that FLETC Manual (FM) 4300: Information Technology System Security Program and Policy, which establishes the policies to be followed when an employee or contractor is separated or terminated, is currently in draft form. Additionally, [redacted] does not require passwords to contain a combination of upper and lower case letters and special characters.	• Continue with their projected plan for decommissioning the [redacted] application. Additionally, develop and implement procedures over access authorizations for [redacted]; • Develop and implement procedures to periodically review the list of [redacted] user accounts; • Finalized and implement FM 4300: Information Technology System Security Program and Policy, requiring the immediate notification of terminated or transferred users with FLETC IT accounts; • Ensure that the [redacted] application to requires a password to be a minimum of eight characters in length and contain a combination of alphabetic, numeric, and special characters to be in compliance with the DHS Sensitive System Policy Directive 4300A.		**X**	**Medium**
FLETC-IT-08-11	We determined that the FLETC Directive (FD) 4320: IT System Security Awareness and Training is in draft form.	No recommendation will be offered as the condition was mitigated during the fiscal year		**X**	**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-08-12	We determined that FLETC is in the process of refining the FD/FM 4300 to be in accordance with the DHS Sensitive System Policy Directive 4300A.	We recommend that FLETC finalize and update FD/FM 4300 based on the most recent version of the DHS Sensitive System Policy Directive 4300A and implement the policy, which provides policies and procedures over the authorization and use of mobile code technologies.		X	Low
FLETC-IT-08-13	We determined that FLETC has developed policies and procedures to proactively monitor sensitive access to system software utilities for [redacted] in the "FM 4300: Information Technology System Security Program and Policy." However, we noted that this policy is in draft form.	Finalize and implement "FM 4300: Information Technology System Security Program and Policy," which provides policies and procedures to proactively monitor sensitive access to system software utilities for [redacted].		X	Low
FLETC-IT-08-14	We determined that FLETC has developed policies for restricting access to [redacted] system software in the "FM 4300: Information Technology System Security Program and Policy." However, we noted that this policy is in draft form.	Finalize and implement "FM 4300: Information Technology System Security Program and Policy," which provides policies for restricting access to [redacted] system software;		X	Low
FLETC-IT-08-15	We noted that FLETC has developed policies for the segregation of duties in the, "FM 4300: Information Technology System Security Program and Policy." However, we noted that the policy is currently in draft form.	• Finalize and implement the "FM 4300: Information Technology System Security Program and Policy," which provides policies for segregation of duties in [redacted].		X	Low

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-08-16	We noted that FLETC has developed polices for the use of Voice Over Internet Protocol (VOIP) technologies, “FM 4300: Information Technology System Security Program and Policy.” However, we noted that the SOP is currently in draft form. Additionally, w learned that the security inspections have not been applied to all VoIP networks but is planned with the new [redacted] scheduled in 2008.	• Continue to finalize and implement the “FM 4300: Information Technology System Security Program and Policy,” which provides policies for the use of VoIP technologies; • Conduct a security inspection of the [redacted] VoIP installations by completing the FLETC VoIP Security Checklist.		X	**Medium**
FLETC-IT-08-17	During our FY 2008 review, we determined that the FLETC has established a process where background checks and periodic reinvestigations for on all new and existing contractors are performed in a timely manner and that supporting documentation be maintained. However, we noted a weakness in that two outstanding users still had access to the FLETC network. As a result, the FLETC responded immediately and removed both users’ access. However, since the risk was present the majority of the fiscal year, this NFR will be reissued without any recommendations	No recommendation will be offered since the condition was mitigated during the fiscal year.		X	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-08-18	We noted that FLETC has developed polices for the review of [redacted] audit logs, "FM 4300: Information Technology System Security Program and Policy." However, we noted that the SOP is currently in draft form. Additionally, we noted that FLETC has continued with the decommissioning of the [redacted] application; however it has not been completed.	• Finalize and implement "FM 4300: Information Technology System Security Program and Policy," which provides policies for the review of audit logs; • Continue with the decommissioning plan of the [redacted] application.		X	**Low**
FLETC-IT-08-20	In FY 2008, FLETC stated that no progress has been made on this weakness. FLETC management recommended setting policy to 5 minutes for all users and then to make exceptions as needed for trainers who need it. FLETC management has submitted an exception waiver to DHS to waiver from the DHS Sensitive System Policy Directive 4300A.	We recommend that FLETC configure the FLETC domain level inactivity threshold of the password protected screensaver to five (5) minutes to be in compliance with the DHS Sensitive System Policy Directive 4300A.		X	**Low**
FLETC-IT-08-21	In FY 2008, we noted that FLETC is in the process of finalizing and implementing FM 4300: Information Technology System Security Program and Policy. Therefore, since the recommendation has not been fully addressed, NFR FLETC-IT-07-21 will be re-issued.	We recommend that FLETC finalize and implement FM 4300: Information Technology System Security Program and Policy, and promulgate to all necessary users.		X	**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-08-22	FLETC has does not capture and maintain user access violations in [redacted] We determined that FLETC has established a process which requires that all [redacted] users will only be granted access once the user access form is appropriately completed and subsequently approved by a supervising authority. Since this improvement was not in place for the majority of the fiscal year, the associated weakness will be reissued with no recommendation. We also determined that FLETC has made progress over the usage of prior passwords. The new process follows the DHS standard of eight iterations. Since this improvement was not in place for the majority of the fiscal year, the associated weakness will be reissued with no recommendation.	Continue with the projected plan for decommissioning the [redacted] application.		**X**	**Low**
FLETC-IT-08-23	In FY 2008, we learned that FLETC has not validated all users for [redacted]. Additionally, FLETC has removed users that no longer have access, but, this process is not being performed consistently. Therefore, since the finding has not been fully addressed, the NFR will be re-issued.	• Perform a recertification of all [redacted] user access and validating the existing [redacted] user access of individuals who stated they still need [redacted] access; • Continue to consistently remove [redacted] user access that is no longer needed.		**X**	**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-08-24	FLETC provided the FLETC [redacted], dated June 18, 2008. However, the contingency plan did not contain evidence to support that the document is stored offsite.	We recommend that the FLETC ensure that several updated copies of the [redacted] Desktop Contingency Plan is located at the Artesia, NM site for use by contingency staff.		**X**	**Low**
FLETC-IT-08-25	During the FY 08 follow-up, we received the finalized SOP 4203 IT Systems Maintenance Management, effective as of April 29, 2008, and 4204 Anti-Virus for Servers, effective as of April 29, 2008. This NFR will be reissued with no recommendation since the condition has existed for the majority of the fiscal year.	As FLETC has effectively implemented the new policies effective April 2008, no recommendation will be offered.		**X**	**Low**
FLETC-IT-08-26	During technical testing, configuration management weaknesses were identified on hosts and databases supporting the [redacted]	• Implement the corrective actions noted in the findings. • Perform periodic scans of the FLETC network environment, including the financial processing environment, for the identification of vulnerabilities, in accordance with NIST Special Publication (SP) 800-42. • Implement corrective actions to mitigate the risks associated with any vulnerabilities identified during periodic scans.		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-08-27	During technical testing, patch management weaknesses were identified on hosts and databases supporting the [redacted]. The fact that these vendor supplied patches have not been applied in a timely manner could allow a remote attacker to gain unauthorized access on the host or database.	• Implement the corrective actions noted in the findings. • Perform periodic scans of the FLETC network environment, including the financial processing environment, for the identification of vulnerabilities, in accordance with NIST SP 800-42. • Implement corrective actions to mitigate the risks associated with any vulnerabilities identified during periodic scans.		**X**	**Medium**
FLETC-IT-08-29	In FY 2008, we learned that [redacted] is still in production; however, no backups are being tested. FLETC management stated that [redacted] decommissioning is planned for the first quarter of FY 08, however at the time of the audit, has not been completed.	Continue with the projected plan for decommissioning the [redacted]		**X**	**Medium**
FLETC-IT-08-30	During FY 2008 testing of controls after [redacted] conversion, we determined that four (4) support contractors and an additional user account used by the support contractor called [redacted] access privileges within [redacted]. Based on notification of this weakness, FLETC management responded by removing the access as of September 24, 2008. Therefore, this finding will be issued with no recommendation.	No recommendation will be offered since the weakness was remediated upon notification.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-08-31	During FY 2008, we noted that the [redacted] application will allow "3 unsuccessful attempts" before the user will be locked out of the application. The application will track these security violations into an audit log; however, the FLETC does not perform a periodic review of the log.	We recommend that application system administrators review security and system-related event logs on a periodic basis.	**X**		**Medium**
FLETC-IT-08-32	During FY 2008 testing of controls after [redacted]'s conversion, we determined that the segregation of duties controls were not effective. Specifically, we found that the [redacted]' role has the ability to create and approve payment vouchers within [redacted]	• Evaluate the access rights for all roles within [redacted] and separate the duties for the creation and payment of vouchers. • Develop a process to ensure the segregation of duties between the Accountant roles is maintained.	**X**		**Medium**

Department of Homeland Security
FY2008 Information Technology
Notification of Findings and Recommendations – Detail

- **Transportation Security Administration**

Department of Homeland Security
FY2008 Information Technology
Notification of Findings and Recommendations – Detail

Transportation Security Administration

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-08-01	The COOP has not been updated to reflect the results of testing and the division BCPs have not been finalized.	We recommend that TSA monitor [redacted] efforts to update the COOP as the result of its testing and finalize the applicable supporting BCPs.		**X**	**Low**
TSA-IT-08-03	During the first half of the year, the contract with the [redacted] and [redacted] software vendor was still in place and no corrective action taken had taken place related to the prior year recommendation. Therefore, the risk of the preexisting condition was present for the majority of the year (October 1, 2007 through April 1, 2008). However due to the Coast Guard decision to terminate the contract with their software vendor, and the Coast Guard Headquarters decision to suspend all SPRs and SCRs until the instructions are lifted this condition did not exist beyond the date of these two events.	We recommend that TSA work with the DHS Chief Information Officer to ensure that Coast Guard Headquarters completes, in a timely manner, the planned corrective actions of the following: • Coast Guard Headquarters enhance their existing Configuration Management/Change Management policies and procedures to explicitly address security configurations and software patches (e.g., those associated with system/application "builds", service packs, and maintenance releases) to better ensure compliance with DHS requirements and NIST guidance. • Coast Guard Headquarters and the applicable Coast Guard locations communicate with and educate affected staff regarding these improved policies and procedures. • Coast Guard Headquarters develop,		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		communicate, and implement procedures to periodically review system changes and system baselines.			
TSA-IT-08-05	Coast Guard Headquarters has developed but not yet implemented policies or procedures to require that a favorably adjudicated background investigation be completed for all contractor personnel.	We recommend that TSA work with the DHS Chief Information Officer to ensure that Coast Guard Headquarters completes, in a timely manner, the planned corrective actions to create and implement contractor background investigation policies and procedures in order to establish requirements and ensure compliance with the DHS Sensitive System Policy Directive 4300A. This includes the verification that all contracts issued by the Coast Guard include the appropriate Coast Guard position sensitivity designation requirements for contracted personnel.		**X**	**High**
TSA-IT-08-06	The Role-Based Training for USCG Information Assurance Professionals Commandant Instruction is still in draft form and has not been fully implemented.	We recommend that TSA monitor Coast Guard Headquarters' efforts to complete planned corrective actions to: • Continue efforts to finalize and implement the Role-Based Training for USCG Information Assurance Professionals Commandant Instruction which would require personnel with significant information security responsibilities to complete specialized role-based training on an annual basis. • Develop and deploy this specialized role-based training throughout the Coast Guard. • Implement the use of the [redacted] in order to track and verify specialized role-based training requirements compliance.		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-08-13	[redacted] is in the process of updating and finalizing the [redacted] Package for [redacted] Suite. The comprehensive [redacted] [redacted] will include the major subsystems [redacted] [redacted] [redacted] [redacted] and financial supporting applications [redacted] and will be used instead of an individual [redacted] for each system. The [redacted] also identifies the management controls around risk assessments, planning, security assessments, [redacted], and systems and services acquisition.	We recommend that TSA monitor that [redacted] is taking corrective action to finalize and implement the [redacted] Package for the [redacted] Suite in accordance with DHS and NIST guidance.		X	Low
TSA-IT-08-15	Of the 669 employees/contractors with current access to the following TSA's financial applications: [redacted] [redacted] [redacted] [redacted] 152 employees/contractors have not completed the IT Security Awareness Training	We recommend that TSA perform the following corrective actions: • Enforce mandatory completion of Security Awareness Training by holding groups responsible and accountable as a performance measure for monitoring the training of their employees. • Revoke system access of employees who do not complete the required annual security awareness training before the deadline and until the employees subsequently completes the required training.		X	Medium
TSA-IT-08-18	Configuration management weaknesses continue to exist on hosts supporting the [redacted] [redacted] and [redacted] applications and the [redacted] Note: See the tables in the NFR for the specific conditions.	We recommend that TSA work with the DHS Chief Information Officer to ensure that Coast Guard's [redacted] completes, in a timely manner, the planned corrective actions of the following: • Implement the corrective actions noted in the tables above. • Implement polices and procedures to ensure that the software builds created by CG are tested, prior to implementation, to ensure that all software security configurations, such as		X	Medium

