DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Information Technology Management Letter for the FY 2007 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-08-77 June 2008

Office of Inspector General

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

Homeland Security

June 27, 2008

Preface

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

This report presents the information technology (IT) management letter for the DHS financial statement audit as of September 30, 2007. 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-08-12, November 2007) and represents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit of DHS's FY 2007 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated December 14, 2007, and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control or conclusion on compliance with laws and regulations.

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

Richard L. Skinner

Richard L. Skinner
Inspector General

KPMG LLP
2001 M Street, NW
Washington, DC 20036

December 14, 2007

Inspector General
U.S. Department of Homeland Security

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

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

Ladies and Gentlemen:

We were engaged to audit the balance sheet of the U.S. Department of Homeland Security (DHS) as of September 30, 2007, 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, 2007 (referred to herein as "other financial statements"). Because of matters discussed in our *Independent Auditors' Report*, dated November 15, 2007, 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) 2007 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, 2007, and the related statement of custodial activity for the year then ended, and had we been engaged to audit the other fiscal year 2007 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 DHS' internal control.

The control deficiencies described in this letter include (1) the significant deficiencies and material weaknesses presented in our *Independent Auditors' Report* dated November 15, 2007, Exhibits I and II, Comment C – *Financial Systems Security*, included in the FY 2007 DHS *Annual Financial Report* and (2) other internal control and operational matters with respect to information technology identified during our audit. The significant deficiencies and other comments described herein have been discussed with the appropriate members of management, or communicated through a Notice of Finding and Recommendation (NFRs); 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 financial systems and information technology infrastructure within the scope of the FY 2007 DHS financial statement audit is provided in Appendix A; a description of each internal control finding is provided in Appendix B; and the current status of the prior year NFRs is presented 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 14, 2007.

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

APPENDICES

OBJECTIVE, SCOPE AND APPROACH

We performed an audit of Department of Homeland Security (DHS) Information Technology (IT) general controls in support of the fiscal year (FY) 2007 DHS balance sheet and statement of custodial activity audit engagement. The overall objective of our audit was to evaluate the effectiveness of IT general controls of DHS' financial processing environment and related IT infrastructure as necessary to support the engagement. The Federal Information System Controls Audit Manual (FISCAM), issued by the Government Accountability Office (GAO), formed the basis of our audit. The scope of the IT general controls assessment included testing at DHS' Office of the Chief Financial Officer (OCFO), and all significant DHS component as described in Appendix A.

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

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

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

Financial IT systems security is essential to achieving effective, reliable reporting of financial and performance data. As a part of the financial statement audit, we performed an evaluation of the general controls over significant DHS financial IT systems. Effective general controls are typically defined by the GAO's FISCAM, in six key control areas: entity-wide security program planning and management, access control, application software development and change control, system software, segregation of duties, and service continuity. In addition to general controls, financial systems contain application controls, which are the structure, policies, and procedures that apply to use, operability, interface, edit and monitoring controls of an application. We tested various application controls of key DHS financial systems as part of our IT audit test work.

The primary IT systems evaluated as a part of our audit are the component general ledger and subsidiary/feeder subledger or modules that support the financial statements and specific accounting processes such as grants, loans, excise tax receipts, etc.

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

During FY 2007, DHS civilian components took significant steps to improve their financial systems security, particularly the FISCAM general control areas entity-wide security program planning and management, and system software, which resulted in the closure of more than 30% of our prior year IT control findings.

During the 2007 IT testing, we re-issued over 200 separate findings. In addition, we identified over 61 new IT findings through our test work this year.

The control areas where the IT Notice of Findings and Recommendations (NFR) present a risk of impacting financial data integrity include: 1) excessive access to key DHS financial applications; 2) application change control processes that are inappropriate in other locations not fully defined, followed, or effective; and 3) service continuity issues impacting DHS' ability to ensure that DHS financial data is available when needed. The re-issuance and the additionally identified internal control weaknesses were the result of a lack of needed prioritization of taking the necessary corrective actions and implement corrective actions that will remediate the root cause of the weaknesses in 2007. Consequently, the corrective actions taken more often address the symptom of the problem and not the root cause.

Many of these weaknesses were inherited from system development activities that did not incorporate strong security controls during the initial implementation of the system more than five years ago, and will take several years to fully address. These weaknesses exist both in the documentation of process and the implementation of adequate security controls over processes and within financial systems. Specifically,

policies and procedures supporting the operation of various processes within control areas such as change control and access controls were developed without taking into account required security practices. Consequently, as policies and procedures are updated, many DHS components are challenged to move away from previous methodologies and fully implement and enforce these new controls in unison with other components.

The effect of these Information Technology General Controls (ITGC) weaknesses limits DHS' ability to ensure that critical financial data is reliable and is maintained in a manner to ensure confidentiality, integrity, and availability. In addition, as a result of the presence of IT weaknesses there is added dependency on the other mitigating manual controls to be operating effectively at all times. Because mitigating controls often require more human involvement, there is an increased risk of human error that could materially affect the financial statements.

FINDINGS BY IT AUDIT AREA

Conditions: In FY 2007, the following IT and financial system control weaknesses were identified at DHS and its components. Many of the issues identified during our FY 2007 engagement were also identified during FY 2006. 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:

- Password configurations do not meet DHS requirements for six DHS components;
- User account lists were not periodically reviewed for appropriateness, and inappropriate authorizations;
- Instances where workstations, servers, or network devices were configured without necessary security patches or were not configured in the most secure manner at four DHS components;
- At one DHS component proactive vulnerability scanning is not being conducted to ensure that the system configuration and patches are appropriate;
- Instances where application and database accounts are not immediately disabled upon an employee or contractor's termination occurred at four DHS components;
- Excessive access existed within financial applications at six DHS components. Specifically, instances of generic shared accounts exist on the financial applications. These accounts have every privilege within the application, including the ability to create/delete/modify user accounts;
- User accounts on financial applications are not timed-out after 20 minutes of inactivity;
- The most restrictive security settings for the audit logging of highly privileged accounts and the protection of data sets were not enabled for a financial application at two DHS components;
- Systems have been configured at three DHS components 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;

- Instances at one component in which the procedures to require the DHS component to update the account management documentation as functions are added, deleted, or modified were not formally developed or implemented;
- Procedures are not formally documented requiring the review of the activities of the operating system administrators for one DHS component which resulted in audit logs of operating system administrators not being reviewed;
- Instances at one DHS component in which the inactivity threshold of the password protected screensaver was not in compliance with DHS regulations;
- One DHS component had personnel with excessive access to the Data Center;
- A large number of instances where financial system access policy and procedures are not documented or not followed at five DHS components. Authorization forms are not consistently completed and excessive access was identified;
- Several instances where there are no procedures for immediately removing accounts upon termination or transfer;
- Changes to user's access are not reviewed by a party independent of the security function;
- Instances where physical access controls over sensitive computer operations were not adequate at three DHS components. Physical access authorizations are not documented or periodically reviewed for appropriateness. Additionally, emergency training is not provided to computer operations staff;
- A large number of instances where user accounts on financial applications are not disabled after 30 days of inactivity,
- A large number of instances where user accounts on financial applications are not disconnected or locked out after a period of inactivity,
- Several instances where financial system audit logs, sensitive system utilities logs are not maintained or periodically reviewed,
- Instance of inappropriate system access privileges which allow users to override system edits. Additionally, override reports are not reviewed,
- Instance where Interconnection Security Agreements (ISA) are not documented and in place for all key financial system interfaces,
- Instance where Computer Incident Response Capability (CIRC) procedures are not finalized and implemented. Additionally, an incident response tracking system has not been implemented,
- Policy and procedures regarding implementation of Voice Over Internet Protocol (VOIP), wireless technologies, cryptographic tools, and sharing data with external parties are not finalized, and

2 Application software development and change controls – we noted:

- One DHS component had implemented a separate and secondary change control process outside of and conflicting with the established change control process. Specifically, this second change control process is used to create additional functionality in the system or correct data in the financial applications to make up for gaps in the customized software. During our testing of this separate process, we identified it to be informal, undocumented, and not effective. This weakness affects two DHS components.
- The contract that a DHS component has with the software vendor does not include security configuration requirements that must be adhered to during the configuration management process. The lack of security configurations on this system affects two DHS components.
- Instances where policies and procedures regarding change controls were not in place to prevent users from having concurrent access to the development, test, and production environments of the system at three DHS components.
- Instances where changes made to the configuration of the system were not always documented or performed through System Change Requests (SCRs), test plans, test results, approvals or software modifications at three DHS components. Additionally, documented approval did not exist, or was not always retained, for emergency enhancements, "bug" fixes, and data fixes, and in some cases, audit logs for tracking changes to the data or systems were not activated.
- At two DHS components, changes to a financial application were implemented in the production prior to management approval.
- Instances of a lack of formal policies and procedures for restricting access to application system software and system support files at two DHS components.
- Several instances of excessive access to the system software and system support files existed across one DHS component. For example, an excessive number of individuals who are able to approve system application changes existed on the DHS component's financial systems.
- Policies and procedures surrounding the System Development Life Cycle (SDLC) process have not been documented or adopted a finalized SDLC.
- Instances where approvals for emergency changes are not documented.
- Instance where version control is not enforced in development environment which resulted in the risk of development code being overwritten by developers.
- Several instances where formal test plans are not documented or reviewed.
- Instances of excessive access to financial system program libraries.
- Instances where workstations, servers, or network devices were configured without necessary security patches.

3 Service continuity – we noted:

- Alternate processing site is not operational for one DHS component.

- Contingency plan testing has not been performed for one DHS component.
- The Continuity of Operations Plan (COOP) does not include an accurate listing of critical information technology systems for one DHS component.
- Backup tapes are not rotated off-site for one DHS component.
- An instance where the policy and procedures for the testing of backups are not developed at one DHS component.
- Backup of financial data are not periodically tested for one DHS component.
- Disaster Recovery Plan (DRP) and COOP need improvement. Specifically, critical data files and the alternate processing facility are not documented for one component.
- Rules of Behavior (ROB) forms are not consistently signed prior to gaining local area network (LAN) access for one DHS component.
- Disaster recovery planning has not been completed. Specifically, DRPs for three DHS components are in draft form and have not been tested.
- The Memorandum of Understanding (MOU) for reciprocal services is not complete for two DHS components.
- Contingency plans are not stored at the alternate processing facilities for one DHS component.
- Backup tape rotation logs are not consistently maintained for one DHS component.
- Procedures regarding the use of anti-virus software have not been finalized for two DHS components which resulted in anti-virus software not being installed on all workstations.
- System maintenance policies and procedures have not been finalized.

4. Entity-wide security program planning and management – we noted:
    - IT security awareness training programs have not been finalized or are lacking appropriate criteria for defining personnel with significant IT responsibilities for three DHS components.
    - Policies and procedures over the authorization and use of mobile code technologies are in draft form for one DHS component.
    - Background investigations were not completed for three DHS components. Specifically, for the three components there was no evidence that background investigations and/or reinvestigations were initiated or completed for contracting and civilian personnel selected for testing. Additionally, for two components, policies and procedures requiring contractor background investigations had not been developed.
    - Despite continued improvements in the process of performing Certification and Accreditation (C&A) of IT systems, a major financial application was not properly certified and accredited, in compliance with DHS guidance for two components.

- Exit procedures have not been fully implemented for two DHS components which resulted in exit documentation not being appropriately completed for individuals separated from the components during fiscal year 2007.
- One DHS component does not maintain a centralized listing of contract personnel.
- An Information System Security Officer (ISSO) has not been designated for one DHS component.
- Standard operating procedures lack approvals and/or effective dates for one DHS component.