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		[redacted], are up to date.			
TSA-IT-08-19	Patch management weaknesses continue to exist on hosts supporting the [redacted] applications and the [redacted] Note: See the tables in the NFR for the specific conditions.	We recommend that TSA work with the DHS Chief Information Officer to ensure that Coast Guard Headquarters' completes, in a timely manner, the planned corrective actions of the following: • Implement the corrective actions noted in the NFR. • Implement polices and procedures to ensure that the software builds created by CG are tested, prior to implementation, to ensure that all software security configurations, such as [redacted].		X	**Medium**
TSA-IT-08-20	We were unable to obtain 21 1163 Forms and 27 1402 Forms for each sample of 40. Additionally, 2 of the 13 1402 Forms received were signed after the forms were requested for audit. The IT Security Policy Handbook requires all TSA personnel including contractors to review and sign the TSA Form 1403: Computer Access Agreement. However, we were unable to obtain 7 of the 25, 1403: *Computer Access Agreements* sampled. Of the 18 forms we obtained, 5 were dated after the sample was requested for audit.	We recommend that TSA perform the following corrective actions: • Implement the Employee Exit Clearance Procedures by completing, certifying, and maintaining all forms required during the exit process for employees and contractors. • Implement the IT Security Policy Handbook by verifying that all TSA employees and contractors sign a computer access agreement prior to being granted system access.		X	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-08-21	The change control policy has not been fully completed and implemented. CG is responsible for making software changes to the [redacted], however, on March 31, 2008, CG HQ terminated its contract with the software vendor/developer for [redacted] which has hindered TSA's ability to fully complete and implement the [redacted] change control policy.	We recommend TSA continue to complete and implements the following sections of the [redacted] Change Control Policy: Build Selection Process, Software Development Process, and Software Testing Process.		**X**	**Medium**
TSA-IT-08-22	Control weaknesses still exist within the design of Coast Guard's Configuration Management policies and procedures for [redacted] as well as the operating effectiveness of those controls. Our test work over the design of the change controls covered both periods of the change control environment; however, our testing of operating effectiveness covered only the period of start of the fiscal year through March 2008, since there were no changes made to [redacted] from April through the remainder of the fiscal year.	We recommend that TSA work with the DHS Chief Information Officer to ensure that Coast Guard Headquarters' completes, in a timely manner, the planned corrective actions of the following: • The [redacted] develop, implement, communicate, and enforce procedures regarding how changes are to be controlled, documented, tracked, and reviewed as these changes progress through testing and into production. • Coast Guard Headquarters develop, implement, communicate, and enforce procedures regarding how change control documentation will be maintained, reviewed, and validated in accordance with the DHS Sensitive System Policy Directive 4300A.		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-08-23	Coast Guard's controls over the scripting process remain ineffective. Weaknesses were noted in controls over script implementation, approvals and testing, as well as active script modification. In addition, Coast Guard has not maintained or developed a population of scripts run since the inception of [redacted] in 2003 nor has it performed a historical analysis of script impact on the cumulative balances in permanent accounts of the financial statements. Specifically: • Coast Guard lacks a formal process to distinguish between the module lead approvers for script approval requests (Conditions #1 & #2); • The Procedures for [redacted] do not specifically state the testing and documentation requirements for blanket approval scripts and this policy remains in draft form (Conditions # 3 & #4); • Coast Guard does not monitor scripts run in the database through audit logging and has not developed a technical solution to monitor who accesses the database through [redacted] to run scripts or review what scripts are run (Conditions #5 & #6); • The [redacted] does not consistently include all testing, approval, and implementation documentation for all scripts (Condition #7); and • Coast Guard has not completed [redacted] documentation for all scripts executed since their implementation (Condition #8). Additionally, although Coast Guard did conduct an	TSA does not have the ability to take corrective actions to remediate these control issues on their own. Therefore it should be made clear that TSA is dependent on the Coast Guard to take the necessary action. In order for management to assert to any financial statement line items, we recommend that TSA work with the DHS Chief Financial Officer and the DHS Chief Information Officer to ensure that Coast Guard Headquarters' completes, in a timely manner, the planned corrective actions to: • Continue to design, document, implement, and demonstrate the effectiveness of internal controls associated with the active (current and future) scripts. • Identify and evaluate the historical scripts (all those implemented prior to those identified in recommendation 1 above) to determine the financial statement impact on cumulative balances in permanent accounts; and develop and maintain supporting procedures related to each script. With respect to procedures already in place, TSA should work with the DHS Chief Financial Officer and the DHS Chief Information Officer to ensure that Coast Guard Headquarters completes, in a timely manner, the corrective actions to: • Continue to update script policies and procedures to include clear guidance over module lead approvers, testing and documentation requirements, monitoring/audit log reviews, and blanket approval		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	examination with an external contractor organization, we have determined that the analysis was incomplete. Specifically, due to the many limitations over scope, it did not consider the full population of scripts run at [redacted], currently or since the inception of [redacted] Furthermore, the analysis did not properly evaluate scripts as to financial statement impact, including current versus prior year effect (Condition #9)	requirements. • Finalize and implement policies and procedures governing the script change control process including completing records within the [redacted], for <u>all</u> executed scripts and ensuring that all scripts are tested in an appropriate test environment prior to being put into production. Regarding the actual scripts themselves, TSA should work with the DHS Chief Financial Officer and the DHS Chief Information Officer to ensure that Coast Guard Headquarters completes, in a timely manner, the corrective actions to: • Determine the root causes and specific detailed actions necessary to correct the conditions that resulted in scripts, for the total population of scripts run at [redacted], in order to develop system upgrades that would eliminate the use of some of the scripts. • Continue efforts to complete an in-depth analysis of active scripts, with the following objectives: ○ All changes to active scripts and new scripts should be subject to an appropriate software change control process to include testing, reviews, and approvals. ○ All active scripts should be reviewed for impact on financial statement balances.			

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-08-24	Although Coast Guard Headquarters is in the process of completing background investigations for all civilian employees, this has not been completed. Additionally, Coast Guard has set its position sensitivity designations to Low for the majority of its employees. However, DHS requires position sensitivity designations no less than Moderate which equates to a [redacted].	We recommend that TSA work with the DHS Chief Information Officer to ensure that Coast Guard Headquarters' completes, in a timely manner, the following planned corrective actions: • Perform the initial background investigations and re-investigations for civilian employees in accordance with position sensitivity designations at no less than the Moderate level as required by DHS directives; and • Conduct civilian background re-investigations every ten (10) years, as required by DHS directives, to ensure that each employee has a favorably adjudicated and valid [redacted]		X	**Medium**
TSA-IT-08-26	Although procedures surrounding user access privilege re-certifications have been developed, we noted that the process does not include all [redacted] [redacted] and [redacted] users and does not involve users' supervisors as required by the DHS Sensitive System Policy Directive 4300A. Additionally, we noted that AAR forms are not being completed for all users on a consistent basis and we identified instances where system access was granted prior to the AAR approval by a supervisor.	We recommend that TSA work with the DHS Chief Information Officer to ensure that the Coast Guard's [redacted] completes, in a timely manner, the planned corrective actions to: • Implement and document the [redacted] user access review procedures to include all [redacted] access privileges and include supervisors in each review. • Update procedures to ensure that a documented and approved access authorization request is completed for each individual prior to granting him/her access to the [redacted] [redacted] [redacted] [redacted] applications or databases.	X		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-08-27	Although TSA has implemented quarterly access reviews for [redacted] user accounts and identified accounts with elevated privileges, TSA has not ensured that the [redacted] [redacted] accounts with an increased risk associated with them are reviewed/authorized on a periodic basis by a supervisor.	We recommend that TSA update the [redacted] and [redacted] Site Administrator User and Role Quarterly Review Process to include procedures surrounding the recertification of accounts with elevated privileges on the [redacted]. In addition, the recertification process should be documented, include supervisor written approval and occur on an at least annual basis.	**X**		**Medium**

Appendix C

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

Department of Homeland Security

Information Technology Management Letter

September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
CIS	CIS-IT-07-01	The NBC has not defined or documented the appropriate user permissions for the various roles granted to [redacted] [redacted]		**CIS-IT-08-01**
CIS	CIS-IT-07-02	NBC does not perform periodic [redacted] [redacted] user access reviews to ensure that users' level of access remains appropriate.		**CIS-IT-08-02**
CIS	CIS-IT-07-03	Management at the CIS HQ and the Service Centers [redacted] has not completed or inadequately completed access forms for [redacted] [redacted] [redacted] system users.		**CIS-IT-08-03**
CIS	CIS-IT-07-04	Access to the [redacted] [redacted] security software is not appropriately authorized and documented. Specifically, we noted there are 22 individuals with administrator access in [redacted]. However, CIS could not provide evidence that the access was limited and authorized.		**CIS-IT-08-04**
CIS	CIS-IT-07-05	We noted various matters which, when considered in aggregate with other DHS IT findings, indicate that ineffective general controls exist over financial management information systems at CIS. Specifically, these matters are highlighted in the related CIS information technology NFRs. See previously issued NFRs: CIS-IT-07-01 through CIS-IT-07-04.	**X**	
ICE	ICE-IT-07-01	From a sample of five users with multiple accounts (ten accounts), which were selected from throughout the year, [redacted] access request forms could not be provided for four accounts. However, all of these accounts for which the appropriate forms could not be provided were initiated in the period prior to a new policy being implemented. For those four accounts that were initiated after April 1, 2007, such access forms were appropriately completed.	**X**	
ICE	ICE-IT-07-02	There is excessive access to the [redacted] [redacted]. Currently, over 800 individuals have access to the computer room.	**X**	
ICE	ICE-IT-07-03	The following weaknesses in [redacted] access controls were identified: • [redacted] Access Request forms could not be provided for 14 of 60 user accounts. • [redacted] Update/Enter Profile Request forms could	**X**	

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		not be provided for 6 of 30 administrator accounts. • Procedures have not been documented for immediately removing [redacted] accounts upon termination or transfer. • Procedures have not been established for identifying and disabling [redacted] accounts after 30 days of inactivity.		
ICE	ICE-IT-07-04	The following weaknesses in [redacted] access controls were identified: • [redacted] Access Request Forms for 5 of 60 accounts were not provided, not completed, or not signed by the user's supervisor. • Evidence of account authorization could not be provided for seven of ten [redacted] administrator accounts. • Procedures have not been documented for immediately removing [redacted] user accounts upon termination or transfer. • Procedures for identifying and disabling [redacted] accounts after 30 days of inactivity are in draft format and have not been standardized across the ICE enterprise. • Procedures have not been established for periodically recertifying or reviewing privileged [redacted] accounts.		**ICE-IT-08-04**
ICE	ICE-IT-07-05	ICE does not perform periodic reviews of [redacted] audit logs.	**X**	
ICE	ICE-IT-07-06	ICE does not perform periodic reviews of [redacted] audit logs.	**X**	
ICE	ICE-IT-07-07	Evidence of approved emergency change requests are not maintained, which would support the validity and authorization of the changes.	**X**	
ICE	ICE-IT-07-08	We noted various matters which, when considered in aggregate with other DHS component findings, indicate that ineffective general controls exist over financial management information systems at ICE. Specifically, these matters are highlighted in the ICE information system related NFRs. See previously issued NFRs, ICE-IT-07-01 through ICE-IT-07-07.	**X**	
CBP	CBP-IT-	Due to the design of [redacted] certain controls can be	**X**	

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
	07-01	overridden without supervisory approval. For example, when a CBP entry specialist attempts to liquidate an import entry in [redacted] the system displays a warning message, indicating that a drawback claim had been filed against the import entry. However, entry specialists could override the warning message without supervisory review and process a refund without investigating pending drawback claims. The purpose of this warning message is to ensure that both a refund and drawback are not paid on the same goods. We also determined that entry specialists could override system edits designed to detect refunds exceeding the total duty, tax, and fees paid on an import entry. [redacted] does not currently generate override reports for supervisory review. In FY 2007, we noted that there has been little change in the status of this finding. CBP is developing a control override report which will record all control overrides that have taken place for a period of time. Management stated that the [redacted] will not be implemented in FY 2007. We concluded that a control mechanism to prevent overrides by specialists without supervisory approval would be an appropriate technical safeguard under application controls.		
CBP	CBP-IT-07-02	A full listing of trade partners was never compiled to assess the full scope of the status of connections to [redacted] We noted that a complete and accurate listing is still not maintained. Of those connections that have been accounted for, we noted that only 7% of identified legacy connections had an Interconnection Security Agreement (ISA) that has not expired. We noted that a [redacted] solution is being phased in and legacy connections are being phased out and that significant progress is being made to move all existing trade partners to the new [redacted] solution, in which they will obtain an ISA documenting the connection.		**CBP-IT-08-02**
CBP	CBP-IT-07-03	CBP does not maintain a centralized listing of contract personnel, including employment status. The only method CBP employs to track terminated contractors is the use of a report of users that had their mainframe accounts deleted. We cannot acknowledge this list as representative of all terminated contractors, since terminated contract personnel may not have mainframe access or their access was not removed after their termination.		**CBP-IT-08-03**
CBP	CBP-IT-	We confirmed that in FY 2007, backup tapes do not	X	