5. System software – we noted:
   - Policies and procedures for restricting privileged access to system software are in draft form for one DHS component.
   - System specific policies and procedures to review suspicious system software activity have not been developed for two components.
   - Two DHS components have not documented procedures to monitor and review sensitive access and system software utilities.
   - The Virtual Private Network (VPN) server does not maintain information on user accounts (such as date account created, date of last logon, etc.) and procedures for recertifying VPN accounts were not fully implemented.
   - Access authorizations are not maintained for personnel that have administrator access to system software for one component.
   - Patches are inconsistently applied to workstations for one DHS component.
   - Procedures are not formally documented identifying how change control should be performed when applying system software changes, including software patches, to the operating system according to a standard schedule or in an emergency situation for two DHS components.
   - Instances where workstations, servers, or network devices were configured without necessary security patches or were not configured in the most secure manner at one DHS component.
   - A large number of instances of missing and weak user passwords on key servers and databases which process and house financial data at one DHS component.

6. Segregation of duties – we noted:
   - An instance where the policy and procedures to define and implement segregation of duties were not properly developed, implemented and/or are in draft form at two DHS components.
   - Incompatible duties have not been identified at one DHS component.
   - Instances of excessive access to sensitive accounts exist where individuals are able to perform incompatible functions at one DHS component.
   - Database administration accounts are shared at two DHS components.

- An instance where the policy and procedures to perform a formal review over financial data before posting to the general ledger was not developed and/or implemented at one DHS component.
- Access control weaknesses identified during our IT testing also contributed to numerous instances where access to data could lead to various incompatible function issues, including an individual who enters an applicant's data into a financial system also has the ability to hire the applicant in the system at one DHS component.
- One developer for a financial system had access to an elevated privilege in production at one DHS component.

Recommendations: We recommend that the DHS Office of Chief Information Officer (OCIO) in coordination with the OCFO make the following improvements to the Departments financial management systems:

1 For access controls:

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

b) Implement a patch and security configuration process, and enforce the requirement that systems are periodically tested by DHS components and the DHS Chief Information Officer (CIO);

c) 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;

d) Implement an account management certification process within all the components to ensure the periodic review of user accounts for appropriate access and to ensure that generic and inactive accounts do not exist on the system;

e) 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;

f) 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;

g) Implement a periodic review process of accounts that have been inactive by the specified period of time outline in DHS guidance and ensure that the principle of least privilege is implemented;

h) Configure financial applications settings to be compliant with DHS guidance, such as ensure that account sessions are locked out after 20 minutes of inactivity;

i) Develop and implement procedures to require the DHS component to update the account management documentation as functions are added, deleted, or modified;

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

k) Configure the domain level inactivity threshold of the password protected screensaver to be in compliance with DHS guidance;

l) Restrict access to the Data Center using the principle of least privilege;

m) Develop access control policies and procedures that include 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;

n) Implement physical access procedures to ensure that physical access to sensitive computer operations is documented and authorized. This process should also include periodically reviewing physical access for appropriateness and training computer operations staff to respond to emergencies;

o) Configure financial applications settings so that accounts are locked/timed-out after a period of inactivity and that passwords are in compliance with DHS guidance;

p) Identify all key financial system interfaces and document an ISA for each connection;

q) Finalize and implement CIRC procedures and a tracking system;

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

s) Implement configuration management improvements, including installing appropriate upgrades, disabling or removing unnecessary services, and implementing strong access controls.

2 For application software development and change control:

a) 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;

b) Reevaluate and revise the contract between DHS and the software vendor or otherwise ensure that the security configurations associated with the application changes and software patches are in compliance with DHS and National Institute of Standards and Technology (NIST) standards for financial applications;

c) 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;

d) 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 DHS Information Technology Security Program Sensitive Systems Handbook, 4300A (DHS 4300A);

e) Remove excessive access on all DHS financial system software and support files;

f) Develop and implement procedures to perform a periodic review of access to financial system software and support files to determine whether access is valid, consistent with job responsibilities, and according to the least privilege principle; and

g) Document, finalize and implement change control procedures which include test plans and emergency changes;

h) Implement version control procedures which prevent the overwriting of development code in the development environment;

i) Limit access to program libraries to the appropriate individuals;

j) Finalize and implement a SDLC methodology guide that ensures that security planning has been incorporated throughout the life cycle of the system; and

k) Apply the appropriate system updates and vendor patches in a timely fashion.

3 For service continuity:

a) Implement an operational alternate processing site;

b) Perform testing of key service continuity capabilities, including contingency planning;

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

d) Rotate financial data backup tapes off-site on a regular basis;

e) Implement policies and procedures developed to enforce testing of financial data backup tapes;

f) Test financial data backup tapes at least annually;

g) Revise the DRP and COOP to incorporate critical data files and alternate processing facility; and

h) Ensure that all employees and contractors acknowledge and sign a ROB prior to being granted LAN access.

i) Develop and implement complete and current business continuity plans and system DRPs;

j) Perform testing of key service continuity capabilities;

k) Finalize MOUs pertaining to current business continuity plans and system DRPs;

l) Store updated copies of contingency plans at the alternate processing sites;

m) Complete and maintain backup tape rotation logs;

n) Complete procedures regarding the use of anti-virus software and ensure that anti-virus software is installed on all workstations; and

o) Finalize and implement system maintenance policies and procedures.

4 For entity-wide security program planning and management:

a) Finalize and implement an IT security awareness training program and ensure that all employees, contractors and individuals with critical security responsibilities complete the training on an annual basis;

b) Finalize and implement policies and procedures over the authorization and use of mobile code technologies;

c) Perform timely background checks on all new and existing contractors and employees and ensure that adequate supporting documentation is maintained;

d) Maintain a central repository that contains critical details about background investigations such as date investigation was initiated or adjudicated; the type of investigation initiated or adjudicated, risk level, status of investigation, etc;

e) Properly develop and implement C&A packages for all major DHS financial applications while including the appropriate analysis and documentation of its associated subsystems according to DHS and federal guidance; and

f) Ensure that all employees and contractors are aware of the exit process and associated requirements prior to their departure from the component. Additionally, perform a periodic review of exit documentation to ensure that such documentation is completed in compliance with requirements and to ensure that all physical and logical access associated with the terminated individual has been revoked.

g) Implement a contractor employee tracking system, deactivate all system access of terminated contractors immediately upon separation from their respective component, and distribute a listing of terminated contract personnel to information system administrators so they remove user access.

h) Formally document the appointment of the ISSO with a formal designation letter.

i) Perform a review of all documentation to update, consolidate and approve the documented procedures in use by operational personnel.

5 For system software:

a) Finalize and implement policies and procedures for restricting privileged and sensitive access to system software.

b) Finalize and implement policies and procedures for the review of suspicious system software activity.

c) Finalize and implement specific procedures to monitor sensitive access and system software utilities.

d) Configure the VPN servers to include account information (such as date account created, etc) and automate the recertification process.

e) Require documented authorization requests and approval for each person requiring access to administrative privileges within system software.

f) Standardize the workstation patch installation process to include the use of a patch management tool.

g) Develop and implement detailed procedures for the performance of standard and emergency system software change control for operating systems.

h) Implement a patch and security configuration process, and enforce the requirement that systems are periodically tested by DHS components and the DHS CIO; and

i) 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.

6 For segregation of duties:

a) Develop and implement policies and procedures that segregate incompatible duties;

b) Document incompatible duties so that they are consistently separated;

c) Ensure that access to sensitive accounts is restricted to only necessary personnel to achieve the principle of least privilege;

d) Create separate database administration accounts to allow for individual accountability; and

e) Develop and implement procedures to perform a formal review over financial data before posting to the general ledger.

f) Document the user responsibilities so that incompatible duties are consistently separated. If this is not feasible given the smaller size of certain functions, then sufficient compensating controls, such as periodic peer reviews, should be implemented;

g) Ensure that no developers on a particular financial application have access to production for that application.

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. DHS has developed a strategy to consolidate the various DHS financial systems into either one of two standard baseline systems. The implementation of this consolidation effort will be on-going for many years to come.

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. Focus is also placed on the tracking of response to recommendations, instead of on developing the most effective method of addressing the actual control weakness. Additionally, insufficient testing of remediation activities limits DHS' ability to confirm that IT weaknesses are addressed.

Further, there is no consistent and thorough testing of IT controls by individual DHS components and by the DHS CIO to identify and mitigate IT system weaknesses. 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. Additionally, when

weaknesses in controls or processes are identified, the corrective actions taken more often address the symptom of the problem and not the root cause.

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. In closing, for this year's IT audit we assessed the DHS component's compliance with DHS 4300A.

MANAGEMENT COMMENTS AND OIG EVALUATION

We obtained written comments on a draft of this report from the DHS CISO and DHS CFO. Generally, the DHS CISO and DHS CFO agreed with all of our findings and recommendations. The DHS CISO and DHS CFO have 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.

Department of Homeland Security
Information Technology Management Letter
September 30, 2007

Appendix A

Description of Key Financial Systems and IT Infrastructure within the Scope of the FY 2007 DHS Financial Statement Audit

Department of Homeland Security
Information Technology Management Letter
September 30, 2007

Below is a description of significant Department of Homeland Security (DHS) financial management systems and supporting Information Technology (IT) infrastructure included in the scope of the financial statement audit for the twelve months ended September 30, 2007.

Immigration and Customs Enforcement (ICE)

Locations of Audit:

Key Systems Subject to Audit:

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

United States Citizen and Immigration Services (CIS)

Locations of Audit:

Key Systems Subject to Audit:

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

- provides CIS with a 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 CIS forms improvement projects. The is located at each of the and the The main purpose of 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] data is centrally stored within one [redacted] Software is developed and maintained in the [redacted] and Microsoft Visual Basic environments.

United States Coast Guard (CG)

Locations of Audit: Coast Guard HQ in Washington, DC; the Aviation Repair and Supply Center (ARSC) in Elizabeth City, North Carolina; [redacted].

Key Systems Subject to Audit:

- [redacted] – [redacted] is the [redacted] 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 Oracle Financials.

- [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] system.

- [redacted] - [redacted] is the document image processing system, which is integrated with an Oracle Developer/2000 relational database. [redacted] allows electronic data and scanned paper documents to be imaged and processed for data verification, reconciliation and payment. [redacted] utilizes MarkView software 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 Windows server.

- [redacted] - [redacted] is a Microsoft Access Database and is maintained at [redacted] and information from [redacted] is uploaded to this instance monthly. After reconciliation, balancing 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 a mainframe application used for paying Coast Guard retiree personnel payroll.

- [redacted] – Formerly named the Supply Center Computer Replacement System, [redacted] is hosted at [redacted] [redacted] is the primary financial

application for the Engineering Logistics Command (ELC), the Supply Fund, and the Coast Guard Yard fund.

- [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.

United States Customs and Border Protection (CBP)

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

Key Systems Subject to Audit:

- [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 Asset Information Management System mainframe-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.

DHS Consolidated

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] applications reside on the Department of Treasury's network and are administered by Treasury. Treasury is responsible for the administration of the [redacted] Windows NT

server, Oracle 8i database, and the [redacted] applications. The DHS Office of Financial Management is responsible for the administration of DHS user accounts within the [redacted] applications.

Federal Law Enforcement Training Center (FLETC)

Location of Audit: [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]

Federal Emergency Management Agency (FEMA)

Locations of Audit: [redacted]

Key Systems Subject to Audit:

- [redacted] is the key financial reporting system, and has several feeder subsystems (budget, procurement, accounting, and other administrative processes and reporting).
- [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]. [redacted] is a mainframe-based application that runs on the National Flood Insurance Program (NFIP) mainframe logical partition in Norwich, Connecticut.
- [redacted] The general ledger application used by Computer Science Corporation (CSC) to generate the NFIP financial statements. [redacted] is a client-server application that runs on a [redacted] which is secured in the local area network room. The

[redacted] client is installed on the desktop computers of the NFIP Bureau of Financial Statistical Control group members.

Grants and Training (G&T)

Location of Audit: G&T HQ in Washington, D.C. As of April 1, 2007, the G&T component transferred over to FEMA. G&T financial information from April 1 2007, through the end of the fiscal year was processed and stored in a separate instance of FEMA's [redacted] Prior to April 1, 2007, G&T financial information was processed and stored in the applications listed below.

Key Systems Subject to Audit (October 1, 2006 through March 31, 2007):

G&T's IT platforms were hosted and supported by the Department of Justice's Office of Justice Programs (OJP). The following was a list of key financial related applications supporting G&T.

- [redacted] *(same application as FEMA's, but hosted at OJP)* [redacted] consists of five modules that include: budget, cost posting, disbursement, general ledger, and accounts receivable. Users access the system through individual workstations that are installed throughout G&T and OJP. The curren [redacted] version does not have the ability to produce external federal financial reports and financial statements. [redacted] was updated in February 2002 with the version certified by the Joint Financial Management Improvement Program.
- [redacted] supports the G&T grant management process involving the receipt of grant applications and grant processing activities. [redacted] is divided into two logical elements. There is a grantee and an administration element within the system. The grantee component provides the Internet interface and functionality required for all of the grantees to submit grant applications on-line. The second component, the administration component, provides G&T/OJP personnel the tools required to store, process, track and ultimately make decisions about the applications submitted by the grantee. This system does not interface directly with [redacted].
- [redacted] – The [redacted] allows recipients of G&T funds to electronically request payment from OJP on one day and receive a direct deposit to their bank for the requested funds usually on the following day. Batch information containing draw down transaction information from [redacted] is transferred to [redacted] The [redacted] system then interfaces with Treasury to transfer payment information to Treasury, resulting in a disbursement of funds to the grantee.
- [redacted] – This system allows grantees to access their grant funds. The system includes a front and back end application. The front-end application provides the interface where grantees make their grant requests. The back end application is primarily used by accountants and certifying officials. The back end application also interfaces with the [redacted] application. Batch information containing draw down transaction information from [redacted] is interfaced with [redacted]. The [redacted] system then interfaces with Treasury to transfer payment information to Treasury, resulting in a disbursement of funds to the grantee.

Transportation Security Administration (TSA)

Locations of Audit: TSA HQ in Washington, D.C. and the Coast Guard [redacted] in [redacted] TSA's financial applications are hosted on the Coast Guard's IT platforms.

Key Systems Subject to Audit:

- [redacted] is the core accounting system that records financial transactions and generates financial statements for the Coast Guard. [redacted] is hosted at the Coast Guard's [redacted] in Chesapeake, Virginia. [redacted] interfaces with [redacted] Additionally, [redacted] fixed asset module for property management is interconnected to the [redacted] system that is hosted a [redacted]
- [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] systems and is located at the [redacted] in Chesapeake, VA.
- [redacted] [redacted] is a customized third party commercial off the shelf product used for TSA and Federal Air Marshals (FAMS) property management. [redacted] interacts directly with the fixed asset module in [redacted]. Additionally, [redacted] is interconnected to the [redacted] system.

Appendix B

FY2007 Notice of IT Findings and Recommendations - Detail by DHS Organizational Element

Notice of Findings and Recommendation – Definition of Risk Ratings:

The Notice 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 general control environment, on the integrity of the financial data residing on the DHS component's financial systems, and the pervasiveness of finding. 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 financial statements. Also 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 the 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 the PCIE / GAO Financial Audit Manual, or the AICPA Professional Standards, and do not necessarily correlate to a significant deficiency, as defined by the AICPA Standards, and reported in our Independent Auditors' Report on the consolidated DHS financial statements.

High Risk: 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.

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

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

Department of Homeland Security
FY2007 Information Technology
Notification of Findings and Recommendations – Detail

- **Citizenship and Immigration Services**

Department of Homeland Security
FY2007 Information Technology
Notification of Findings and Recommendations – Detail

Citizenship and Immigration Services (CIS)

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CIS 07-01	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.			**Medium**
CIS 07-02	[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 NBC 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** **X**		**Medium**
CIS 07-03	Management at the CIS [redacted] has not completed or inadequately completed access forms for [redacted], and [redacted] users.	Establish and enforce procedures for the completion and maintenance of user access forms for [redacted], [redacted] and [redacted] users.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CIS 07-04	Access to the [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.	• Conduct an annual review of all users with [redacted] administrator access to determine whether access is appropriate. • Establish specific policy and procedures for granting administrator access to [redacted]. These procedures should be standardized and used across the CIS enterprise. Additionally, the procedures should require use of standard forms that are maintained on file.	**X**		**Medium**
CIS 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.	Address and remediate the weaknesses identified in Information Technology NFRs and develop and implement policies and procedures to ensure they are in full compliance with the Federal Financial Management Improvement Act (FFMIA).	**X**		**Medium**

Department of Homeland Security
FY2007 Information Technology
Notification of Findings and Recommendations – Detail

▪ Immigration and Customs Enforcement

Department of Homeland Security
FY2007 Information Technology
Notification of Findings and Recommendations – Detail

Immigration and Customs Enforcement (ICE)

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
ICE 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.	As ICE has effectively implemented a new policy as of April 1, 2007, and as we have subjected the new policy to audit procedures, noting no exceptions, we consider this matter to be closed. This NFR is issued because the condition observed in the prior year continued into the current year and there were continued weaknesses because the condition had not yet been remediated. This condition is considered remediated as of September 30, 2007.	**X**		**Medium**
ICE 07-02	There is excessive access to the [redacted] Currently, over 800 individuals have access to the computer room.	Establish and implement procedures for reviewing computer room access logs on a periodic basis. In addition, we recommend that ICE investigate any suspicious activity.	**X**		**Medium**
ICE 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 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.	• Complete and authorize the standard [redacted] access request form for all new [redacted] user accounts. • Identify all users with administrator privileges and validate that the accounts are necessary and authorized. • Develop procedures for immediate removal of [redacted] accounts upon termination or transfer for all [redacted] users including contractors. • Ensure that personnel managers of either government employees or contractors are aware of their responsibility to notify ICE Office of Financial Management when an employee or	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		contractor is separated or transferred. • Develop and implement procedures for periodically reviewing and disabling [redacted] accounts after 30 days of inactivity.			
ICE 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.	• Develop and implement a standard process for requesting, authorizing, and granting [redacted] access. This procedure should include a standard [redacted] account request form. • Identify all users with [redacted] administrator privileges and validate that the accounts are necessary and authorized. • Develop and implement a standard process for requesting, authorizing, and granting [redacted] administrator accounts. This procedure should include a standard request form and address specific approvals that are necessary. • Develop and implement procedures for immediately removing [redacted] accounts upon termination or transfer for all [redacted] users. Ensure that supervisors are aware of their responsibility to notify the Operations Division when an employee or contractor is separated or transferred. • Finalize and implement procedures for periodically reviewing and disabling inactive accounts on a monthly basis. • Develop and implement procedures for annually recertifying [redacted] administrator accounts.	**X**		**Medium**
ICE 07-05	ICE does not perform periodic reviews of [redacted] audit logs.	Develop and implement procedures for reviewing [redacted] audit logs on a monthly basis. The procedures should include investigation of suspicious activity or suspected violations and reporting findings to appropriate officials.	**X**		**Medium**
ICE 07-06	ICE does not perform periodic reviews of [redacted] audit logs.	Develop and implement procedures for reviewing [redacted] audit logs on a monthly basis. The	**X**		**Medium**

		procedures should include investigation of suspicious activity or suspected violations and reporting findings to appropriate officials.			
ICE 07-07	Evidence of approved emergency change requests are not maintained, which would support the validity and authorization of the changes.	• Document and implement a formal process for recording all necessary aspects of emergency change requests to enable post-implementation review. • Retain evidence of approved emergency change requests.	**X**		**Low**
ICE 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.	Management should continue to develop and implement policies and procedures to ensure they are in full compliance with FFMIA.	**X**		**Medium**

Department of Homeland Security
FY2007 Information Technology
Notification of Findings and Recommendations – Detail

▪ Customs and Border Protection

Department of Homeland Security
FY2007 Information Technology
Notification of Findings and Recommendations – Detail

Customs and Border Protection (CBP)

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CBP-IT-07-01	Due to the design of [redacted], certain controls can be 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	• Develop and implement a management review process of a control override report to facilitate independent review of any control overrides that take place. • Implement the appropriate controls in [redacted] so that supervisory approval is required before a control override can occur.	X		High

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	approval would be an appropriate technical safeguard under application controls.				
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 Virtual Private Network (VPN) 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 VPN solution, in which they will obtain an ISA documenting the connection.	Identify all connections in place with the [redacted] and account for each connection with a documented ISA.	X		**Medium**
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.	• Continue work towards implementation of a contractor employee tracking system. • Deactivate all systems access of terminated contractors immediately upon separation from CBP. • Periodically distribute a listing of terminated contract personnel to information system administrators so they remove user access and periodically assess contractor access to CBP systems.	X		**High**
CBP-IT-07-04	We confirmed that in FY 2007, backup tapes do not 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	Develop a method for labeling tapes that will not interfere with the tape library machinery.	X		**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	risk still remains.				
CBP-IT-07-05	We noted the following issues related to password parameters: • Mainframe minimum password length is set to six characters • Password complexity is not set on the Mainframe • [redacted] local area network (LAN) minimum password length is set to six characters • Password complexity is not set on the [redacted]	• Configure [redacted] password policies to reflect those set forth in CBP and DHS guidance. • Configure [redacted] password policies to reflect those set forth in CBP and DHS guidance.		**X**	**High**
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.	• Modify CBP's automatic session disconnection policy so that it is consistent with DHS policy. • Modify CBP policy to reflect that only the password-protected screensaver must be activated after 5 minutes of inactivity. • Continue deployment of [redacted] and Windows 2003 in order to establish and maintain group policy and enforce password-protected screensaver settings on the workstations.	**X**		**Medium**
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	Implement procedures which prevent the overwriting of development code in the development environment.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	folders they may be overwriting existing changes.				
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].	• Configure the [redacted] system to maintain audit logs and track security events according to CBP and DHS policies. • That [redacted] audit logs be reviewed on a regular bases, according to CBP and DHS policy, to detect potential security events.	X		**Medium**
CBP-IT-07-09	We noted that accounts are not deactivated automatically after 30 days of inactivity. Accounts are disabled for inactivity once a month using a manually initiated job.	Implement a control to automatically disable or remove accounts after thirty days of inactivity in the system.			**High**
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.	• Continue to work towards improving the recertification process. • Require an access request form before access is granted to the data center, as stated in policies and procedures. • Remove terminated employees' access immediately upon termination of the employee.	X X		**Medium**
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.	• Maintain complete and accurate records of [redacted] logs according to CBP document retention policy. • Regularly review the [redacted] logs for suspicious activity according to CBP policy.	X		**Medium**
CBP-IT-07-12	As identified in prior year issues reported in FY 2003, FY 2004, FY 2005 and FY 2006, we	Ensure that [redacted] is installed on all workstations under the control of CBP.			**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	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 [redacted] will not be installed on all workstations for the majority of the fiscal year.				
CBP-IT-07-13	During testwork around the application of security patches, we noted that a complete listing of workstations is not maintained by System Security. We noted that System Security does not have the ability to quickly compile a listing of all workstations under CBP's ownership.	• Work to eliminate the use of local workgroups and include all CBP workstations in a CBP administered domain. • Compile and regularly maintain a full and accurate listing of CBP workstations and use this list to monitor and maintain patch levels for all CBP workstations.	X		Medium
CBP-IT-07-14	We noted that tape withdrawal requests are not documented.	Monitor tape withdrawal requests that come from employees and log these requests to ensure that tape withdrawals are being completed appropriately.			Low
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.	• Change the configuration for [redacted] to disable accounts after 30 days of inactivity. • Change the job schedule for the deactivation procedure to run on a daily basis to minimize the time difference between the inactivity period and deactivation time.	X X		High
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.	• Require supervisory approval each time a user requires activation of emergency access abilities. • Perform regular recertifications of the emergency access table to ensure persons with the capability to request emergency access need to remain on the emergency access table.	X		Medium
CBP-IT-07-17	CBP System Security does not conduct reviews of powerful system utilities. Specifically, the	Implement policies and procedures that have been developed for monitoring and reviewing logs of			Medium