Department of Homeland Security

Information Technology Management Letter

September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
	07-04	have external labels affixed in order to indicate the sensitivity of the data contained in the tapes. Instead, containers in which the tapes are stored are labeled with media labels. Currently, CBP has obtained a waiver which waives the responsibility to label media directly. However, CBP remains non-compliant and the risk still remains.		
CBP	CBP-IT-07-05	We noted the following issues related to password parameters: • [redacted] minimum password length is set to six characters • Password complexity is not set on the [redacted] • [redacted] minimum password length is set to six characters • Password complexity is not set on the [redacted] [redacted]	**X**	
CBP	CBP-IT-07-06	We noted the following issues: • CBP's policy stated that sessions should automatically disconnect after 30 minutes of inactivity, which is not consistent with DHS policy. • CBP's policy stated that the workstation should log off from all connections after 5 minutes of inactivity. According to applicable guidance, all system connections do not have to be terminated after 5 minutes of inactivity on the workstation. • CBP workstations could not enforce the activation of a password-protected screensaver after five minutes of inactivity. The settings could be disabled or changed by individual users.	**X**	
CBP	CBP-IT-07-07	We determined that [redacted] does not have the ability to prevent developers from overwriting existing code in the development environment. The developer is able to extract the code from the development environment and place it into a personal folder on the user's personal computer. If multiple users are modifying a program in their own personal folders they may be overwriting existing changes.	**X**	
CBP	CBP-IT-07-08	A solution has not been implemented to maintain [redacted] audit logs for an appropriate period of time. Audit logs are not being reviewed for security violations for the [redacted]		**CBP-IT-08-08**
CBP	CBP-IT-	We noted that accounts are not deactivated		**CBP-IT-**

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
	07-09	automatically after 30 days of inactivity. Accounts are disabled for inactivity once a month using a manually initiated job.		**08-09**
CBP	CBP-IT-07-10	We reviewed the procedures and evidence of the most recent recertification performed for physical access to the data center. We noted the following: • Two people had access that was not appropriately documented with an approved access request form. • One terminated employee retained access after the recertification. • One user was marked to be removed as a result of the recertification but was not removed appropriately.	**X**	
CBP	CBP-IT-07-11	CBP System Security does not consistently retain audit logs of powerful mainframe system utilities. We reviewed the existence of [redacted] logs for a selection of dates and noted that logs were not available for a series of dates. We noted that within a 90 day window, complete logs were available for all selected dates except one. For the year long window, 17 summary reports were unavailable.	**X**	
CBP	CBP-IT-07-12	As identified in prior year issues reported in FY 2003, FY 2004, FY 2005 and FY 2006, we noted that improvements are still needed in CBP's Incident Handling and Response Capability which may potentially limit CBP's ability to respond to incidents in an appropriate manner. In FY 2007, we noted that [redacted] will not be installed on all workstations for the majority of the fiscal year.		**CBP-IT-08-12**
CBP	CBP-IT-07-13	During testwork around the application of security patches, we noted that a complete listing of workstations is not maintained [redacted]. We noted that [redacted] does not have the ability to quickly compile a listing of all workstations under CBP's ownership.		**CBP-IT-08-13**
CBP	CBP-IT-07-14	We noted that tape withdrawal requests are not documented.	**X**	
CBP	CBP-IT-07-15	We noted that the [redacted] is currently configured to disable accounts after 90 days of inactivity. We also noted that the job is configured to run weekly, which does not comply with the requirement for automatic disabling of accounts.	**X**	

Department of Homeland Security
Information Technology Management Letter
September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
CBP	CBP-IT-07-16	We noted that the [redacted] has been adjusted to limit active emergency access to 24 hours after the request. We noted however that the emergency table is still being used and that administrator or supervisory approval is not required each time emergency access is activated.		**CBP-IT-08-16**
CBP	CBP-IT-07-17	CBP [redacted] does not conduct reviews of powerful system utilities. Specifically, the utilities [redacted] are not reviewed by management. Additionally, while procedures are now in place for review of these logs, these procedures were not in place for the majority of the fiscal year.	**X**	
CBP	CBP-IT-07-18	We noted there are currently no procedures in place for the completion of semi-annual recertifications of [redacted] [redacted] accounts. We also note that a recertification of [redacted] [redacted] accounts is not performed on a semi-annual basis.		**08-18**
CBP	CBP-IT-07-19	We noted that the completion of security awareness training is not appropriately tracked at CBP. We noted that out of a selection of 45 CBP employees, one employee maintained access to [redacted] without having completed the refresher security awareness training course. The individual completed an awareness course that was not the CBP-wide security awareness training required for all CBP employees.	**X**	
CBP	CBP-IT-07-20	We noted several access control weaknesses for the [redacted] solution during testwork. Specifically, we noted: • The [redacted] sever does not maintain information on user account creation and inactivity and therefore cannot terminate inactive accounts or provide audit information regarding the creation of [redacted] accounts, • Accounts that did not recertify during the recertification time period or were marked for deletion during the recertification period remained active on the system after the accounts should have been deactivated by [redacted] administrators, • Procedures for recertifying accounts were not fully implemented and accounts were recertified by means beyond those identified in documented procedures	**X**	
CBP	CBP-IT-07-21	We noted that when changes to a user's access are performed in [redacted] [redacted], the log of these events is		**CBP-IT-08-21**

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		not regularly reviewed by personnel independent from those individuals that made the changes.		
CBP	CBP-IT-07-22	We noted that the following documents as not having documented approval and/or approval dates: • System Development Life Cycle (SDLC) Configuration Management Plan – No approval for majority of fiscal year • Configuration Management Code Migration Procedures for [redacted] – No approval or effective date • Configuration Management Code Migration Procedures for [redacted] – No approval date or effective date • Production Management Team Procedures – No approval, no change history • NDC Operations: Standard Operating Procedures – No approval	**X**	
CBP	CBP-IT-07-23	3 out of 5 selected [redacted] Emergency Changes did not have post implementation Executive Approval as required by the new OIT emergency change procedures.	**X**	
CBP	CBP-IT-07-24	The [redacted] re-certification process has several weaknesses. Of the 45 selected ports, 45 ports did not have formally documented communication between the responsible Director of Field Operations (DFO) and Office of Field Operations (OFO) HQ as directed by the FY 2006 memorandum put out by Office of Finance.	**X**	
CBP	CBP-IT-07-25	We noted that the [redacted] does not have an Information System Security Officer (ISSO), but has been assigned an interim ISSO. We noted that this interim ISSO is not formally documented as the [redacted] ISSO.	**X**	
CBP	CBP-IT-07-26	We noted that evidence of the review of mainframe security violation logs for 6 of 25 dates were not available for review.		**CBP-IT-08-26**
CBP	CBP-IT-07-27	We noted that authorizations are not being maintained for personnel that have administrator access to [redacted]		**CBP-IT-08-27**
CBP	CBP-IT-07-28	We noted that access policies and procedures have not been formally documented for the [redacted] [redacted] We also noted that access authorization forms were not		**CBP-IT-08-28**

Department of Homeland Security
Information Technology Management Letter
September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		completed for 27 out of 45 accounts created in FY 2007.		
CBP	CBP-IT-07-29	We noted that procedures have been developed and a new termination form (CF-241) has been developed for use in terminating employees. We note that while these procedures address the submission of the form to [redacted] and require notification of removal of system access from [redacted], the new procedures were developed and activated in June, 2007. The procedures are currently not implemented, however.		**CBP-IT-08-29**
CBP	CBP-IT-07-30	We noted that multiple terminated employees retained active accounts on the [redacted] They were disabled as a result of accounts being inactive for 90 days. Therefore, these accounts were active 90 days after the employee terminated from CBP.	**X**	
CBP	CBP-IT-07-31	We noted that 12 of the 45 selected ports/headquarters did not have self inspection worksheets completed. Accordingly, we were not able to determine whether specific [redacted] high risk combinations of roles were performed at these ports/headquarters.	**X**	
CBP	CBP-IT-07-32	We selected 20 out of 201 changes and noted the following: • 9 of the 20 changes did not have formal test plans or documented results • 20 of the 20 changes did not have evidence of review of the documented test results.	**X**	
CBP	CBP-IT-07-33	We selected 15 of 90 [redacted] changes and noted the following: • 3 of the 15 selected changes did not have formally documented test plans or test results. • 15 of the 15 changes did not have evidence of review of the test results documented.	**X**	
CBP	CBP-IT-07-34	We noted that virus protection is not installed on all CBP workstations. Specifically, we noted at the time of testing that approximately 6000 of CBP's approximate 38000 workstations do not have antivirus protection installed. Since the initial testing was performed, we noted that immediate remediation has begun and as of September 28, improvements have been made but 1,557 out of 42,429 workstations still are missing virus protection software.		**CBP-IT-08-34**
CBP	CBP-IT-	During our technical testing, eighteen configuration		**CBP-IT-**

Department of Homeland Security
Information Technology Management Letter
September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
	07-35	management exceptions were identified on [redacted] and hosts supporting the [redacted] application.		**08-35**
CBP	CBP-IT-07-36	During our technical testing, thirty-seven patch management exceptions were identified on [redacted] and hosts supporting the [redacted] application.		**CBP-IT-08-36**
CG	CG-IT-07-01	[redacted] has replaced the [redacted] concept with the development of a [redacted] which addresses disaster recovery, business continuity and continuity of government. However, [redacted] is in draft form and has not yet been tested and the [redacted] with the [redacted] for reciprocal services is still in draft form as well.		**CG-IT-08-01**
CG	CG-IT-07-02	The [redacted] change control policy does not detail requirements for requesting, testing, and approving changes. Furthermore, there are no formalized requirements pertaining to retention of supporting documentation and the roles and responsibilities of [redacted] personnel in the process. Additionally, the policy does not adequately reflect the [redacted] environment and change control process that was utilized during the [redacted] upgrade performed during FY07. Examples of inconsistencies include the references to service packs, data fixes, and the testing procedures completed.	**X**	
CG	CG-IT-07-03	The [redacted] system does not meet DHS password complexity requirements and the [redacted] system is not scheduled for decommissioning until December 2007.	**X**	
CG	CG-IT-07-04	There are 4 conditions present in this NFR, which were identified during our FY07 follow-up testwork associated with NFR CG-IT-06-013: • From October 1 2006 through July 24, 2007, PSC had not yet implemented policies and procedures for use in managing terminations, including the use of the Outgoing Personnel Form. • Outgoing Personnel Forms were not completed for one of five individuals selected for testing. • One terminated individual remained active within [redacted] until 90 days after his last logon before his account was revoked as part of the [redacted] account review process. • The account of a second terminated individual remains active within the system, although it has	**X**	

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		been configured to automatically log out the terminated individual if he attempts to login. Although this is a low risk issue, the existence of this account still presents a potential risk to the [redacted] data.		
CG	CG-IT-07-05	Policies and procedures regarding requesting, authorizing, testing, and approving operating system changes are not consistently followed. Additionally, a testing baseline standard has not been established to ensure that operating system changes have not adversely affected portions of the system that were not intended to be affected. Lastly, [redacted] was unable to reconcile changes to the operating system to a listing of authorized operating system changes to ensure that all changes have been appropriately approved.	**X**	
CG	CG-IT-07-06	The contract CG HQ has with the [redacted] software vendor does not include security configuration requirements that must be adhered to during the configuration management process. Consequently, [redacted] builds and maintenance packs may not be configured and implemented with comprehensive security configuration requirements. CG recognizes the absence of security requirements and indicated that the contract with the vendor will be reassessed in 2008 during the contract renewal process with CG HQ and corrective actions will be taken at that time.		**CG-IT-08-06**
CG	CG-IT-07-07	[redacted] has not implemented the following password requirements: • Passwords shall contain special characters • Passwords shall not contain any dictionary word • Passwords shall not contain any proper noun or name of any person, pet, child, or fictional character • Passwords shall not contain any employee serial number, social security number, birth date, phone number, or any information that could be readily guessed about the creator of the password • Passwords shall not contain any simple pattern of letters or numbers, such as qwerty or xyz123 • Passwords shall not be any word, noun, or name spelled backwards or appended with a single digit or with a two digit year string, such as 98xyz123		**CG-IT-08-07**

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		• Passwords shall not be the same as the User ID		
CG	CG-IT-07-08	Two generic accounts have access to [redacted] and [redacted]. Additionally, we determined that the [redacted] and [redacted] settings were not enabled. Furthermore, four accounts assigned to [redacted] personnel had both SPECIAL and [redacted], two of which were system programmers.	**X**	
CG	CG-IT-07-09	Every individual with access to the [redacted] data center has not completed the required emergency response training. Additionally, four employees were identified with 24 hour access to the data center that had not completed the training as of July 2007. Lastly, the security guards, with unrestricted access to the data center, have not yet been required to complete the training.	**X**	
CG	CG-IT-07-10	No formal procedures have been developed or implemented by CG HQ to address DHS requirements surrounding the suitability screening of contractors accessing DHS IT systems. DHS directives and policies require CG and other DHS components to ensure the completion of background investigations for all contractors accessing IT systems. The type of background investigation should be based on the risk level of the job position at CG and should be completed prior to the start of work. However, no CG guidance exists to require CG components to clear their contractors for suitability, especially those with sensitive IT positions.		**CG-IT-08-10**
CG	CG-IT-07-11	Session lockout times need to be changed from 40 to 20 minutes to meet DHS requirements.	**X**	
CG	CG-IT-07-12	The [redacted] Disaster Recovery Plan has not been tested and we were unable to obtain a finalized MOU between [redacted] and [redacted].	**X**	
CG	CG-IT-07-13	[redacted] is not consistently following the [redacted] for all [redacted] application changes. For four system change proposals and their associated sub-tasks, supporting documentation (i.e., evidence of testing, peer reviewer, approvals, evidence of joint application design meetings and business sponsor approvals) was not available.	**X**	
CG	CG-IT-07-14	Lack of criteria for defining personnel with significant IT responsibilities within the USCG IT Security Awareness, Training and Education Plan. Additionally, the personnel that are defined in the guidance are very limited and do not fully cover the scope of security responsibilities addressed in DHS		**CG-IT-08-14**

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		requirements.		
CG	CG-IT-07-15	The [redacted] application database [redacted] is using [redacted], which is no longer supported by the vendor. Additionally, an account on the [redacted] database has a password the same as account name (sccr_browse). The database also has a directory manipulation vulnerability in the binary file oracle.		**CG-IT-08-15**
CG	CG-IT-07-16	[redacted] has developed and implemented policies and procedures that address the review of inactive [redacted] accounts and lock those that have been inactive for 90 days. However, DHS guidance requires that inactive accounts be locked after 30 days.	X	
CG	CG-IT-07-17	[redacted] access control weakness were noted: • Passwords shall contain special characters • Passwords shall not contain any dictionary word • Passwords shall not contain any proper noun or name of any person, pet, child, or fictional character • Passwords shall not contain any employee serial number, social security number, birth date, phone number, or any information that could be readily guessed about the creator of the password • Passwords shall not contain any simple pattern of letters or numbers, such as qwerty or xyz123 • Passwords shall not be any word, noun, or name spelled backwards or appended with a single digit or with a two digit year string, such as 98xyz123		**CG-IT-08-17**
CG	CG-IT-07-18	[redacted] access control weaknesses were noted: • Passwords shall contain special characters • Passwords shall not contain any dictionary word • Passwords shall not contain any proper noun or name of any person, pet, child, or fictional character • Passwords shall not contain any employee serial number, social security number, birth date, phone number, or any information that could be readily guessed about the creator of the password • Passwords shall not contain any simple pattern of letters or numbers, such as qwerty or xyz123	X	

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		• Passwords shall not be any word, noun, or name spelled backwards or appended with a single digit or with a two digit year string, such as 98xyz123 • [redacted] accounts of terminated individuals are not removed in a timely manner including one individual who had user account management capabilities within the system. Additionally, [redacted] application and database accounts are not being reviewed for appropriateness.		
CG	CG-IT-07-19	[redacted] access control weaknesses were noted: • Documented access request forms could not be located for two new [redacted] users granted access to the application. • [redacted] accounts are not immediately disabled upon an employee's termination. • Procedures have not been developed to require periodic account reviews to be performed to ensure that all users and their associated privileges are appropriate. • [redacted] has not been configured to track and deactivate accounts that have not been used in 30 days. • An excessive number of individuals have user administrator capabilities within [redacted] until the implementation of the centralized user management (August 19, 2007). • Password configuration is not in compliance with DHS guidance.	**X**	
CG	CG-IT-07-20	The periodic review of [redacted] accounts only cover 1% of all user accounts with roles greater than [redacted] and that have been modified within the last 90 days. The population that is validated during this [redacted] system review was found to be insufficient as the user population of the system is approximately 60,000 user accounts.	**X**	
CG	CG-IT-07-21	The procedures for the periodic review of [redacted] user accounts does not require a review of all active user accounts and privileges to be performed and validated.	**X**	
CG	CG-IT-07-22	Password configuration weaknesses associated with the [redacted] application. Also, the [redacted] application is configured to terminate idle sessions after 30 minutes of inactivity instead of 20 minutes.		**CG-IT-08-22**

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
CG	CG-IT-07-23	While audit logging has been turned on for the [redacted] database, reviews of actions being taken on that database are still not being performed.		**CG-IT-08-23**
CG	CG-IT-07-24	Policies and procedures regarding [redacted] data used for the Coast Guard environmental liability report on the DHS Consolidated balance sheet have been developed but are currently in draft form and have not been implemented.	**X**	
CG	CG-IT-07-25	We noted the following [redacted] access control weaknesses: • Excessive access exists within the [redacted] database; • Password configurations for the [redacted] and [redacted] profiles have been configured to permit passwords to be a minimum of six characters in length. Additionally, the password history requirement is the only password requirement that has been configured for the [redacted] profile. • Audit logging has not been enabled within the [redacted] application or database. • Documented access request forms could not be located for nine out of 22 new [redacted] users granted access to the application. Additionally, although the automated access request forms for the other 13 out of 22 new [redacted] users granted access to the application were approved, the level of access/privileges associated with the new user were not documented on the access request form. • Individuals who are no longer employed with [redacted] were found to have active accounts within [redacted] • [redacted] account reviews have not been performed on a periodic basis.		**CG-IT-08-25**
CG	CG-IT-07-26	The [redacted] system has been configured to automatically end date accounts that have been inactive for six months. However, DHS requirements require accounts to be disabled after 30 days of inactivity.	**X**	
CG	CG-IT-07-27	Accounts within [redacted] that have been inactive for more than 90 days have not been disabled, access request authorization forms were unavailable for 19 of the 30 individuals who had accounts created during FY07, a recertification of [redacted] accounts is not performed, and terminated employees are not deactivated in a timely		**CG-IT-08-27**

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		manner.		
CG	CG-IT-07-28	From the sample selected, a developer had elevated production privileges in Also, two procedures/packages (were added to privileges.	**X**	
CG	CG-IT-07-29	The individual who enters an applicant's data into the also has the ability to hire the applicant in the system	**Transferred to Audit Team.**	
CG	CG-IT-07-30	functional change control policies and procedures did not reflect the change control process for the changes and did not adequately detail guidance for the change control process. Specifically, the policy does not include requirements for requesting, testing, and approving changes prior to implementing the functional change into the production environment.	**X**	
CG	CG-IT-07-31	Coast Guard has only eliminated a small number of the scripts used on a consistent basis and is projecting that this approach will continue into the delivery of 4.2 and beyond. Additionally, we noted that as of April 27, 2007, 240 scripts were run during a week long period. The number and type of scripts that are executed during any one period in time varies from week to week depending on the issues encountered. Of the 240 scripts noted during this particular week, several were run numerous times for the same software gap. Consequently, has not fully integrated the two change control processes or eliminated the need for the scripts.		**CG-IT-08-31**
CG	CG-IT-07-32	Coast Guard does not maintain a centralized listing of contracted personnel, including employment status, such as start date and termination date, so that system accounts can be timely updated.		**CG-IT-08-32**
CG	CG-IT-07-33	Coast Guard does not consistently notify system owners that individuals are terminating from the Coast Guard so that system accounts can be updated timely.		**CG-IT-08-33**
CG	CG-IT-07-34	is not consistently implementing policies and procedures regarding the change control process. Specifically, supporting documentation is not maintained for all changes and emergency changes. Additionally, changes may be approved prior to the change being tested and passing the test.		**CG-IT-08-34**
CG	CG-IT-07-35	Policies and procedures for the overall change control process surrounding changes and		**CG-IT-08-35**

Department of Homeland Security
Information Technology Management Letter
September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		emergency changes are inadequate. Specifically, the policies and procedures do not fully include guidance for the roles and responsibilities [redacted] possesses in the change control process. Additionally, they do not include detailed requirements and guidance on requesting changes, initial approvals, [redacted] testing, final approvals and documentation retention requirements for changes made to the system.		
CG	CG-IT-07-36	Configuration management weaknesses exist on hosts supporting the [redacted] applications and [redacted]		**CG-IT-08-36**
CG	CG-IT-07-37	Patch management weaknesses exist on hosts supporting the [redacted] applications and [redacted]		**CG-IT-08-37**
CG	CG-IT-07-38	[redacted] program changes are implemented in production prior to approval from the Financial Reports & Analysis (FF) Branch Chief or the Financial Control & Information (FC) Division Chief as required by [redacted] policy and procedures. Additionally, systems personnel move program changes into production without signing off on the Request Change to [redacted] Database form as required by the [redacted] procedures.	**X**	
CG	CG-IT-07-39	Coast Guard has not completed the process of filing the background investigation records that were recovered and recreating the records that were not found during the migration of records from the Department of Transportation to DHS.	**X**	
CG	CG-IT-07-40	Civilian background investigations and reinvestigations are not being performed in accordance with DHS Minimum Background Investigation standards per the DHS Sensitive System Policy Directive 4300A.		**CG-IT-08-40**
CG	CG-IT-07-41	Per review of the [redacted] package, we noted that system boundary definitions do not fully reflect the systems environment in which CG operates, [redacted] does not reflect system changes made in the [redacted] [redacted]de, and [redacted] is classified by CG as a subsystem of [redacted] however, there is no documentation within the [redacted] that defines [redacted] as a subsystem and addresses the appropriate security controls for [redacted] in this capacity according to NIST requirements for subsystems		**CG-IT-08-41**
CG	CG-IT-07-42	Coast Guard is not compliant with the FFMIA from an information technology perspective and in the		**CG-IT-08-42**

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		following areas: • Computer Security Act Requirements, including aspects of the Federal Information Security Management Act (FISMA) • System Documentation • Internal Controls • Training and User Support • System Maintenance • System Information Flow		
CONS	CONS-IT-07-01	The [redacted] application has not been configured to meet the following password requirements as defined by the DHS Sensitive System Policy Directive 4300A: • Contain special characters • Not be the same as the previous 8 passwords • Passwords shall not contain any proper noun or the name of any person, pet, child, or fictional character. Passwords shall not contain any employee serial number, Social Security number, birth date, phone number, or any information that could be readily guessed about the creator of the password • Passwords shall not contain any simple pattern of letters or numbers, such as "qwerty" or "xyz123" • Passwords shall not be any word, noun, or name spelled backwards or appended with a single digit or with a two-digit "year" string, such as 98xyz123 • Passwords shall not be the same as the UserID Additionally, the [redacted] password configuration does not meet the following service provider's password requirements as outlined in the [redacted] • Passwords must not contain dictionary words pertaining to personnel data (e.g. user's name, date of birth, address, telephone number, and social security number) • Passwords are not to be reused	**X**	

Department of Homeland Security

Information Technology Management Letter

September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		• Passwords must be composed of upper/lower case and special characters		
CONS	CONS-IT-07-02	DHS OFM has taken corrective action to address the Prior Year (PY) NFR and we noted that [redacted] Access Request Forms were appropriately completed for each new DHS user added to the system. However, in February 2007, a Treasury contractor, responsible for system development, created two user accounts within [redacted] to be used to test various functions in the new [redacted] release. These accounts were created without completing the [redacted] Access Request Form. Although we are unable to obtain evidence supporting the date the accounts were removed, we were able to confirm that the accounts had been removed by April 16, 2007.	**X**	
CONS	CONS-IT-07-03	DHS OFM has taken corrective action to address the PY NFR by removing all DHS OFM personnel from having access to the [redacted] role, which should be limited to one [redacted] developer only. However, DHS OFM did not take corrective action to address this NFR until August 2007, in which seven users with inappropriate access were removed. Although DHS OFM has addressed the recommendation in the prior year NFR CONS-IT-06-01, because the corrective action was not taken until 11 months into the fiscal year, we determined that the NFR will be reissued in 2007.	**X**	
CONS	CONS-IT-07-04	DHS OFM had taken corrective action to address the PY NFR. Specifically, 10 users had the [redacted] role in April 2007. However, in August 2007, DHS OFM reduced the number of individuals with this access to only one, the Assistant Branch Chief of the Financial Reporting Branch (FRB).	**X**	
CONS	CONS-IT-07-05	DHS OFM has taken corrective action to address the PY NFR in June 2007. Specifically, DHS OFM has developed and implemented procedures requiring DHS components to perform a formal review of [redacted] financial data, by a separate approving official, to the general ledger before moving it into the [redacted] repository. Additionally, the procedures require each DHS component to complete a CFO Certification Form for each [redacted] submission. The CFO Certification Form includes a sign-off from the component that the financial data review was performed. We inspected the CFO Certification Forms for each DHS component for June and July 2007 and	**X**	