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	utilities [redacted] for CICS 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.	powerful system utilities for suspicious activity.			
CBP-IT-07-18	We noted there are currently no procedures in place for the completion of semi-annual recertifications of [redacted] accounts We also note that a recertification of [redacted] accounts is not performed on a semi-annual basis.	• Develop formal procedures for recertifying [redacted] accounts and access to shared data. • Perform regular recertifications of [redacted] accounts and access to shared data as required by developed procedures.	**X**		**Medium**
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.	• Ensure that security awareness training is completed in a timely manner by all employees with access to CBP information systems. • Continue to work towards implementing online training for all CBP personnel to facilitate automated tracking of the completion of security awareness training.	**X**		**Low**
CBP-IT-07-20	We noted several access control weaknesses for the VPN solution during testwork. Specifically, we noted: • The VPN 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 VPN 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	• Automate the recertification process in order to remove the need for after the fact recertification via methods not documented in recertification procedures (email, verbal, etc.) • Configure the VPN servers to store information about the creation dates and activity of users in order to be able to properly identify inactive accounts and allow for their deletion. • Improve the process of deactivating accounts at the end of the recertification period and ensure that all accounts that should be removed from the system are removed.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	VPN administrators, • Procedures for recertifying accounts were not fully implemented and accounts were recertified by means beyond those identified in documented procedures				
CBP-IT-07-21	We noted that when changes to a user's access are performed in [redacted] and [redacted] the log of these events is not regularly reviewed by personnel independent from those individuals that made the changes.	Formalize procedures for reviewing these access change logs and that review of these logs is implemented on a periodic basis as set forth in criteria.			**Medium**
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 • [redacted] Operations: Standard Operating Procedures – No approval	Implement procedures in Office of IT (OIT) divisions to perform a review of all documentation to update, consolidate and approve the documented procedures in use by operational personnel.	**X** **X**		**Low**
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.	Consistently apply emergency change management post implementation procedures to all [redacted] emergency changes. Furthermore, post implementation procedures should be regularly reviewed and provide regular feedback to change administrators to determine any post implementation steps that may have been missed due to the expeditious nature of emergency changes.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
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.	• Apply procedures outlined in the newly distributed memorandum from OFO dated April 27, 2007 • Consistently document results of re-certifications at the port level and maintain documentation.		**X**	**Medium**
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.	• Formally document the appointment of the [redacted] Interim ISSO with a formal designation letter, and • Appoint a full time ISSO for the [redacted] and document that appointment with a formal designation letter.	**X**		**Low**
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.	Perform periodic review of access violation logs.	**X**		**Medium**
CBP-IT-07-27	We noted that authorizations are not being maintained for personnel that have administrator access to Top Secret.	• Develop and implement procedures to restrict access to mainframe administrative capabilities, and • Require documented authorization requests and approval for each person requiring access to the mainframe administrative capabilities.	**X**		**High**
CBP-IT-07-28	We noted that access policies and procedures have not been formally documented for the [redacted] We also noted that access authorization forms were not completed for 27 out of 45 accounts created in FY 2007.	• Develop and implement access policies and procedures for the [redacted] to document formal methods for requesting and approving access for the [redacted]. • Require documented authorization requests and approval for each person requiring access to the [redacted]	**X**		**Medium**
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	• Implement the recently developed procedures for completion of the termination forms and notify System Security for all terminating employees so that systems access can be		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	submission of the form to System Security and require notification of removal of system access from System Security, the new procedures were developed and activated in June, 2007. The procedures are currently not implemented, however.	removed appropriately.			
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.	• Work with other CBP Offices and within OIT to receive notice of termination of employees in a timely manner so that accounts can be deactivated on the departure of the employee. • Terminate accounts for terminated employees in a timely manner.	**X**		**High**
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.	• Apply procedures outlined in the newly distributed memorandum from OFO. • Consistently document results of re-certifications at the port level.	**X**		**Medium**
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.	Ensure that all program offices appropriately document all test data, transactions, and program change results.	**X**		**Medium**
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.	Ensure that all program offices appropriately document all test data, transactions, and program change results to monitor the quality of program changes.	**X**		**Medium**
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	Ensure that antivirus protection is installed on all workstations under the control of CBP.	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	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-07-35	During our technical testing, eighteen configuration management exceptions were identified on [redacted] Domain Controllers and hosts supporting the SAP application.	Implement corrective actions to ensure that information systems that support the [redacted] application and other financial systems are configured to the security requirements outlined in DHS policy. Configurations that should be addressed include, but are not limited to: stronger password configurations, restrictions on access granted to ports on servers and audit log generation and maintenance.	**X**		**High**
CBP-IT-07-36	During our technical testing, thirty-seven patch management exceptions were identified on [redacted] Domain Controllers and hosts supporting the [redacted] application.	Complete corrective actions surrounding the vulnerabilities identified and implement policies and procedures to ensure that the information systems that support and maintain CBP financial data are secured with the most up to date and tested patches provided by vendors. Patches that have been validated as appropriate for CBP information systems should be applied to these systems to address the conditions noted.	**X**		**High**

Department of Homeland Security
FY2007 Information Technology
Notification of Findings and Recommendations – Detail

- **United States Coast Guard**

Department of Homeland Security
FY2007 Information Technology
Notification of Findings and Recommendations - Detail
United States Coast Guard

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

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CG-IT-07-01	The business Contingency and Disaster Recovery Plan (DRBC) is in draft form and has not been tested for [redacted] and [redacted]. Additionally, [redacted] has drafted a memorandum of understanding (MOU) with the [redacted] for reciprocal services; however, the MOU is currently in draft form.	[redacted] Finalize and implement the Continuity of Operations Plan (COOP) and ensure that it addresses disaster recovery procedures for [redacted] and [redacted] • Finalize the MOU with the [redacted] and document associated restoration procedures so that the [redacted] can serve as an alternate processing site in the event that the finance center is unavailable. • Periodically test the COOP and evaluate the results of the testwork so that the COOP can be adjusted to correct any deficiencies identified during testing.	X		**Medium**
CG-IT-07-02	The [redacted] change control policy is not adequate as it does not accurately reflect a robust change management process. Specifically, the 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.	• Modify the current policies and procedures to reflect the change control and emergency change control process for [redacted] in accordance with DHS and National Institute of Standards and Technology (NIST) standards. Specifically, develop and implement a formalized process for the initial approval, testing, and final approval	X		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Additionally, the policy does not adequately reflect the [redacted] environment and change control process that was utilized during the [redacted] upgrade performed this fiscal year. Examples of inconsistencies include the references to service packs, data fixes and the testing procedures completed.	of all system changes. Additionally, this documentation should include roles and responsibilities of [redacted] personnel in this process. • Develop and implement a formalized process for the retention of documentation throughout the change control process.			
CG-IT-07-03	[redacted] has not implemented corrective action to address the prior year finding and the [redacted] system is not scheduled for decommissioning until December 2007. However [redacted] has implemented a mitigating control to reduce the risk associated with the finding. Specifically, [redacted] implemented the use of Common Access Cards (CAC) in May 2007 which must be used to authenticate to the network using a six to eight digit pin. Prior to implementing the use of a CAC, [redacted] required users to log onto the network using a strong password.	[redacted] should continue with their projected plan for decommissioning the [redacted] system.	**X**		**Low**
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: • We determined that from October 1, 2006 through July 24, 2007, [redacted] had not yet implemented policies and procedures for use in managing terminations, including the use of the Outgoing Personnel Form. We are reporting this as an issue since the policy and procedures were not in place for a majority of the fiscal year. This condition will not have an associated recommendation since [redacted] has taken the corrective action to develop and issue [redacted] Instruction 1320.2A.	[redacted] should: • Strictly enforce the newly developed procedure and ensure that outgoing personnel forms or checkout sheets are completed for all departing military, civilian and contractor personnel. • Removal the accounts by the [redacted] Technical Support group of terminated individuals immediately upon receiving notification of the termination.	**X**		**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• Outgoing Personnel Forms were not completed for one of five individuals selected for testing. • We also identified that the account of one terminated individual remained active within [redacted] until 90 days after his last logon before his account was revoked as part of the [redacted] review process. • The account of a second terminated individual remains active within the system, although it has 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-IT-07-05	[redacted] has developed policies and procedures for requesting, authorizing, testing and approving operating system changes. However, we noted during our testing that those polices and procedures are not being consistently followed for such changes. 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.	[redacted] should: • Modify the SDLC document or create new change management procedures that are tailored to the operating system environment. These procedures should detail out the requirements for requesting, authorizing, testing and approving operating system changes and should note the documentation that should be retained for each change. • Establish a testing baseline/standard that can be tested each time a change is introduced into the operating system to ensure that each change does not affect portions of the system that were not intended to be changed. This could be accomplished by developing a	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		checklist and requiring that the checklist be completed each time a change is made. • Establish procedures to be followed to ensure that all changes to the operating system can be tied back to a listing of authorized operating system changes.			
CG-IT-07-06	The contract that CG HQ has with the [redacted] and [redacted] software vendor does not include security configuration requirements that must be adhered to during the configuration management process. Consequently, [redacted] and [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-841 should reevaluate and revise the contract between CG and the [redacted] and [redacted] software vendor or otherwise ensure that the security configurations associated with the builds, service packs, and software patches are in compliance with DHS and NIST standards for [redacted] and [redacted]	**X**		**High**
CG-IT-07-07	[redacted] now requires [redacted] passwords to be eight characters in length and does not allow a user to set his/her password to the same as the previous eight passwords. However, KPMG 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	[redacted] should: • Continue to seek improvements to [redacted] sign-on technology that would enforce password complexity requirements to meet DHS Sensitive Systems Policy Directive 4300A (DHS 4300A) standards. • Educate all employees and contractors of DHS 4300A password requirements so they can set their passwords in accordance with policy despite the systems inability to enforce them.	**X**		**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	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 User ID				
CG-IT-07-08	The [redacted] function is set to the default [redacted] and the [redacted] is not enabled. [redacted] enables the activities of users with the [redacted] attribute to be logged to the system management facility while [redacted] protects datasets by requiring every dataset to have a [redacted] rule covering it. Additionally, during our testing of [redacted] accounts, we determined that five [redacted] personnel accounts have both the [redacted] and [redacted] attributes and two of these individuals are system programmers. Although each account has been assigned to only one individual, no audit logging to track accountability has been enabled. Furthermore, two highly privileged generic accounts exist in the [redacted] system. The first account, [redacted] is a system account that has both [redacted]	[redacted] should: • Set [redacted] security settings to the most restrictive modes possible. Specifically, the following [redacted] settings should be changed: - [redacted] - Enable [redacted] in fail mode • Develop policies and procedures for the generation and review of audit logs to ensure that actions performed by individuals with privileged accounts are appropriate. • Review access to sensitive [redacted] privileges to ensure that the principle of least privilege is enforced so that users privileges extend to only those needed to perform their job functions. Additionally, for those accounts	X		Medium

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	attributes. According to IBM security standards, the [redacted] account should be disabled. However, this account is still active within the system and used by the system programmer to reset the password on his account when he gets locked out. The second account noted, [redacted], was identified as an old account used for a system install and [redacted] management indicated that this account will be revoked in the system..	determined to have excessive privileges, revoke unneeded privileges. • Revoke the [redacted] account in [redacted]. • Revoke the TSO5 account in [redacted].			
CG-IT-07-09	Although [redacted] has developed re-entry procedures, continued to limit entry into the data center and created a curriculum that must be completed annually by data center staff, weakness were noted in the process. Specifically, we determined that 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 KPMG with supporting evidence.	We recommend that [redacted] implement corrective action to ensure that all personnel with access to the data center have completed the data center emergency response training.	**X**		**Low**
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	• Implement procedures to ensure compliance with DHS policies for the background investigations of contracting personnel, such as DHS 4300A. • Ensure that all contracts procured by	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	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.	CG HQ, include the appropriate suitability designation for contracting personnel working on the contract and require completion of suitability checks specific to the position risk level prior to beginning work at CG. Additionally, ensure that all current contracts are updated with the required language. • Provide resources to CG Components to fully implement the developed procedures.			
CG-IT-07-11	Terminal sessions to [redacted] are locked out after 40 minutes of inactivity, rather than 20 minutes as required by DHS.	[redacted] should configure the terminal sessions to be locked out after 20 minutes of inactivity as required by DHS.			**Low**

CG-IT-07-12	• [redacted] General Support System (GSS) was tested and the [redacted] Disaster Recovery Plan (DRP) was tested at the CG [redacted] which now serves as [redacted]'s disaster recovery (DR) facility as of July 2007.
	• Additionally, KPMG received a signed copy of the finalized contract between the [redacted] and Equinix (the off-site disaster recovery facility from October 2006 through June 2007).
	• However, KPMG noted that the following prior year weaknesses as not remediated:
	  • The [redacted] DRP was not tested.
	  • A MOU between [redacted] and [redacted] was not completed. [redacted] was responsible for conducting a [redacted]) switch for the [redacted] for the period of October 2006 through June 2007.
		[redacted] should implement corrective action to ensure that the [redacted] DRP is tested at [redacted] and that the test is documented in accordance with DHS requirements.
		
		No further recommendation regarding the MOU with [redacted] is required. A memorandum of agreement (MOA) is in place between the [redacted] and [redacted].
			X	**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CG-IT-07-13	[redacted] is not consistently following the SDLC for all [redacted] application changes. Specifically, we inspected documentation associated with four system change proposals (SCP) and their associated sub-tasks and determined that supporting documentation (i.e., evidence of testing, peer reviewer approvals, evidence of joint application design meetings and business sponsor approvals) was not available for each change selected for testing.	[redacted] should enforce the change control requirements outlined in the SDLC and perform periodic spot checks to ensure that all documentation associated with each change is appropriately retained as required.		**X**	**Low**
CG-IT-07-14	CG IT Security Awareness Policies and Procedures lack 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.	• Enhance current policies and procedures for IT role based training to require those with critical security responsibilities, such as network administrators, system administrators, senior managers and system owners, to complete the role based training on an annual basis. • Deploy the IT role-based training of civilian personnel with critical IT positions down to the CG component levels for implementation.	**X**		**Low**
CG-IT-07-15	During our FY 2007 follow-up testing, we determined that [redacted] had taken corrective action on several of the previously noted vulnerabilities, however several remained. The remaining vulnerabilities are in the following four areas: • Account management - 1 medium-risk vulnerability • Configuration management – 1 high vulnerability • Password management – 5 medium risk vulnerabilities • Patch management - 1 medium risk vulnerability	[redacted] should complete the following corrective actions to reduce the risk of access control weaknesses associated with [redacted]: • Upgrade the Oracle Database to a version that is currently supported by Oracle. • Apply strong passwords to all database accounts. • Implement vendor provided fix: remove the setUID bit from the oracle file with command: cd [redacted]	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		• Set minimum password age to five days on all accounts. • Set maximum password age to 180 days on all accounts. • Enable the password expiration parameter. • Enable the password expiration parameter. • Document the current process used for both performing vulnerability scans of the [redacted] network environment as required by DHS 4300A and for implementing corrective action on identified and appropriate scan vulnerabilities.			
CG-IT-06-16	[redacted] has developed and implemented policies and procedures that address the review of inactive [redacted] accounts and lock those that have been inactive for ninety (90) days. However, DHS guidance requires that inactive accounts be locked after thirty (30) days.	[redacted] should modify [redacted] account lockout procedures for inactive accounts to be in accordance with DHS guidance.	**X**		**Low**
CG-IT-07-17	[redacted] password configuration does not meet the following DHS requirements for [redacted] • Passwords must 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 number, Social Security number, birth date, phone number, or any information that could be readily guessed about the creator of the password	[redacted] should implement the use of mitigating controls for those DHS password requirements that cannot be enforced by the system. An example of mitigating controls would include providing the password requirements to each existing and new system user and encouraging them to set their password in compliance with the requirements even though it cannot be enforced or to require both new and existing users to sign a Rules of Behavior (ROB) that notes they	**X**		**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• 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.	are utilizing and will utilize a password in compliance with DHS guidance.			
CG-IT-07-18	• The [redacted] application and database does not meet the following password requirements noted in DHS 4300A: -Passwords must 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 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. • [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	• Ensure that the [redacted] password configuration meets DHS requirements. For those requirements that cannot be implemented, due to system limitation, implement the use of mitigating controls to reduce the risk associated with weak passwords (i.e., review invalid logon attempts to the system, review audit logs, etc). • Remove/end-date/disable the accounts of terminated individuals from the system immediately upon their departure. This includes both terminated employees and contractors. • Develop and implement access control procedures for the [redacted] system and database accounts. These procedures should include, at a minimum, steps for reviewing the system and database user listings to ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked, and that privileges		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	not being reviewed for appropriateness.	associated with each individual are still authorized and necessary. Additionally, the procedures should note the parties that should be involved in the review process (i.e. – supervisors, database administrators and system administrators) and supporting documentation that should be maintained as a result of the review.			
CG-IT-07-19	• We were unable to obtain a copy of the [redacted] password configuration from the CG point of contact. 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: • Access request authorizations were unavailable for two individuals granted access to the [redacted] database during FY 2007. • [redacted] application and database accounts are not immediately disabled upon an employee or contractor'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. • Although the [redacted] system has been configured to track and lock accounts that have not been utilized in 90 days, DHS guidance now requires that accounts that have not been used in 30 days be deactivated. • An excessive number of individuals had user administrator capabilities within [redacted] until the	• Configure the [redacted] password configuration to be in compliance with DHS guidance. For those requirements that cannot be implemented, due to system limitation, implement the use of mitigating controls to reduce the risk associated with weak passwords (i.e., review invalid logon attempts to the system, review audit logs, etc). • Ensure that a documented and approved access authorization request is completed for each individual prior to granting him/her access to the [redacted] application or database. • Ensure that the system administrators, system owners, and database administrators are notified of terminated employees and contractors so that they can be removed in the system in a timely manner. • Develop and implement procedures to require a periodic review of [redacted]	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	implementation of the centralized user management (August 19, 2007). • Specifically, four individuals had unauthorized access during this time. Additionally, once centralized user management was implemented we noted the use of four generic shared accounts: [redacted]. These accounts have every privilege within the application, including the ability to create/delete/modify user accounts within FPD.	accounts and their associated privileges be reviewed for appropriateness. • Configure the system to track and lock inactive [redacted] accounts in compliance with DHS requirements. • Remove all generic shared system accounts or establish individual accountability for these accounts. If these accounts cannot be removed, enable audit logging to capture the user's operating system logon ID so that individual accountability can be established for each instance of when these accounts are used.			
CG-IT-07-20	[redacted] has begun to implement corrective actions to address the prior year findings. Specifically, we determined that [redacted] has implemented new procedures to guide the periodic review of Direct Access accounts. However, the reviews only cover 1% of all user accounts with roles greater than Self Service and that have been modified within the past 90 days. The population that is validated during this Direct Access system review was found to be insufficient as the user population of the system is approximately 60,000 user accounts.	[redacted] should develop policies and modify procedures to include the periodic review of all Direct Access accounts to ensure that all accounts and their associated privileges have appropriate access to the system, specifically to sensitive areas.	**X**		**Medium**
CG-IT-07-21	[redacted] has begun to implement corrective action to address the prior year finding. Specifically, we noted that [redacted] has developed and implemented a formalized process for requesting and authorizing access to [redacted]. We tested this process and determined it to be operating effectively. Additionally, [redacted] system administrators	[redacted] should modify procedures to include the periodic reviews of all [redacted] accounts to ensure that all accounts and their associated privileges have appropriate access to the system, specifically sensitive areas.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	implemented a review of accounts for terminated, transferred and retired individuals. This review is performed on a monthly basis to ensure that accounts are owned by individuals who are still employed by CG. Also, [redacted] has developed and implemented policies and procedures that address the review of inactive [redacted] accounts and lock those that have been inactive for ninety (90) days. However, we noted that 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.				
CG-IT-07-22	Password rules have 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 We acknowledge that a waiver was obtained by CG to address the DHS requirement that systems disable idle accounts after 20 minutes.	• Modify the [redacted] application password configurations to be compliant with DHS and CG policy. For those requirements that cannot be implemented, due to system limitation, implement the use of mitigating controls to reduce the risk associated with weak passwords (i.e., review invalid logon attempts to the system, review audit logs, etc). • Configure the [redacted] application to terminate idle sessions after a specified period of inactivity as defined in DHS and CG policy.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	No determination was made on the waiver for this NFR.				
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. • We acknowledge that a waiver was obtained by CG to address the DHS requirement that audit logs over the use of sensitive system utilities be reviewed. No determination was made on the waiver for this NFR.	• Develop and implement procedures to monitor the actions of the Database Administrators (DBA) for the [redacted] application to determine whether actions taken in the system environment are appropriate to their job function. • Develop and implement procedures to periodically review the actions taken by [redacted] users while performing operations in the system and determine whether the actions taken by [redacted] end users are appropriate to their job function.	**X**		**High**
CG-IT-07-24	End user computing procedures have been developed, but that they are currently in draft form. At the time of testing, CG was in the process of reviewing the procedures, but had not implemented the updated process. Therefore these procedures cannot be relied upon in order to perform further testwork.	CG should formalize the draft policies that have been developed and implement these procedures around the calculation of the environmental liability using data stored in the [redacted] application.	**X**		**Medium**
CG-IT-07-25	• Excessive access exists within the [redacted] database. During our FY 2007 follow-up testing, we noted that [redacted] has reduced the number of individuals with access to the [redacted] role to 388 and limited the number of tables that can be updated to 396. Additionally, each user has been granted SQL flow roles within the application which limits the forms they can view and sub sequentially, the tables that they can update in the database. However, [redacted] has not documented the	• Continue with efforts to reduce the number [redacted] role and the number of tables that can be updated to ensure that each user has a business need to update each table. Additionally, document a mapping between the SQL flow roles and the associated database tables that are affected. • Configure the [redacted] password		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	mapping between the SQL flow roles and the related database tables; therefore, we are unable to determine if the tables associated with each SQL flow role have been appropriately restricted. Additionally, although these 388 users are not responsible for logging directly into the [redacted] database to make updates and would have to have the client SQL+ installed on their desktop, the risk still exists that these users could gain access to the database and modify data that they are not authorized to modify. • The [redacted] profiles do not meet DHS password requirements. (Although the [redacted] profile was not assigned to any new WINS users during FY 2007, users with this profile were transferred to the [redacted] profile during the fiscal year.) • Nine out of 30 automated access request (AAR) forms did not contain the privileges the user was to be assigned within [redacted]. Additionally, three of the 30 AAR forms did not contain a supervisor's approval. • [redacted] application and database accounts are not immediately disabled/end-dated upon an employee or contractor's termination. • [redacted] application and database accounts are not being reviewed for appropriateness.	configuration to be in compliance with DHS guidance. For those requirements that cannot be implemented, due to system limitation, implement the use of mitigating controls to reduce the risk associated with weak passwords (i.e., review invalid logon attempts to the system, review audit logs, etc). • Ensure that a documented and approved access authorization request is completed for each individual prior to granting him/her access to the [redacted] application or database. • Ensure that the system administrators, system owners, and database administrators are notified of terminated employees and contractors so that they can be removed in the system in a timely manner. • Develop and implement procedures to require a periodic review of [redacted] accounts and their associated privileges be reviewed for appropriateness.			
CG-IT-07-26	[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.	[redacted] should track and end-date/disable [redacted] accounts in compliance with DHS requirements.	**X**		**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CG-IT-07-27	[redacted] weaknesses still exist. Specifically, we noted that: • A review of inactive accounts is not being performed. We noted that accounts inactive for more than 90 days still remained active on the [redacted] application • Access request authorization forms were unavailable for 19 of a selected 30 individuals who had accounts created during FY 2007. • A recertification of [redacted] accounts is not performed. • Terminated employees are not terminated in a timely manner. Reliance is placed on the compensating control of deactivating accounts after 90 days.	• Immediately deactivate accounts that have not been used in 90 days. • Work with the Customer Service Division (CSD) at [redacted] to document access requests and approvals for all new accounts created to access the system and maintain those requests for at least one year. • Implement procedures to perform a periodic review of user accounts on the system and the roles associated with each account. • Work with [redacted] to receive termination notices of individuals in a timely manner so that access to the [redacted] system can be removed in a timely manner.	X		**Medium**
CG-IT-07-28	• One developer had access to an elevated privilege in [redacted] production. • We also noted that [redacted] privileges in [redacted] role was removed from production environment during FY 2006. However, upon inspection in FY 2007, we identified two procedures/packages [redacted] that had been added to [redacted] privileges. We noted that upon identification of this issue on September 26, 2007, the two procedures/packages were removed from the [redacted] role.	• Remove developer's elevated privileges in the production environment. • Periodically review [redacted] role to ensure that [redacted] privileges are not available in production.	X		**Medium**
CG-IT-07-29	[redacted] has not taken corrective action to address the user roles surrounding the entering and hiring of	Segregate the roles by requiring that the person who enters an applicant's data is	X		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	an applicant by the same individual. Specifically, the individual who enters an applicant's data into the Direct Access system also has the ability to hire the applicant in the system.	not the person that hires the applicant. However if the roles cannot be segregated, implement the use of a mitigating control. (i e have an independent party at [redacted] monitor Direct Access audit trails on a regular basis to ensure that activities are authorized.)			
CG-IT-07-30	[redacted] has begun to take corrective actions surrounding the [redacted] functional change control process by developing policies and procedures. However, upon review of the policies and procedures, we noted that they did not reflect the change control process for the Matchpass 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 [redacted] production environment. We noted that the guidance is minimal in the requirements for initial approval and does not fully address the testing requirements, final approvals and documentation retention requirements for the process.	• Further develop and implement functional change control polices and procedures to include requirements for requesting, testing, and approving changes. Additionally, include the various branches involved in the process as well as their roles and responsibilities. • Develop and implement a formalized process for the retention of documentation throughout the change control process for [redacted] functional changes.	**X**		**Medium**
CG-IT-07-31	CG has and continues to operate a separate, informal and largely undocumented change development and implementation process effecting CG Financial Systems, outside of and conflicting with the formal change control process. This informal script development and implementation process began with the implementation of [redacted] in June of 2003. [redacted] reports that the documentation and tracking of the scripts was not developed until June of 2005 but is unable to provide a complete	• Immediately implement a single, integrated change control process over CG Financial Systems with appropriate internal controls to in include clear lines of authority to CG financial management personnel, enforced responsibilities of all participants in the process and documentation requirements • Continue with plans to further commence an in depth examination	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	population of implemented scripts, to include the type, purpose and intended effect on financial data. The implemented process is ineffective as the approval, testing and documentation procedures of the script changes are not appropriately designed and the current process is ineffective to control the intended and actual effect on financial data.	of the CG Financial Systems with an external independent organization trained in financial information systems, process analysis and with a demonstrated understanding of the federal accounting environment to determine the root causes and specific, detailed actions necessary to correct the conditions that caused scripts as well as manual adjustments to be implemented. CG's root cause analysis needs to specifically determine if the causes are process or system driven to determine the appropriate corrective actions. • In conjunction with item number two above, begin an in depth examination to determine and document, in detail, the effects of the identified root causes and implemented automated and manual adjustments on financial data and affected financial statements for prior reporting periods and make appropriate restatements, if necessary.			
CG-IT-07-32	CG does not maintain a centralized listing of contract personnel, including employment status, such as start date and termination date, so that system accounts can be timely updated.	CG HQ should implement policies and procedures to track the status of CG contractors.	**X**		**Medium**
CG-IT-07-33	CG does not consistently notify system owners that individuals are terminating from the CG so that system accounts can be updated timely.	CG HQ should develop a method to inform system owners that individuals are terminating from the CG and that their systems access should be locked and/or removed upon their termination from the	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		CG.			
CG-IT-07-34	[redacted] has begun to take corrective actions surrounding the [redacted] change control process by further developing policies and procedures to address the [redacted] change control process for both scheduled changes and emergency changes. However upon review of a selection of changes, we determined that [redacted] is not consistently implementing the policies and procedures. Specifically, we inspected documentation associated with 25 system 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 the twenty (20) of the changes and emergency changes selected for testing. Additionally, one of the changes provided for testing, indicated in the initial tests that an error was occurring in the pre-production instance. Documentation indicated that developers worked on this change to eliminate the error and the change finally passed testing. However, upon review of the approval to move the change into production, we noted that the change was approved prior to the change being tested and passed appropriately.	[redacted] should implement the following: • Approve and complete each field related to the SCR within PVCS Tracker in accordance with the documented requirements of the Finance Center Staff Instructions. • Ensure that the information retained in the Tracker includes detailed documentation surrounding test plans, testing, and approving changes and emergency changes. • Ensure that all changes follow the change control process and are tested and fully pass testing prior to approval to move the change into production.		**X**	**Medium**
CG-IT-07-35	Policies and procedures for the overall change control process surrounding [redacted] changes and emergency changes are inadequate. Specifically procedures detail the overall process and phases for [redacted] change control, but lack detailed guidance for the roles and responsibilities executed by [redacted] personnel and do not address emergency changes. Additionally,	[redacted] should complete the following: • Continue to develop and implement a more detailed change control policy and procedure to formally define the change control process for [redacted] to include the different roles and responsibilities that personnel within CG-[redacted] must complete. Additionally, ensure	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	[redacted] is not consistently retaining documentation to support the change control and emergency change control process.	that the policies and procedures developed include the emergency change control. • Develop and implement policies and procedures to specifically address initial approvals of the changes proposed by the software vendor, including technical changes, testing involved, and additional testing performed by [redacted]. • Continue to develop and implement a formalized process for the retention of documentation throughout the change control process.			
CG-IT-07-36	Technical testing identified patch management weaknesses on hosts supporting the [redacted] applications which could allow for a remote attacker to gain full control of the affected host and could lead to the compromise of the availability, confidentiality and integrity of [redacted] data.	[redacted] should complete corrective actions surrounding the vulnerabilities identified and implement policies and procedures to ensure that the software builds created by the CG software developer are tested, prior to implementation, to ensure that all software security configurations, such as software patches and non-compliant settings, are up to date.			**High**
CG-IT-07-37	Technical testing identified configuration management weaknesses on hosts supporting the [redacted] applications. Specifically, servers were identified with excessive access privileges, and password and auditing configuration weaknesses.	[redacted] should complete corrective actions surrounding the vulnerabilities identified and implement policies and procedures to ensure that the software builds created by the CG software developer are tested, prior to implementation, to ensure that all software security configurations, such as software patches and non-compliant settings, are up to date.	**X** **X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CG-IT-07-38	[redacted] has taken corrective actions surrounding the CG [redacted] change control process by developing a policies and procedures that reflect an adequate change control process. However upon review of the implementation of the process, we determined that the 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. Consequently, all three program changes selected for testing were not approved by the appropriate individuals prior to implementation in the production environment. Additionally, the systems personnel moving the program changes into production informed us that they do not sign off on the Request Change to TIER Database form after moving the change as required by the [redacted] procedures.	[redacted] should complete the following: • Ensure that personnel involved in the CG [redacted] change control process follow the policies and procedures set forth in [redacted]'s Financial Reporting Procedures for Changes to CG [redacted]. • Ensure that all CG TIER changes are tested and that the test results are reviewed and approved by the appropriate [redacted] management prior to implementation in the production environment. • Require that all individuals that have a role in the change control process complete the appropriate fields in the Request Change to [redacted] Database form.	**X**		**Medium**
CG-IT-07-39	CG is making progress in the number of background investigation records that remain to be restored. However, CG has not completed the process of filing the records that were recovered and recreating of the records that were not found during the migration of records from the Department of Transportation to DHS.	CG should complete the process of restoring the background investigation records of their military and civilian personnel that were not included during the migration of records from the Department of Transportation to DHS.	**X**		**Low**
CG-IT-07-40	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 DHS 4300A.	CG should completion of performing initial background investigations and reinvestigations for civilian employees in accordance with DHS directives.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Additionally, 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.				
CG-IT-07-41	[redacted] management had not adequately completed the [redacted] Certification and Accreditation (C&A) package to reflect the current state of the application. For example, we noted: • System boundary definitions do not fully reflect the systems environment in which CG operates; • C&A does not reflect system changes made in the [redacted] 4.1 upgrade; and • Sunflower is classified by CG as a subsystem of [redacted] However, we noted that there is no documentation within the [redacted] system [redacted] as security plan (SSP) that defines a subsystem and specifically addresses the appropriate security controls for [redacted] in this capacity according to NIST requirements for subsystems. [redacted] management indicated that C&A package is in the process of being updated due to the [redacted] 4.1 build. However, the process has not yet been completed.	[redacted] should complete corrective actions to update the [redacted] C&A package in accordance with DHS and NIST guidance. For example, appropriately complete steps to accurately define subsystems and system boundaries, remote connections and the new [redacted] 4.1 build..	**X**		**Low**
CG-IT-07-42	As a result of our audit test work and supported by all the IT NFRs issued during the current year, we determined that CG is non-compliant with the FFMIA in an information technology perspective and in the following areas:.	• Continue to implement and monitor compliance with DHS, CG and Federal security policies and procedures in the areas of: • Change Controls	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• 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	• Access Controls • Entity-wide Security Planning • Service Continuity • Segregation of Duties • System Software • Application Controls • Develop and implement corrective action plans to remediate the NFRs issued during the FY 2007 audit. These corrective action plans should be developed 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.			