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		noted no exceptions. We determined that DHS OFM has taken appropriate action to remediate prior year NFR CONS-IT-06-05. However, because corrective action was not taken to address the NFR until eight months into the fiscal year, the NFR will be reissued in FY 2007.		
CONS	CONS-IT-07-06	DHS OFM has taken partial corrective action to address the prior year NFR. Specifically, the [redacted] system has been configured to lock accounts that have not been logged into in 90 days; however, DHS guidance was revised and released during FY 2007 which requires systems be configured to disable user accounts after 30 days of inactivity. However, DHS OFM has applied for and received an exception to the 30 day requirement with the DHS Chief Information Security Officer (CISO) and has instead configured the system to lock accounts after 90 days of inactivity due to a business needs. The [redacted] assword configuration has not been configured to meet all of the password requirements as defined by the DHS Sensitive System Policy Directive 4300A. The [redacted] assword configuration does not meet the service provider's password requirements as outlined in the [redacted] or the Treasury Information Technology Security Program Handbook.	**X**	
CONS	CONS-IT-07-07	Treasury has not established individual accountability within the [redacted] database. Specifically, two [redacted] utilize one generic accoun [redacted], to perform maintenance on the [redacted] database that supports the [redacted] application. Additionally, these two [redacted] also share the following [redacted] accounts: [redacted], anc [redacted] [redacted] is the owner of the database and has access to the entire database while [redacted] and [redacted] are default system accounts that are used for various oracle system functions such as backups and configuration management and are required to operate and run batch jobs.		**CONS-IT-08-07**
CONS	CONS-IT-07-08	Not Used.		
CONS	CONS-IT-07-09	During FY 2007, we noted that access to the [redacted] module and the [redacted] group appears to be excessive. Specifically, up until the last week of FY 2007, six individuals had such access which allows them to perform account management capabilities within [redacted] (such as creating, deleting,	**X**	

Department of Homeland Security
Information Technology Management Letter
September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		and modifyin[redacted] [redacted] user accounts). Two of these six individuals were Treasury personnel who should not be able to modify user accounts belonging to DHS. Additionally, we inspected a log of all DHS [redacted] accounts created between October 1, 2006 and May 11, 2007 and noted that one DHS OFM personnel was responsible for creating the accounts. During the last week of FY 2007, one DHS OFM personnel and one Treasury contractor had their [redacted] module access revoked. However, we still determined access to be excessive as four individuals (three DHS OFM personnel and one Treasury contractor) still have access to the [redacted] module and the [redacted] group and the [redacted] only notes the [redacted] to be responsible for creating/modifying/deleting accounts within [redacted]		
CONS	CONS-IT-07-10	During our FY 2007 follow-up testing, we identified exceptions upon comparing the [redacted] Specifications Table and its congruency with the analytics guidance documented in the Component Guide.	**Transferred to Audit Team.**	
CONS	CONS-IT-07-11	DHS OFM has developed change control procedures that document DHS OFM's change management responsibilities. However, these procedures were not implemented until June 29, 2007. As a result: • Formal change requests were not available for our review for [redacted] changes implemented into production this fiscal year. • Documentation supporting five [redacted] changes selected for testing was not available for our review. Specifically, out of five changes selected for testing, we were missing the following documentation: • Evidence of Development, Testing and Production [redacted] were not available for four of five changes. • Evidence of DHS approval for five of five changes was not available for our review. • Evidence of Treasury testing was not available for one of five [redacted] selected for testing. • Two of five changes selected for testing were not approved by the Department of the Chief		**CONS-IT-08-11**

Department of Homeland Security
Information Technology Management Letter
September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		Financial Officer Team Lead, as required. • Four of five [redacted] selected for testing were missing the [redacted] [redacted] therefore, we were unable to determine that the individual responsible for development was not the same person who migrated the change to production. • The change management procedures documented in the DHS [redacted] [redacted] do not include procedures for notifying components of system changes so that they are aware of changes to the functionality of the system, etc. • The change management procedures documented in the DHS [redacted] do not include procedures for handing emergency changes to the system.		
CONS	CONS-IT-07-12	Weakness were identified surrounding the [redacted] change control process: • DHS OFM has developed change control procedures that document DHS OFM's change management responsibilities. However, these procedures were not implemented until June 29, 2007. As a result: • Formal change requests were not available for our review for [redacted] changes implemented into production this fiscal year. • The [redacted] change control process is informal. Therefore, the only documentation we received supporting the five changes selected for testing was e-mail documentation sent between DHS OFM and Treasury (requests for the change and notification that the change was complete). No evidence of approvals or testing was available for our review. • The change management procedures documented in the DHS OFM [redacted] do not include procedures for notifying components of system changes so that they are aware of changes to the functionality of the system, etc. • The change management procedures documented in the DHS OFM [redacted] do not include procedures for handing emergency		**CONS-IT-08-12**

Department of Homeland Security

Information Technology Management Letter

September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		changes to the system.		
FEMA	FEMA-IT-07-01	During our technical testing, patch management weaknesses were identified on [redacted] [redacted] and [redacted] systems.	X	
FEMA	FEMA-IT-07-02	During our technical testing, configuration management weaknesses were identified on [redacted] [redacted] [redacted] [redacted]		**FEMA-IT-08-02**
FEMA	FEMA-IT-07-03	We determined that the Financial Services Branch (FSB) has created procedures to review [redacted] user access on a semi-annual basis for appropriateness of access privileges granted to employees or contractors within their organization. Additionally, we noted that a recertification of all [redacted] users, which is also their semi-annual review of user access, began in June 2007. Currently, FSB is in the process of validating [redacted] access for users who responded to FSB's recertification request. In addition, FSB is locking out the [redacted] users who did not respond. We determined that the recertification of all existing [redacted] users has not been completed for FY 2007.		**FEMA-IT-08-03**
FEMA	FEMA-IT-07-04	The FEMA alternate processing site located in [redacted] [redacted] is not operational for [redacted] FEMA is in the process of setting up [redacted] to replicate data from the [redacted] production server at [redacted]. [redacted] and send it to the [redacted] servers in [redacted], [redacted]. Currently the [redacted] not complete and therefore, the [redacted] facility does not have the capability of functioning as the alternate processing site for [redacted] if a disaster were to occur.	X	
FEMA	FEMA-IT-07-05	The [redacted] Security Test & Evaluation (ST&E) did not provide adequate documentation of the results to the accrediting authority and that the prior year weakness still exists.	X	
FEMA	FEMA-IT-07-06	There is not formal, documented procedures are in place to require updates to the [redacted] system documentation as [redacted] functions are added, deleted, or modified.		**FEMA-IT-08-06**
FEMA	FEMA-IT-07-07	We determined that FEMA has identified the [redacted] [redacted] as the alternate processing facility for [redacted] [redacted]; however, it will not be fully operational until September 2007. Therefore, we determined that the [redacted] contingency plan has not undergone a full-scale test to show that the system can be brought back to an operational state at the designated alternate site.	X	

Department of Homeland Security

Information Technology Management Letter

September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
FEMA	FEMA-IT-07-08	We determined that the FEMA [redacted] has not been updated to include the new listing of FEMA mission critical IT systems as outlined in the Information Technology Services Directorate (ITSD) [redacted] Implementation Plan.	**X**	
FEMA	FEMA-IT-07-09	We noted that FEMA has begun to standardize all user workstations to [redacted] with [redacted] installed, which would ensure that all [redacted] settings are properly applied to all users. Currently, FEMA is upgrading older user workstations to [redacted] or providing users with new workstations. However, we noted that this process will not be fully complete until January 2008. This weakness impacts [redacted] We noted that FEMA users are locked out of the system at the domain level after three (3) consecutive failed login attempts; however, the user account becomes unlocked and active again after five (5) minutes of inactivity.	**X**	
FEMA	FEMA-IT-07-10	We determined that FEMA has begun to standardize all user workstations to [redacted] installed, which would ensure that all [redacted] settings are properly applied to all users. Currently, FEMA is upgrading older user workstations to [redacted] or providing users with new workstations. However, we noted that this process is not fully completed, and FEMA has estimated this process will not be completed until January 2008.	**X**	
FEMA	FEMA-IT-07-11	We noted that passwords for the [redacted] application can be re-used after six (6) iterations which is not in compliance with the DHS Sensitive System Policy Directive 4300A.	**X**	
FEMA	FEMA-IT-07-12	We determined that the FEMA Chief Information Officer (CIO) provided procedures to all Office Directors, Regional Directors and FEMA Coordinating Officers for the periodic review of all [redacted] accounts and position assignments on June 28, 2007. We noted that detailed procedures are listed for the review of [redacted] accounts; however, the procedures do not state the frequency of this review. We noted that this review began on June 29, 2007 with a deadline of July 26, 2007 for accepting responses from users recertifying their [redacted] accounts. Therefore, risk of unauthorized users accessing [redacted] was present for a majority of the fiscal year.		**FEMA-IT-08-12**

Department of Homeland Security
Information Technology Management Letter
September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
FEMA	FEMA-IT-07-13	We determined that the FSB has created procedures to review [redacted] user access on a semi-annual basis for appropriateness of access privileges granted to employees or contractors within their organization. Additionally, we noted that a recertification of all [redacted] users was performed in June 2007. Currently, [redacted] is in the process of validating [redacted] access for the users who responded to [redacted] recertification request and locking out the [redacted] users who did not respond. We determined that the recertification of all existing [redacted] users is not yet complete for FY 2007. We determined that the FEMA CIO provided procedures to all Office Directors, Regional Directors and FEMA Coordinating Officers for the periodic review of all [redacted] accounts and position assignments on June 28, 2007. However, the procedures do not state the frequency of this review. Furthermore, we noted that this review began on June 29, 2007 with a deadline of July 26, 2007 for accepting responses from users recertifying their [redacted] accounts. Therefore, the risk of unauthorized users accessing [redacted] was present for a majority of the fiscal year. We noted that twenty-seven (27) terminated or separated FEMA employees and contractors maintain active [redacted] user accounts. We noted that seven hundred seventy (770) terminated or separated FEMA employees and contractors maintain active [redacted] user accounts.		**FEMA-IT-08-13**
FEMA	FEMA-IT-07-14	We determined that IT Operations has created backup procedures entitled, Backup Media Protection and Control, for [redacted] and [redacted] dated July 27, 2007. However, we noted that the procedures were finalized on July 27, 2007, and that the risk was present for a majority of the fiscal year. We noted that both [redacted] [redacted] [redacted] backup tapes are not rotated off-site to the [redacted] [redacted] We noted that the FEMA alternate processing site located in [redacted] [redacted] is not operational for [redacted] We also noted that the [redacted] back-up facility has redundant servers in place for the [redacted] [redacted] Database in June 2007. Therefore, the risk was present for a majority of the fiscal year.	**X**	
FEMA	FEMA-IT-07-15	We determined that FEMA created the [redacted] Configuration Management Plan, Version 0.1, dated June 29, 2007. We noted that this plan was in draft	**X**	

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		form and that it does not fully identify the configuration management process of [redacted] We determined that FEMA created the Supplemental Security Policy to the DHS Sensitive System Policy Directive 4300A, which details policies for restricting access to the system software of FEMA IT systems. However, we noted that the draft policy is dated June 14, 2007. We noted that procedures over restricting access to [redacted] system software entitled, Database Administration Access Procedures and [redacted] patch management procedures were approved on June 29, 2007. However, we noted that the risk was present for a majority of the fiscal year, and as a result, the NFR will be re-issued for FY 2007.		
FEMA	FEMA-IT-07-16	FEMA created the Supplemental Security Policy to match the DHS Sensitive System Policy Directive 4300A, which details policies for restricting access to system software. However, we noted that the policy is in draft and dated June 14, 2007. FEMA has not documented procedures for restricting access to [redacted] system software.	**X**	
FEMA	FEMA-IT-07-17	We determined that FEMA created a System Change Request [redacted] for [redacted] However, the System Change Request [redacted] was approved by the OCFO on June 29, 2007. Furthermore, we noted the evidence that the [redacted] [redacted] account was locked within the [redacted] environment on July 24, 2007. Therefore, we noted that the risk was present for a majority of the fiscal year.		**FEMA-IT-08-17**
FEMA	FEMA-IT-07-18	FEMA created the Supplemental Security Policy to match the DHS Sensitive System Policy Directive 4300A detailed policies for investigating and reporting any suspicious activity detected when reviewing audit logs. However, we noted that the policy is dated June 14, 2007 and is in draft form. FEMA has not documented specific procedures to review suspicious system software activity and access controls for [redacted]	**X**	
FEMA	FEMA-IT-07-19	FEMA created the Supplemental Security Policy to match the DHS Sensitive System Policy Directive 4300A detailed policies for monitoring sensitive access and investigating and reporting any suspicious activity detected when reviewing audit logs. However, we noted that the policy is dated June 14, 2007 and is in		**FEMA-IT-08-19**

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		draft form. FEMA has not documented procedures to monitor and review sensitive access, system software utilities and suspicious system software and access activities for [redacted]		
FEMA	FEMA-IT-07-20	FEMA has adopted the DHS [redacted] for [redacted] This policy establishes required practices for managing DHS IT systems and infrastructure solutions through a progression of activities for initiation, planning, development, testing, implementation, operation, maintenance, and retirement. However, we noted that the policy is dated January 27, 2006 and is in draft form.	X	
FEMA	FEMA-IT-07-21	FEMA has adopted the DHS [redacted] for [redacted] This policy establishes required practices for managing DHS IT systems and infrastructure solutions through a progression of activities for initiation, planning, development, testing, implementation, operation, maintenance, and retirement. However, we noted that the policy is dated January 27, 2006 and is in draft form.	X	
FEMA	FEMA-IT-07-22	FEMA did not have an operational alternate processing site for [redacted] for a majority of the fiscal year. We determined that the alternate processing site in [redacted], [redacted] has redundant servers in place for the [redacted] effective as of June 2007.		**FEMA-IT-08-22**
FEMA	FEMA-IT-07-23	[redacted] lacks [redacted] backup testing procedures. Additionally, we determined that the [redacted] backups are not periodically tested.		**FEMA-IT-08-23**
FEMA	FEMA-IT-07-24	[redacted] lacks [redacted] backup testing procedures. Additionally, we determined that the [redacted] backups are not periodically tested.		**FEMA-IT-08-24**
FEMA	FEMA-IT-07-25	We noted that the [redacted] contingency plan has not been tested on an annual basis, per the DHS Sensitive System Policy Directive 4300A.		**FEMA-IT-08-25**
FEMA	FEMA-IT-07-26	During our review of user access rights for the approval of [redacted] system change requests, we noted that excessive access rights existed. Specifically, we determined that three (3) people were authorized to approve [redacted] system change requests, however, one (1) individual was transferred to another DHS agency. Therefore, this person's job responsibilities no longer required this access nor is this individual a current FEMA employee. Upon notification of this issue, FEMA took corrective	X	

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		action and removed the individual's access rights.		
FEMA	FEMA-IT-07-27	We noted that testing documentation for [redacted] application level changes are not consistently documented or performed timely.	X	
FEMA	FEMA-IT-07-28	Per the DHS Sensitive System Policy Directive 4300A, all changes to major applications must be formally approved, tested and documented prior to the change being implemented. For the test of this control we selected a sample of nine (9) [redacted] application level changes. We noted that one (1) out of the sample did not have testing performed.		**FEMA-IT-08-28**
FEMA	FEMA-IT-07-29	We noted that the [redacted] approvals for [redacted] application level emergency changes are not consistently documented. Specifically, we determined that five (5) out of a sample of eight (8) [redacted] application level emergency changes did not gain [redacted] approval.		**FEMA-IT-08-29**
FEMA	FEMA-IT-07-30	We determined that excessive access is designed to be permitted within [redacted] to make offline changes to the general ledger account tables via the [redacted] Group. We identified six (6) users in the [redacted] group that have the ability to make offline changes to the general ledger account tables, which are not within their job responsibilities.	X	
FEMA	FEMA-IT-07-31	[redacted] does not timeout after a period of inactivity. Additionally, we determined that all [redacted] workstations use a password protected screensaver after fifteen (15) minutes of inactivity, which is not in compliance with the DHS Sensitive System Policy Directive 4300A. [redacted] access is not reviewed on a periodic basis to determine if access is valid and commensurate with job responsibilities.	X	
FEMA	FEMA-IT-07-32	While a standard form has been developed for documenting [redacted] change requests, [redacted] change management procedures have not been documented. System software change management procedures have not been developed or implemented. Additionally, installation of the operating system upgrade in FY 2007 was not formally documented or approved.	X	
FEMA	FEMA-IT-07-33	[redacted] has made improvements in the area of Administrator account management. However, we	X	

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		noted that system activity logs are not being reviewed.		
FEMA	FEMA-IT-07-34	[redacted] has updated the [redacted] [redacted] baseline configuration document. However, we noted that procedures have not been developed which require approvals prior to implementation. Additionally, of 30 changes selected, 14 changes did not have documented Operations Service Request (OSR) forms or documented approvals.	**X**	
FEMA	FEMA-IT-07-35	A system programmer [redacted] had write access to the [redacted] and [redacted] datasets of the [redacted] production member. [redacted] removed the system programmer's access shortly after this finding was identified.	**X**	
FEMA	FEMA-IT-07-36	Access to the [redacted] excel files is excessive. Specifically, we identified that modify and write access permissions to the excel files are inappropriate for five individuals of the Bureau of Finance and Statistical Control group.	**X**	
FEMA	FEMA-IT-07-37	We noted there is excessive access to [redacted] application software and support files. Specifically, we noted that all individuals within the Bureau of Finance and Statistical Control group have modify and write access to the [redacted] application software and support files.	**X**	
FEMA	FEMA-IT-07-38	[redacted] has not documented incompatible duties within [redacted], developed policy and procedures regarding segregation of duties, or implemented segregation of duties controls within [redacted]. All users of [redacted] have full application level access.		**FEMA-IT-08-38**
FEMA	FEMA-IT-07-39	The [redacted] contingency plan has not been tested. As a result, the system fail-over capability for the [redacted] alternate processing site has not been tested. The [redacted] does not identify the following: • The [redacted] [redacted] alternate processing facility; and • [redacted] critical data files are not documented.		**FEMA-IT-08-39**
FEMA	FEMA-IT-07-40	The ROB forms are not consistently signed prior to users gaining access to the [redacted] Bureau [redacted] Specifically, we determined that three (3) out of a sample of twelve (12) new [redacted] Bureau [redacted] users did not sign the [redacted] prior to obtaining [redacted] Bureau [redacted] access.	**X**	

Department of Homeland Security
Information Technology Management Letter
September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
FEMA	FEMA-IT-07-41	We determined that policies and procedures over periodic review of [redacted] access lists have been documented. However, we noted that the periodic review determining if logical user access is valid and consistent with job responsibilities is not effective as an instance of excessive system developer access was identified within [redacted]	**X**	
FEMA	FEMA-IT-07-42	We determined that periodic review policies and procedures have not been developed for access to the [redacted] Bureau [redacted] [redacted] As a result, we noted that there are two (2) employees with excessive access to the [redacted] Bureau [redacted] room.	**X**	
FEMA	FEMA-IT-07-43	The [redacted] [redacted] [redacted] has been configured to permit users to reuse prior passwords after five (5) iterations which is not in compliance with the DHS Sensitive System Policy Directive 4300A.	**X**	
FEMA	FEMA-IT-07-44	We noted that proactive vulnerability scanning is not performed over [redacted] backend database or the [redacted] Bureau [redacted]	**X**	
FLETC	FLETC-IT-07-01	The Change Control and Configuration Management [redacted] for all preventative maintenance and patch management over [redacted] is currently in draft form. Additionally, the Change Control and Configuration Management [redacted] does not detail testing procedures. Documented policies and procedures for [redacted] bug fixes and enhancements do not exist, including a description for the emergency change process. The access group, "[redacted]" has modify, read, execute, and write access to the [redacted] application program libraries. We determined that this gives all FLETC domain level users modify, read, execute, and write access to the [redacted] application program libraries.		**FLETC-IT-08-01**
FLETC	FLETC-IT-07-02	The Change Control and Configuration Management [redacted] for all preventative maintenance and patch management over [redacted] is currently in draft form. Additionally, the Change Control and Configuration Management [redacted] does not detail testing procedures. Documented policies and procedures for [redacted] [redacted] bug fixes and enhancements do not exist, including a description for the emergency change process.		**FLETC-IT-08-02**

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		All FLETC domain level users inappropriately have modify, read, execute, and write access to the [redacted] support files.		
FLETC	FLETC-IT-07-03	The installation of [redacted] system software is not currently logged or reviewed by FLETC management.		**FLETC-IT-08-03**
FLETC	FLETC-IT-07-04	The SDLC for [redacted] is currently in draft form.		**FLETC-IT-08-04**
FLETC	FLETC-IT-07-05	[redacted] server level and [redacted] backups are not periodically tested. Procedures or a testing schedule are not in place for [redacted] server level and [redacted] database backups.		**FLETC-IT-08-05**
FLETC	FLETC-IT-07-06	The [redacted] contingency plan has not been fully tested. We determine that the recovery and resumption procedures were not tested during the table-top test of the [redacted] contingency plan.		**FLETC-IT-08-06**
FLETC	FLETC-IT-07-07	FLETC Computer Security Operations Center and Computer Security Incident Response Capability [redacted], is currently in draft form. We noted that incidents are not tracked from inception to resolution in an incident response management system.		**FLETC-IT-08-07**
FLETC	FLETC-IT-07-08	We noted that incompatible duties over [redacted] have not been identified nor have policies and procedures been developed to segregate incompatible duties.		**FLETC-IT-08-08**
FLETC	FLETC-IT-07-09	We determined that FLETC has documented procedures entitled, "[redacted] Access Standard Operating Procedures", which are currently in draft form. All personnel on the [redacted] access listing and regular visitors to the [redacted] will have fire suppression training provided. However, FLETC failed to provide the fire suppression training materials or a listing of individuals who attended the training.		**FLETC-IT-08-09**
FLETC	FLETC-IT-07-10	Procedures over access authorizations and the periodic review of user accounts for [redacted] do not exist. FLETC Manual (FM) 4300: Information Technology System Security Program and Policy establishes the policies to be followed when an employee or contractor is separated or terminated, which is currently in draft form.		**FLETC-IT-08-10**

Department of Homeland Security
Information Technology Management Letter
September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		We found that termination [redacted] for [redacted] and [redacted] are currently under development. [redacted] does not require passwords to contain a combination of upper and lower case letters and special characters.		
FLETC	FLETC-IT-07-11	We determined that the FLETC Directive (FD) 43220: IT System Security Awareness and Training is in draft form.		**FLETC-IT-08-11**
FLETC	FLETC-IT-07-12	We determined that FLETC has developed policies and procedures over the authorization and use of mobile code technologies in "FM 4300: Information Technology System Security Program and Policy." However, we noted that this policy is in draft form.		**FLETC-IT-08-12**
FLETC	FLETC-IT-07-13	We determined that FLETC has developed policies and procedures to proactively monitor sensitive access to system software utilities for [redacted] in the "FM 4300: Information Technology System Security Program and Policy." However, we noted that this policy is in draft form.		**FLETC-IT-08-13**
FLETC	FLETC-IT-07-14	We determined that FLETC has developed policies for restricting access to [redacted] system software in the "FM 4300: Information Technology System Security Program and Policy." However, we noted that this policy is in draft form. We noted that FLETC has developed procedures for restricting access to privileged and sensitive access including [redacted] system software in the [redacted], which is currently in draft form.		**FLETC-IT-08-14**
FLETC	FLETC-IT-07-15	We noted that FLETC has developed policies for the segregation of duties in the, "FM 4300: Information Technology System Security Program and Policy." However, we noted that the policy is currently in draft form. We noted that FLETC has developed procedures for the segregation of duties in the, "Logical Access Controls [redacted]", which is currently in draft form.		**FLETC-IT-08-15**
FLETC	FLETC-IT-07-16	We noted that FLETC has developed polices for the use of [redacted], "FM 4300: Information Technology System Security Program and Policy." However, we noted that the [redacted] is currently in draft form. The [redacted] hardening guide and [redacted] are currently in development and not finalized.		**FLETC-IT-08-16**

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		We determined that FLETC has not completed a security assessment of the [redacted] site's [redacted] installation.		
FLETC	FLETC-IT-07-17	We sampled thirty (30) IT contractors for evidence of background investigations and noted the following: • Nine (9) IT contractors did not have evidence that a background investigation was initiated or completed; and • For twelve (12) IT contractors, we were not able to validate if background investigations were initiated or adjudicated, due to a lack of documentation or poor documentation of background investigations initiated.		**FLETC-IT-08-17**
FLETC	FLETC-IT-07-18	We determined that FLETC has developed polices for the review of [redacted] audit logs in the, "FM 4300: Information Technology System Security Program and Policy." However, we noted that the policy is currently in draft form. Procedures around the detailed review of audit records do not exist. Audit logs are not maintained for [redacted] on an application level.		**FLETC-IT-08-18**
FLETC	FLETC-IT-07-19	We noted that [redacted] has been configured to permit users to reuse prior passwords after three (3) iterations which is not in compliance with the DHS Sensitive System Policy Directive 4300A. Upon notification of this issue, FLETC took corrective action and [redacted] is now configured to permit users to reuse prior passwords after eight (8) iterations.	**X**	
FLETC	FLETC-IT-07-20	We noted that the [redacted] is configured to trigger a domain level password protected screensaver after twenty (20) minutes of inactivity on user workstations, which is not in compliance with the DHS Sensitive System Policy Directive 4300A.		**FLETC-IT-08-20**
FLETC	FLETC-IT-07-21	We noted that FM 4300: Information Technology System Security Program and Policy documents policies for the following areas: • Use of cryptographic tools over the FLETC [redacted] • Use of wireless technologies; and • Data sharing with external parties outside of FLETC. However, we noted that the policy is currently in draft		**FLETC-IT-08-21**