Department of Homeland Security
FY2007 Information Technology
Notification of Findings and Recommendations - Detail

- **Federal Emergency Management Agency**

Department of Homeland Security
FY2007 Information Technology
Notification of Findings and Recommendations - Detail

Federal Emergency Management Agency (FEMA)

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-07-01	During our technical testing, patch management weaknesses were identified on [redacted] systems.	FEMA should implement the corrective actions listed in the NFR for each technical control weakness identified.		X	High
FEMA-IT-07-02	During our technical testing, configuration management weaknesses were identified on [redacted] and key support servers.	FEMA should implement the corrective actions listed in the NFR for each technical control weakness identified.			High
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 al [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.	• Complete the recertification of [redacted] user access by removing the access of individuals who did not complete FEMA Form 20-24, [redacted] Access Control Form, and validating the existing [redacted] user access of individuals who completed FEMA Form 20-24. • Implement the Office of the Chief Financial Officer (OCFO) Procedures for Granting Access to [redacted] by continuing to perform a review of all [redacted] access on a semi-annual basis including verifying the access privileges granted to federal employees and contractors.	X X		High
FEMA-IT-07-04	The FEMA alternate processing site located in Denton, TX is not operational for [redacted]. FEMA is in the process of setting up a	FEMA should complete its efforts to implement the [redacted] Data Center's "real-time" back-up facility			High