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		form.		
FLETC	FLETC-IT-07-22	The following [redacted] access control weaknesses were identified: • User access violation information is not maintained on an application level; • All new users (a total of eight) requesting access to [redacted] failed to have an authorized access request form. • Password parameters have been configured to permit users to reuse prior passwords after six (6) iterations; and • The [redacted] Administrator is not informed of separated employees via Human Resources (HR), thus, terminated employees access is not removed in a timely manner. Upon notification of this issue, FLETC took corrective action and the [redacted] Administrator is now on the listing of individuals who are informed when an employee is separated.		**FLETC-IT-08-22**
FLETC	FLETC-IT-07-23	The following [redacted] access control weaknesses were identified: • Lack of documented procedures in to recertify users logical access on a yearly basis; and • Recertification of [redacted] users is not performed over all users.		**FLETC-IT-08-23**
FLETC	FLETC-IT-07-24	We noted that copies of the [redacted] Contingency Plan are not securely stored off-site at the alternate processing facility.		**FLETC-IT-07-24**
FLETC	FLETC-IT-07-25	The following [redacted] service continuity weaknesses were identified: • FLETC SOP - Anti-Virus Software for Servers is not finalized; and • FLETC SOP - System Maintenance Policy and Procedures is not finalized.		**FLETC-IT-08-25**
FLETC	FLETC-IT-07-26	During technical testing, configuration management weaknesses were identified on hosts and databases supporting the [redacted] and [redacted] applications.		**FLETC-IT-08-26**
FLETC	FLETC-IT-07-27	During technical testing, patch management weaknesses were identified on hosts and databases		**FLETC-IT-08-27**

Department of Homeland Security
Information Technology Management Letter
September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		supporting the [redacted] and [redacted] application. The fact that these vendor supplied patches have not been applied in a timely manner could allow a remote attacker to gain unauthorized access on the host or database.		
FLETC	FLETC-IT-07-28	We noted that [redacted] server backup tape rotation logs are not consistently maintained.	**X**	
FLETC	FLETC-IT-07-29	We noted that [redacted] server level and [redacted] database backups are not periodically tested. We noted that procedures or a testing schedule are not in place for [redacted] server level and [redacted] database backups.		**FLETC-IT-08-29**
TSA	TSA-IT-07-01	The disaster recovery aspect of the [redacted] will be completed by September 30, 2007 with the business continuity and continuity of government aspects of the [redacted] not being completed until December 2007. Because the [redacted] is in draft form, it has not yet been tested; however, [redacted] plans to test the entire [redacted] prior to it being implemented. Lastly, the [redacted] has drafted a memorandum of understanding (MOU) with the [redacted] [redacted] for reciprocal services; however, the MOU is currently in draft form.		**TSA-IT-08-01**
TSA	TSA-IT-07-02	[redacted] is in the process of developing of a Continuity of Operations Plan [redacted] which addresses disaster recovery, business continuity and continuity of government for [redacted] The disaster recovery aspect of the [redacted] will be completed by September 30, 2007 with the business continuity and continuity of government aspects of the [redacted] not being completed until December 2007. Because the [redacted] is in draft form, it has not yet been tested; however, [redacted] plans to test the entire [redacted] prior to it being implemented. Lastly, the [redacted] has drafted a MOU with the [redacted] for reciprocal services; however, the MOU is currently in draft form.	**X**	
TSA	TSA-IT-07-03	The contract that CG HQ has with the [redacted] [redacted] and [redacted] software vendor does not include security configuration requirements that must be adhered to during the configuration management process. Consequently, [redacted] [redacted] [redacted] builds and maintenance packs may not be configured and implemented with comprehensive security configuration requirements. CG recognizes the		**TSA-IT-08-03**

Department of Homeland Security
Information Technology Management Letter
September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		absence of security requirements and indicated that the contract with the vendor will be reassessed in 2008 during the contract renewal process with CG HQ and corrective actions will be taken at that time.		
TSA	TSA-IT-07-04	19 individuals, specified below, had 24 hour a day access to the data center and had not yet completed the training: 13 individuals (building owners, property managers and their respective contractors) 4 members of [redacted] Senior Management 2 security guards Lastly, we identified four employees, each with 24 hour access to the data center that had not yet completed the training as of July 2007. Upon notifying [redacted] of this exception, the four individuals completed the training and [redacted] provided supporting evidence.	**X**	
TSA	TSA-IT-07-05	No formal procedures have been developed or implemented by Coast Guard Headquarters to address DHS requirements surrounding the suitability screening of contractors accessing DHS IT systems. DHS directives and policies require Coast Guard and other DHS components to ensure the completion of background investigations for all contractors accessing IT systems. The type of background investigations should be based on the risk level of their future position at CG and are required to be completed prior to the start of work. However, no CG guidance exists to require CG components to clear their contractors for suitability, especially those with sensitive IT positions.		**TSA-IT-08-05**
TSA	TSA-IT-07-06	The IT Security Awareness, Training and Education Plan lacks appropriate criteria for defining personnel with significant IT responsibilities. Additionally, the personnel that are defined in the guidance are very limited and do not fully cover the scope of security responsibilities addressed in DHS requirements.		**TSA-IT-08-06**
TSA	TSA-IT-07-07	The following access control weakness surrounding [redacted] were identified: • TSA management did not receive a response from the Federal Air Marshalls Service FAMS Division [redacted] user base for the May and for the July 2007 [redacted] review. Therefore, TSA assumed that no response indicated that all roles were appropriate and did not follow-up to ensure that a	**X**	

Department of Homeland Security

Information Technology Management Letter

September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		response was received. • Privileges associated with each user were not included in the May and July 2007 reviews performed. We also noted that the accounts of terminated employees are not removed from the system in a timely manner. Although TSA requested that several of the accounts of terminated individuals be deactivated/end-dated by [redacted] the requests were not submitted to [redacted] until months after the employees departed and we were unable to obtain evidence that these accounts had in fact been deactivated/end-dated.		
TSA	TSA-IT-07-08	The following access control weakness surrounding [redacted] were identified: • The [redacted] application and database does not meet the password requirements noted in the DHS Sensitive System Policy Directive 4300A. • [redacted] accounts of terminated individuals are not removed in a timely manner including one individual who had user account management capabilities within the system. • [redacted] application and database accounts are not being reviewed for appropriateness.	**X**	
TSA	TSA-IT-07-09	The following access control weakness surrounding [redacted] were identified: • We were unable to obtain a copy of the [redacted] password configuration. However, we performed a demonstration/walkthrough of the password with a [redacted] point of contact and was able to determine that the password configuration is not in compliance with DHS guidance. • Although the [redacted] system has been configured to track and lock accounts that have not been utilized in 90 days, DHS guidance requires that accounts that have not been used in 30 days be deactivated.	**X**	
TSA	TSA-IT-07-10	An excessive number of individuals had user administration capabilities within [redacted] until the implementation of the centralized user management (August 19, 2007). We also noted the existence of two shared generic accounts with this privilege: [redacted]. These accounts have every privilege within the application,	**X**	

Department of Homeland Security

Information Technology Management Letter

September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		including the ability to create/delete/modify user accounts within [redacted]		
TSA	TSA-IT-07-11	[redacted] accounts are not immediately disabled upon an employee's termination. Additionally, formalized policies and procedures for the periodic review of the [redacted] accounts do not exist. Lastly, [redacted] access request forms are not consistently completed.	X	
TSA	TSA-IT-07-12	The accounts of terminated contractors are not end-dated or disabled in a timely manner. Additionally, we noted that TSA has not developed policies or procedures that require a periodic review of [redacted] application and database accounts, and their associated privileges, be performed to determine that access is appropriate.	X	
TSA	TSA-IT-07-13	Management had not adequately completed the [redacted] package to include the [redacted] system. Specifically, [redacted] management stated that [redacted] is a subsystem of [redacted] and a separate [redacted] does not need to be completed since it is covered by the [redacted] [redacted] Package. However, we determined that there is no documentation within the [redacted] [redacted] that defines [redacted] as a subsystem and specifically addresses the appropriate security controls for [redacted] in this capacity.		**TSA-IT-08-13**
TSA	TSA-IT-07-14	[redacted] and [redacted] systems have been configured to automatically end date accounts that have not been used in six months; however, DHS guidance requires accounts that have been inactive for 30 days be disabled.	X	
TSA	TSA-IT-07-15	The policies and procedures over a formalized sanctioning process have not been fully developed and implemented. Specifically, the policies and procedures do not include consequences for individuals who do not sign the computer access agreements or complete initial or refresher security awareness training. Furthermore, out of the nine individuals selected, only one had completed a Computer Access Agreement. Additionally, we determined that TSA allows individuals to complete security awareness training within sixty days of beginning work and gaining access to their [redacted] and application accounts. However DHS guidance requires that all individuals complete security awareness training prior to gaining access to the Information systems. Furthermore, out of the selection of nine individuals, one contractor had not completed initial security awareness training this		**TSA-IT-08-15**

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		fiscal year and a second employee had not completed their refresher training for this fiscal year.		
TSA	TSA-IT-07-16	Procedures are not formally documented requiring the review of the activities of the [redacted] administrators. We also noted that reviews of the audit logs that document the actions of [redacted] administrators in the [redacted] operating environment are not being performed.	**X**	
TSA	TSA-IT-07-17	Procedures are not formally documented identifying how change control should be performed when applying system software changes, including software patches, to the [redacted] operating system according to a standard schedule or in an emergency situation. While a policy exists, it lacks detailed procedures in order to be effective.	**X**	
TSA	TSA-IT-07-18	Configuration management weaknesses continue to exist on hosts supporting the [redacted] [redacted] and [redacted] applications and the [redacted]		**TSA-IT-08-18**
TSA	TSA-IT-07-19	Patch management weaknesses continue to exist on hosts supporting the [redacted] [redacted] and [redacted] applications and the [redacted]		**TSA-IT-08-19**
TSA	TSA-IT-07-20	Implementation of the formalized exit process for TSA personnel policies and procedures has not been fully executed. Specifically, only eleven (11) out of a selection of thirty (30) TSA 1402 Forms, the Separating Non-Screener Employee and Contractor IT Certificates, were received. Additionally, of the eleven received, seven (7) of the forms did not have the appropriate TSA application(s) identified in order to deactivate the separating employee's accounts. Furthermore, we selected thirty (30) TSA 1163 forms, the Employee Exit Clearance form, for both contractors and TSA personnel and only received nine (9) completed forms. The purpose of the 1163 form is to document sign-offs for access removal of financial and related administrative system accounts for applications such as [redacted] and [redacted] access to the [redacted].		**TSA-IT-08-20**
TSA	TSA-IT-07-21	The following weaknesses were identified in the [redacted] [redacted] [redacted] [redacted] change control process: • TSA has not fully documented policies and procedures surrounding the change control process for [redacted] to define the overlap in the responsibilities between [redacted] and [redacted] or guidance for ensuring that changes that are		**TSA-IT-08-21**

Department of Homeland Security
Information Technology Management Letter
September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		passed/deferred to [redacted] are tested and operate appropriately prior to approval by TSA and implementation into production. - Additionally, TSA does not consistently retain documentation associated with the [redacted] and [redacted] changes - Policies and procedures for the emergency change control process are not documented.		
TSA	TSA-IT-07-22	[redacted] has not fully developed and implemented their policies and procedures for the change control and emergency change control process to guide staff in the implementation of this process at [redacted] Specifically, we noted that the policies and procedures remain at a high-level and to do not include requirements for who is responsible for the initial approvals of the changes proposed by the vendor, including technical changes, the testing plan requirements for each phase of testing ([redacted] [redacted]) and the capacity in which [redacted] is involved, and the final approval of all changes to the system. Instead, the procedures detail the overall process and phases for [redacted] [redacted] and [redacted] change control, but lack detailed guidance for the roles and responsibilities executed by [redacted] personnel. Additionally, we noted that [redacted] follows the same change control process for emergency changes. However, the details surrounding that emergency change control process are not formally documented in the [redacted] procedures for [redacted] [redacted] and [redacted] For example, requirements for the categorization of priority levels and response time requirements for each priority level are not included. Furthermore, [redacted] has not fully implemented the procedures documented in the [redacted] [redacted] and [redacted] System Change Procedures. Specifically, we noted that [redacted] Checklists were not completed for changes made to the [redacted] suite as of June 2006. Upon review of a selection of changes, we determined that [redacted] is not consistently retaining documentation to support the change control and emergency change control process. Specifically, we inspected documentation associated with 30 [redacted] [redacted] and [redacted] system changes and emergency changes and determined that various pieces of supporting		**TSA-IT-08-22**