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	[redacted]) to replicate data from the [redacted] production server at [redacted] and send it to the [redacted] servers in [redacted] Currently the [redacted] is 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.	as its alternate processing site and create redundant servers for the two [redacted] servers located at [redacted].			
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.	Document the results of the [redacted] ST&E by providing a detailed listing for the vulnerabilities and/or corrective action for the vulnerabilities in the Authorization to Operate (ATO) as well as documenting them in an individual manner in the POA&M when the system is re-certified and accredited in FY 2008.	**X**		**Medium**
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.	Develop and implement procedures to require updates to [redacted] documentation as functions are added, deleted, or modified.			**Low**
FEMA-IT-07-07	We determined that FEMA has identified the [redacted] as the alternate processing facility for [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.	Perform a full-scale test of the [redacted] Contingency Plan once the [redacted] Data Center is operational as the alternate processing site for [redacted] As a part of the full-scale contingency plan test, FEMA should include the critical IT components, such as key contingency personnel, backup servers at the alternate processing site, and use of backup tapes to bring up the system, in order to assess if they will operate as planned. Additionally, testing of the [redacted] Contingency Plan should be performed annually.	**X** **X**		**Medium**
FEMA-IT-07-08	We determined that the FEMA COOP has not been updated to include the new listing of FEMA mission critical IT systems as	Update the FEMA COOP to clearly state and prioritize the listing of twenty-two (22) mission critical IT systems to be restored at its alternate	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	outlined in the Information Technology Services Directorate (ITSD) COOP Implementation Plan.	processing site in the event of a disaster.			
FEMA-IT-07-09	• We noted that FEMA has begun to standardize all user workstations to Microsoft Windows XP with Service Pack 2 installed, which would ensure that all [redacted] settings are properly applied to all users. Currently, FEMA is upgrading older user workstations to Microsoft Windows XP 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.	• Continue upgrading all FEMA domain level user's workstations operating system to Windows XP with Service Pack 2 installed and ensure that all [redacted] settings are properly applied to those users, including disabling the user's ability to change the inactivity threshold of the password protected screensaver. • Ensure that FEMA users locked out of the system at the domain level after three consecutive failed login attempts remain locked for 20 minutes, per DHS 4300A.	**X**		**Medium**
FEMA-IT-07-10	We determined that FEMA has begun to standardize all user workstations to Microsoft Windows XP with Service Pack 2 installed which would ensure that all [redacted] settings are properly applied to all users. Currently, FEMA is upgrading older user workstations to Microsoft Windows XP or providing users with new workstations. However, we noted that this process is not fully completed, and FEMA has estimated this process will not	Continue upgrading all FEMA domain level user workstation operating systems to Windows XP with Service Pack 2 installed and ensure that all [redacted] settings are properly applied to those users, including disabling the user's ability to change the inactivity threshold of the password protected screensaver.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	be completed until January 2008. This weakness impacts [redacted].				
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 DHS 4300A.	• Configure the [redacted] application to require passwords to not be reused until eight (8) iterations have passed to be in compliance with DHS 4300A.			**Medium**
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.	• Complete implementation of procedures regarding the periodic review of [redacted] access lists, including the frequency of the review. Furthermore, FEMA should complete the review of [redacted] user access for FY 2007 by taking all responses received for users and updating [redacted] user access accordingly. • Continue to develop the automated process around granting, removing and validating [redacted] user access and implement by March 2008, per the FY 2006 FEMA IT Financial Audit Remediation Plan.	**X** **X**		**Medium**
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	• Complete the recertification of [redacted] user access by removing the access of individuals who did not complete FEMA Form 20-24, [redacted] Access Control Form, and validating the existing [redacted] user access of individuals		**X**	**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	within their organization. Additionally, we noted that a recertification of all [redacted] users was performed in June 2007. Currently, FSB is in the process of validating [redacted] access for the users who responded to FSB's 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	who completed FEMA Form 20-24. • Implement the OCFO Procedures for Granting Access to [redacted] by continuing to perform a review of all I[redacted] access on a semi-annual basis including verifying the access privileges granted to federal employees and contractors. • Complete implementation of procedures regarding the periodic review of [redacted] access lists, including the frequency of the review. Furthermore, FEMA should complete the review of [redacted] user access for FY 2007 by taking all responses received for users and updating [redacted] user access accordingly. • Continue to develop the automated process around granting, removing and validating [redacted] user access and implement by March 2008, per the FY 2006 FEMA IT Financial Audit Remediation Plan. • Per FEMA Instruction 1540.3, perform a review of authorized accounts on a semi-annual basis and remove terminated employees' access to all FEMA systems.			

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	(770) terminated or separated FEMA employees and contractors maintain active [redacted] user accounts.				

FEMA-IT-07-14	• We determined that IT Operations has created backup procedures entitled, *Backup Media Protection and Control*, for [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] backup tapes are not rotated off-site to the Virginia NPSC.
	
	• We noted that the FEMA alternate processing site located in Denton, Texas is not operational for [redacted]. We also noted that the Denton back-up facility has redundant servers in place for the [redacted] Oracle Database in June 2007. Therefore, the risk was present for a majority of the fiscal year.
		• Implement the *Backup Media Protection and Control* by performing the [redacted] backups on a regular basis. When performing [redacted] backups, FEMA should:
		  ◦ Maintain a documented backup inventory for [redacted],
		  ◦ Rotate [redacted] backups off-site to the Virginia NPSC on a regular basis,
		  ◦ Log the deposit and withdrawal of [redacted] backup tapes is maintained, and
		  ◦ Ensure that logs are maintained per the stated retention time period.
		
		• Complete its efforts to implement the [redacted] "real-time" back-up facility as its alternate processing site. Ensure that redundant servers are created at the [redacted] for the [redacted]
			X		**High**

FEMA-IT-07-15	[redacted] 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 form and that it does not fully identify the configuration management process of [redacted].	• Finalize the [redacted] Configuration Management Plan to be in compliance with DHS 4300A. • Finalize and implement the Supplemental Security Policy to the DHS 4300A and 4300B.	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• We determined that FEMA created the Supplemental Security Policy to the DHS 4300A and 4300B, 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.	• Implement the *Database Administration Access Procedures* and [redacted] patch management procedures.			
FEMA-IT-07-16	• FEMA created the Supplemental Security Policy to the DHS 4300A and 4300B, 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.	• Finalize and implement the Supplemental Security Policy to the DHS 4300A and 4300B. • Develop and implement specific procedures for restricting access to [redacted] system software, and promulgate it to all needed personnel, to be in compliance with DHS 4300A.	**X**		**Medium**
FEMA-IT-07-17	• We determined that FEMA created a System Change Request Standard Operating Procedures (SOP) for [redacted]. However, the System Change Request SOP was approved by the OCFO on	Implement the System Change Request SOP by keeping the [redacted]" account locked at all times, except when a change needs to be deployed in the [redacted] production environment, and by monitoring the "[redacted] directory and sub-directories to	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	June 29, 2007. Furthermore, we noted the evidence that the [redacted]" account was locked within the UNIX environment on July 24, 2007. Therefore, we noted that the risk was present for a majority of the fiscal year.	detect updates.			
FEMA-IT-07-18	• FEMA created the Supplemental Security Policy to the DHS 4300A and 4300B 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]	• Finalize and implement the Supplemental Security Policy to the DHS 4300A and 4300B. • Develop and implement specific procedures for the review of suspicious system software activity and access controls for [redacted], and promulgate it to all needed personnel.	**X**		**Medium**
FEMA-IT-07-19	• FEMA created the Supplemental Security Policy to the DHS 4300A and 4300B 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 draft form. • FEMA has not documented procedures to monitor and review sensitive access, system software utilities and suspicious system software and access activities	• Finalize and implement the Supplemental Security Policy to the DHS 4300A and 4300B, • Develop and implement specific procedures to monitor sensitive access and system software utilities for [redacted] and promulgate it to all needed personnel, and • Develop and implement specific procedures to review suspicious system software and access activities for [redacted], and promulgate it to all needed personnel.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	for [redacted]				
FEMA-IT-07-20	FEMA has adopted the DHS SDLC Version 0.5.1 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.	Implement the DHS SDLC for [redacted] program development when DHS finalizes the document. Additionally, FEMA should ensure that the SDLC methodology is promulgated to all personnel involved in the design, development, and implementation process.		**X**	**High**
FEMA-IT-07-21	FEMA has adopted the DHS SDLC Version 0.5.1 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.	Implement the DHS SDLC for [redacted] program development when DHS finalizes the document. Additionally, FEMA should ensure that the SDLC methodology is promulgated to all personnel involved in the design, development, and implementation process.		**X**	**High**
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] has redundant servers in place for the [redacted] Oracle Database effective as of June 2007.	FEMA should complete its efforts to implement the [redacted] "real-time" back-up facility as its alternate processing site. Ensure that redundant servers are created at the [redacted] for the [redacted]	**X**		**High**
FEMA-IT-07-23	FEMA lacks [redacted] backup testing procedures. Additionally, we determined that the [redacted] backups are not periodically tested.	• Develop and implement procedures to periodically test the [redacted] backups in compliance with DHS Information Technology Security Program Publication	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		4300A. • Periodically test [redacted] backups at least annually in compliance with DHS 4300A.			
FEMA-IT-07-24	FEMA lacks [redacted] backup testing procedures. Additionally, we determined that the [redacted] backups are not periodically tested.	• Develop and implement procedures to periodically test the [redacted] backups in compliance with DHS 4300A. • Periodically test [redacted] backups at least annually in compliance with DHS 4300A.	**X**		**High**
FEMA-IT-07-25	We noted that the [redacted] contingency plan has not been tested on an annual basis, per DHS 4300A.	Perform an annual test of the [redacted] Contingency Plan, which covers all critical phases of the plan.	**X**		**High**
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 action and removed the individual's access rights.	Develop a process to review user access for the approval of [redacted] system change requests to determine if access is needed.	**X**		**Medium**
FEMA-IT-07-27	We noted that testing documentation for [redacted] application level changes are not consistently documented or performed	• Ensure all [redacted] application level changes are tested in a timely fashion.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	timely.	• Ensure all test data and transactions are appropriately documented and maintained with the respective system change request within the system, per the [redacted] *Configuration Management Plan*.			
FEMA-IT-07-28	Per DHS 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.	• Ensure all [redacted] application level changes are tested. • Ensure all test data and transactions are appropriately documented and maintained with the respective system change request within the system.	**X**		**Medium**
FEMA-IT-07-29	We noted that the Technical Review Committee (TRC) 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 TRC approval.	Ensure all [redacted] application level emergency changes obtain TRC approval prior to being implemented into the production environment.	**X**		**Medium**
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] 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.	Implement a solution to limit the excessive access to make offline changes to the general ledger account tables. Access rights should be periodically reevaluated and limited to people who have a business need.	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FEMA-IT-07-31	• [redacted] does not timeout after a period of inactivity. Additionally, we determined that all NFIP workstations use a password protected screensaver after fifteen (15) minutes of inactivity, which is not in compliance with DHS 4300A. • [redacted] access is not reviewed on a periodic basis to determine if access is valid and commensurate with job responsibilities.	• Configure the domain level inactivity threshold of the password protected screensaver to five (5) minutes to be in compliance with DHS 4300A. • Develop and implement policies and procedures regarding periodic review of [redacted] access lists in order to determine whether logical user access is valid, consistent with job responsibilities, and in accordance with the principle of least privilege.		**X**	**Medium**
FEMA-IT-07-32	• While a standard form has been developed for documenting [redacted] change requests, [redacted] 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.	• Document the change management procedures for [redacted] • Develop and implement change management procedures over system software changes and establish documented approvals prior to installing or upgrading system software.		**X**	**Medium**
FEMA-IT-07-33	[redacted] has made improvements in the area of Administrator account management. However, we noted that system activity logs are not being reviewed.	Ensure that CSC develop and implement procedures for reviewing [redacted] LAN system logs on a monthly basis. The procedures should include investigation of suspicious activity or suspected violations and reporting findings to appropriate officials.	**X**		**Low**
FEMA-IT-07-	[redacted] has updated the [redacted] mainframe baseline configuration document. However,	Ensure that CSC document and implement change management procedures requiring approvals prior			**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
34	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.	to implementing changes in the production environment.			
FEMA-IT-07-35	A system programmer (user ID [redacted] had write access to the [redacted] datasets of the [redacted] production member. NFIP removed the system programmer's access shortly after this finding was identified.	Ensure that CSC develop and implement procedures to perform a periodic review of access to mainframe production datasets to determine whether access is valid, consistent with job responsibilities, and according to the least privilege principle.	**X**		**Medium**
FEMA-IT-07-36	Access to the Loss Adjustment Expense (LAE) 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.	Ensure that CSC restricts access to the LAE excel files to the Actuary and Finance Director in order to achieve the principle of least privilege.	**X**		**Medium**
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.	• Remove excessive access to the [redacted] application software and support files. • Develop and implement procedures to perform a periodic review of access to [redacted] application software and support files to determine whether access is valid, consistent with job responsibilities, and according to the least privilege principle.	**X**		**Medium**
FEMA-IT-07-38	[redacted] has not documented incompatible duties within [redacted], developed policy and procedures regarding segregation of	• Identify and document incompatible duties, and system roles and responsibilities within [redacted].			**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	duties, or implemented segregation of duties controls within [redacted] All users of [redacted] have full application level access.	• Develop and implement policies and procedures segregating incompatible duties within [redacted], to be in compliance with DHS 4300A. • Identify and implement capabilities within [redacted] that enforce segregation of incompatible duties.			