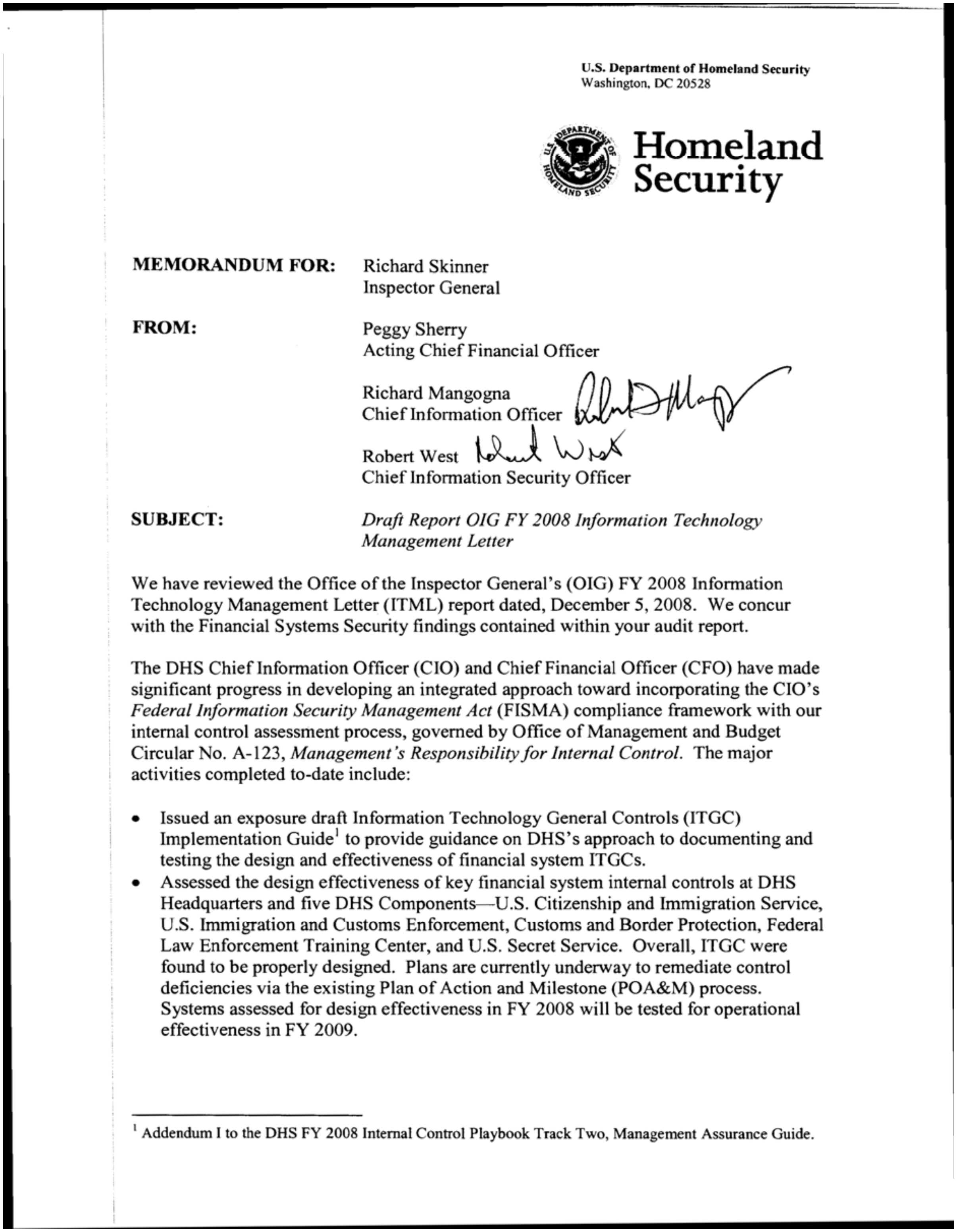
Department of Homeland Security
Information Technology Management Letter
September 30, 2008

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		documentation (i.e., functional resolution documents, test plans for the different phases of testing, evidence of testing, and approvals) were insufficient and/or not available for all 30 of the changes and emergency changes selected for testing.		
TSA	TSA-IT-07-23	Coast Guard change controls related to Coast Guard and TSA financial systems are not appropriately designed, operating effectively or in compliance with Office of Management and Budget (OMB) Circular No. A-130, Security of Federal Automated Information Resources, the DHS Sensitive System Policy Directive 4300A requirements and the National Institute of Standards and Technology Special Publications (NIST SP). Coast Guard has and continues to operate a separate, informal and largely undocumented change development and implementation process effecting Coast Guard and TSA Financial Systems, outside of and conflicting with the formal change control process. Coast Guard is unable to provide a complete population of implemented scripts, to include the type, purpose and intended effect on both CG and TSA financial data. The implemented process is ineffective as the approval, testing and documentation procedures of the script changes are not appropriately designed and the current process is ineffective to control the intended and actual effect on TSA financial data. Coast Guard has only eliminated a small number of the scripts used on a consistent basis and is projecting that this approach will continue into the delivery of [redacted] 4.2 and beyond.		**TSA-IT-08-23**
TSA	TSA-IT-07-24	Civilian background investigations and reinvestigations are not being performed in accordance with DHS guidance. Specifically, sixteen (16) out of twenty (20) individual background investigations reviewed did not meet the DHS minimum standard of investigation of an Minimum Background Investigation (MBI) per the DHS Sensitive System Policy Directive 4300A. Furthermore, upon review of a selection of five (5) civilian personnel, one (1) individual had an investigation that had not been adjudicated since 1988. DHS guidance requires that civilian personnel are reinvestigated every ten (10) years.		**TSA-IT-08-24**
TSA	TSA-IT-07-25	TSA has not taken corrective actions to develop and implement TSA specific change control policies and procedures for the TSA [redacted] change control or emergency change control process. Furthermore, upon	**X**	

			Disposition	
Component	**NFR #**	**Description**	**Closed**	**Repeat**
		review of a selection of changes, we determined that TSA is not consistently implementing the change control process. Specifically, we inspected documentation associated with seven system changes and emergency changes and determined that supporting documentation (i.e., test plans, evidence of testing, and approvals to move the change into production) were not available for all seven of the changes and emergency changes selected for testing. Additionally, we noted that testing was not fully completed by TSA prior to passing the change for testing for three of the changes.		

Appendix D

Management Comments



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

Homeland
Security

MEMORANDUM FOR: Richard Skinner
Inspector General

FROM: Peggy Sherry
Acting Chief Financial Officer

Richard Mangogna
Chief Information Officer

Robert West
Chief Information Security Officer

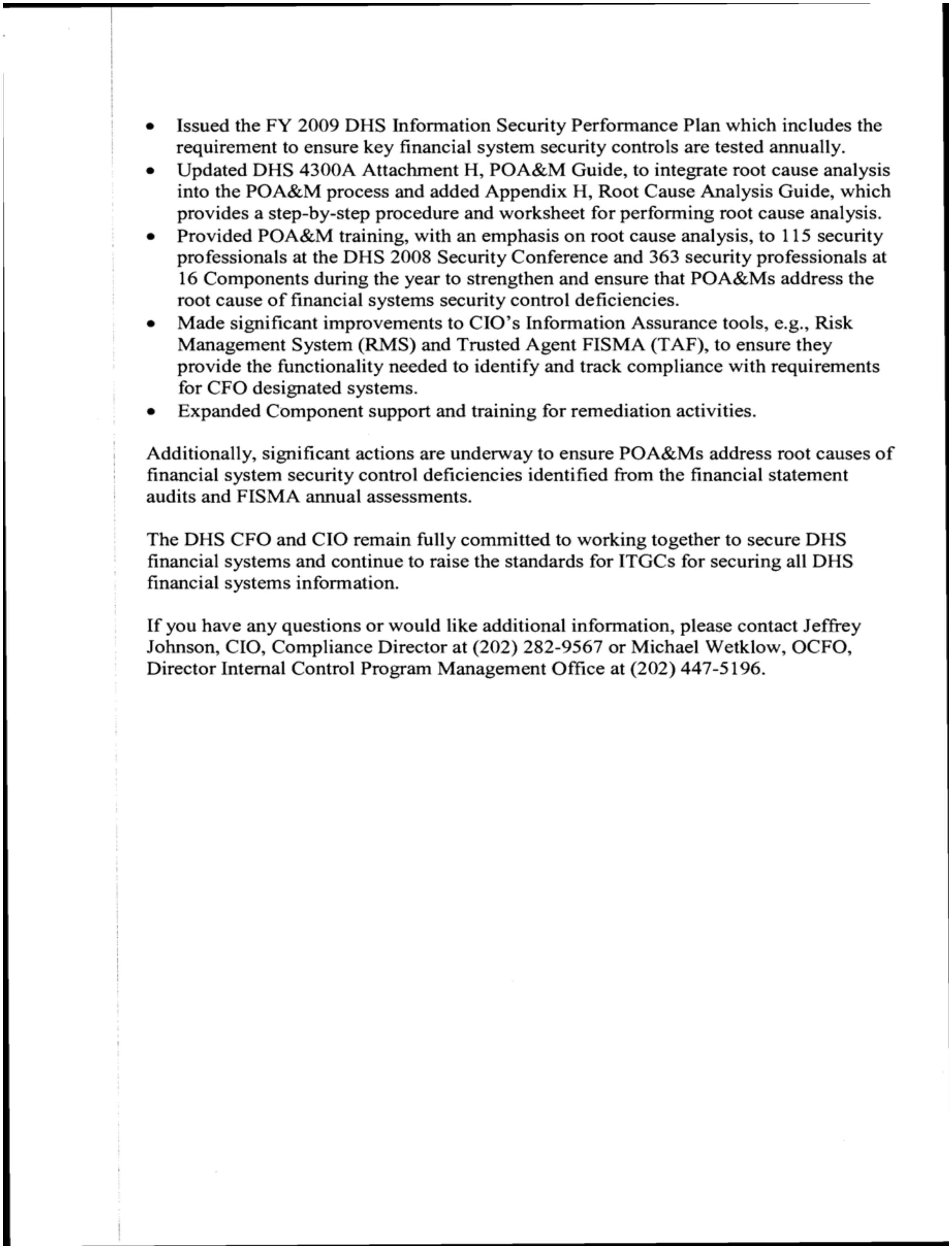
SUBJECT: *Draft Report OIG FY 2008 Information Technology Management Letter*

We have reviewed the Office of the Inspector General's (OIG) FY 2008 Information Technology Management Letter (ITML) report dated, December 5, 2008. 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 made significant progress in developing an integrated approach toward incorporating the CIO's *Federal Information Security Management Act* (FISMA) compliance framework with our internal control assessment process, governed by Office of Management and Budget Circular No. A-123, *Management's Responsibility for Internal Control*. The major activities completed to-date include:

- Issued an exposure draft Information Technology General Controls (ITGC) Implementation Guide[1] to provide guidance on DHS's approach to documenting and testing the design and effectiveness of financial system ITGCs.
- Assessed the design effectiveness of key financial system internal controls at DHS Headquarters and five DHS Components—U.S. Citizenship and Immigration Service, U.S. Immigration and Customs Enforcement, Customs and Border Protection, Federal Law Enforcement Training Center, and U.S. Secret Service. Overall, ITGC were found to be properly designed. Plans are currently underway to remediate control deficiencies via the existing Plan of Action and Milestone (POA&M) process. Systems assessed for design effectiveness in FY 2008 will be tested for operational effectiveness in FY 2009.

[1] Addendum I to the DHS FY 2008 Internal Control Playbook Track Two, Management Assurance Guide.



- Issued the FY 2009 DHS Information Security Performance Plan which includes the requirement to ensure key financial system security controls are tested annually.
- Updated DHS 4300A Attachment H, POA&M Guide, to integrate root cause analysis into the POA&M process and added Appendix H, Root Cause Analysis Guide, which provides a step-by-step procedure and worksheet for performing root cause analysis.
- Provided POA&M training, with an emphasis on root cause analysis, to 115 security professionals at the DHS 2008 Security Conference and 363 security professionals at 16 Components during the year to strengthen and ensure that POA&Ms address the root cause of financial systems security control deficiencies.
- Made significant improvements to CIO's Information Assurance tools, e.g., Risk Management System (RMS) and Trusted Agent FISMA (TAF), to ensure they provide the functionality needed to identify and track compliance with requirements for CFO designated systems.
- Expanded Component support and training for remediation activities.

Additionally, significant actions are underway 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 CFO and CIO 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 Jeffrey Johnson, CIO, Compliance Director at (202) 282-9567 or Michael Wetklow, OCFO, Director Internal Control Program Management Office at (202) 447-5196.

Report Distribution

Department of Homeland Security

Secretary
Acting Deputy Secretary
Chief of Staff for Operations
Chief of Staff for Policy
Acting General Counsel
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) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;

- Fax the complaint directly to us at (202) 254-4292;

- Email us at DHSOIGHOTLINE@dhs.gov; or

- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigations - Hotline,
  245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

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