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] Disaster Recovery and COOP does not identify the following:
	  • The [redacted] and [redacted] alternate processing facility; and
	  • [redacted] critical data files are not documented.
		• Perform a test the [redacted] Contingency Plan, covering all critical phases of the plan on an annual basis.
		• Perform a test of the system fail-over capability at the alternate processing site.
		• Revise the Disaster Recovery and Continuity of Operation Plan to incorporate the [redacted] and [redacted] alternate processing facility and the [redacted] critical data files.
			X		**Medium**

FEMA-IT-07-40	The ROB forms are not consistently signed prior to users gaining access to the [redacted]. Specifically, we determined that three (3) out of a sample of twelve (12) new [redacted] users did not sign the ROB prior to obtaining [redacted] access.	Ensure that CSC require all employees and contractors acknowledge and sign a ROB prior to being granted access to the [redacted].	X		**Medium**
FEMA-IT-07-41	We determined that policies and procedures over periodic review of [redacted] access lists have been documented. However, we noted	Ensure that CSC develop and implement procedures to perform a periodic review of access to mainframe production datasets to determine			**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	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].	whether access is valid, consistent with job responsibilities, and according to the least privilege principle.			
FEMA-IT-07-42	We determined that periodic review policies and procedures have not been developed for access to the [redacted] room. As a result, we noted that there are two (2) employees with excessive access to the [redacted] room.	Ensure that CSC develops and implements policies and procedures to periodically review physical access listings over the [redacted] Room to determine if access is still required or if access levels commensurate with users' job responsibilities.	**X**		**Medium**
FEMA-IT-07-43	The [redacted] has been configured to permit users to reuse prior passwords after five (5) iterations which is not in compliance with the DHS 4300A.	Ensure that CSC configures the [redacted] to require passwords to not be reused until eight (8) iterations have passed to be in compliance with DHS 4300A.	**X**		**Medium**
FEMA-IT-07-44	We noted that proactive vulnerability scanning is not performed over [redacted] backend database or the NFIP Bureau LAN.	Ensure that CSC perform vulnerability scans over the [redacted] backend database or the NFIP Bureau LAN on an annual basis.	**X**		**Medium**

Department of Homeland Security
FY2007 Information Technology
Notification of Findings and Recommendations – Detail

- **Consolidated**

Department of Homeland Security
FY2007 Information Technology
Notification of Findings and Recommendations – Detail

Consolidated

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
CONS-IT-07-01	The [redacted] application has not been configured to meet the following password requirements as defined by DHS 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]) SSP: • Passwords must not contain dictionary words pertaining to personnel data (e.g. user's name,	DHS Office of Financial Management (OFM) should coordinate with Treasury to implement the corrective actions to ensure that the [redacted] password configuration meets both DHS and Treasury requirements. For those requirements that cannot be implemented, due to system limitation, implement the use of mitigating controls to reduce the risk associated with weak passwords (i.e., review invalid logon attempts to the system, review audit logs, etc).	**X**		**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	date of birth, address, telephone number, and social security number) • Passwords are not to be reused • Passwords must be composed of upper/lower case and special characters				
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 DHS [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.	• Continuing to enforce the requirements documented within DHS 4300A and the DHS OFM SOP. • Create [redacted] Access Request forms for all new DHS [redacted] users wither they are DHS or Treasury employees/contractors. • Periodically review the audit log of [redacted] accounts created to ensure that no unauthorized accounts have been created.	**X**		**Medium**
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]_SUPER role, which should be limited to one DHS [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, KPMG has determined that the NFR will be reissued in 2007.	No recommendation required as corrective action to address the weakness was performed during the audit period.	**X**		**Medium**
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	No recommendation required as corrective action to address the weakness was performed during the audit period.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	access to only one, the Assistant Branch Chief of the Financial Reporting Branch (FRB).				
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 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.	No recommendation required as corrective action to address the weakness was performed during the audit period.		**X**	**Medium**
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.	DHS OFM should coordinate with Treasury to implement the corrective actions to ensure that the [redacted] password configuration meets both DHS and Treasury requirements. For those requirements that cannot be implemented, due to system limitation, implement the use of mitigating controls to reduce the risk associated with weak passwords (i.e., review invalid logon attempts to the system, review audit logs, etc).	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	• The [redacted] password configuration has not been configured to meet all of the password requirements as defined by DHS 4300A. • The [redacted] password configuration does not meet the service provider's password requirements as outlined in the Treasury FARS SSP or the Treasury Information Technology Security Program Handbook.				
CONS-IT-07-07	Treasury has not established individual accountability within the [redacted] database. Specifically, two DBAs utilize one generic account, TREASDBA, to perform maintenance on the Oracle database that supports the [redacted] application. Additionally, these two DBAs also share the following Oracle accounts: SYS, SYSTEM, and SYSMAN. SYS is the owner of the database and has access to the entire database while SYSTEM and SYSMAN 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.	DHS OFM should independently verify, on an ongoing basis, that Treasury has performed the : • Create separate accounts for each database administrator to allow for individual accountability or implement alternate individual user accountability mechanisms, where technically feasible.	**X**		**Medium**
CONS-IT-07-08	Not Used.				
CONS-IT-07-09	During FY 2007, we noted that access to the UAM module and the DHS_USER_MANAGER 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, and modifying DHS [redacted] user accounts). Two of these six individuals were Treasury personnel who should not be able to modify user accounts belonging to DHS. Additionally, KPMG inspected a log of all DHS [redacted] accounts created between October 1, 2006 and May 11, 2007	DHS OFM should restrict access to the [redacted] UAM module and the DHS_USER_MANAGER group to the FRB Systems Accountant to be in compliance with the OFM SOP and so that the concept of least privilege has been implemented.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	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 UAM 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 UAM module and the DHS_USER_MANAGER group and the OFM SOP only notes the FRB Systems Accountant to be responsible for creating/modifying/deleting accounts within [redacted].				
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. See the NFR for the specifics on the discrepancies identified.	DHS OFM should update the DHS Component Guide and the [redacted] Specification Table so that they are consistent with each other. Additionally, continue to update the guidance to ensure consistency with the analytics performed by [redacted]	**X**		**Medium**
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. • [redacted] TIER 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 software change requests (SCR)	• Maintain supporting documentation for each change. At a minimum, the following documentation should be maintained for each change: change request, change request approval, evidence of testing, final approval. • Modify the DHS OFM SOP to include procedures to notify components of changes made to the system and to include procedures for handling emergency changes. • Independently verify that Treasury is following the change control process as required and maintaining	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	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 SCRs selected for testing. • Two of five changes selected for testing were not approved by the Department of the Chief Financial Officer Team Lead, as required. • Four of five SCRs selected for testing were missing the Development SCR; 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 OFM SOP 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 SOP do not include procedures for handing emergency changes to the system.	supporting documentation for each change.			
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	• Maintain supporting documentation for each change. At a minimum, the following documentation should be maintained for each change: change request, change request approval, evidence of testing, final approval. • Modify the DHS OFM SOP to include procedures to notify components of changes made to the	**X**		**Medium**

	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 SOP 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 SOP do not include procedures for handing emergency changes to the system.	system and to include procedures for handling emergency changes. • Independently verify that Treasury is following the change control process as required and maintaining supporting documentation for each change.			

Department of Homeland Security
FY2007 Information Technology
Notification of Findings and Recommendations - Detail

- **Federal Law Enforcement and Training Center**

Department of Homeland Security
FY2007 Information Technology
Notification of Findings and Recommendations – Detail

Federal Law Enforcement and Training Center (FLETC)

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-07-01	• The Change Control and Configuration Management SOP for all preventative maintenance and patch management over [redacted] is currently in draft form. Additionally, the Change Control and Configuration Management SOP 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, "FTC\Domain Users" 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.	• Develop and implement test plan standards and procedures into the Change Control and Configuration Management – SOP. • Finalize, approve and implement the Change Control and Configuration Management – SOP. • Develop and implement policies and procedures over the configuration management process for [redacted] application level changes. • 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-07-02	• The Change Control and Configuration Management SOP for all preventative maintenance and patch management over [redacted] is currently in draft form. Additionally, the Change Control and Configuration Management SOP 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. • All FLETC domain level users inappropriately have modify, read, execute, and write access to the [redacted] support files.	• Develop and implement test plan standards and procedures into the Change Control and Configuration Management – SOP. • Finalize, approve, and implement the Change Control and Configuration Management – SOP. • Continue with their projected plan for decommissioning the [redacted] application. Additionally, 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-07-03	The installation of [redacted] system software is not currently logged or reviewed by FLETC management.	Upon implementation of the [redacted], 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-07-04	The SDLC for [redacted] is currently in draft form.	• 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. • Ensure that the SDLC methodology is promulgated to all personnel involved in the design, development, and implementation process of the SDLC methodology.		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-07-05	• [redacted] server level and [redacted] are not periodically tested. • Procedures or a testing schedule are not in place for [redacted] server level and Oracle database backups.	• Develop and implement procedures to periodically test the [redacted] in compliance with DHS 4300A. • Periodically test the [redacted] at least annually in compliance with DHS 4300A.		**X**	**Medium**
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.	• 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-07-07	• FLETC Computer Security Operations Center and Computer Security Incident Response Capability SOP, is currently in draft form. • We noted that incidents are not tracked from inception to resolution in an incident response management system.	• Finalize and implement the FLETC Computer Security Operations Center and Computer Security Incident Response Capability SOP to establish procedures are incident response management. • Establish and implement an incident response tracking mechanism to be in compliance with compliance with DHS 4300A.		**X**	**Medium**
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.	• Continue with their projected plan for decommissioning the [redacted] application. • Develop and implement policies and procedures that segregate the documented incompatible duties over [redacted]		**X**	**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
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.	• Document access procedures within the [redacted] Access SOP, including the use of a user authorization form. • Finalize and implement the [redacted] Access SOP. • 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-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. • We found that termination SOPs for [redacted] are currently under development. • [redacted] does not require passwords to contain a combination of upper and lower case letters and special characters.	[redacted] Continue with their projected plan for decommissioning the [redacted] application. Additionally, develop and implement [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. • Continue to develop, finalize and implement SOPs over the removal of terminated and transferred [redacted] and [redacted] users. • 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 DHS 4300A.		**X** **Medium**	
FLETC-IT-07-11	We determined that the FLETC Directive (FD) 43220: IT System Security Awareness and Training is in draft form.	Ensure that the "FD 43220: IT System Security Awareness and Training" is finalized, and enforced by having all new and existing FLETC users and contractors complete the training by May 31 of each year.		**X**	**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
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.	Finalize and implement "FM 4300: Information Technology System Security Program and Policy," which provides policies and procedures over the authorization and use of mobile code technologies.		**X**	**Low**
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.	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-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 Logical Access Controls - SOP, which is currently 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. • Finalize and implement the "Logical Access Controls – SOP," which provides procedures for restricting access to privileged and sensitive access including [redacted] system software.		**X**	**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
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 – SOP", which 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] • Finalize and implement the "Logical Access Controls – SOP," which provides procedures for the segregation of duties in [redacted]		**X**	**Low**
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 SOP is currently in draft form. • The [redacted] hardening guide and SOP are currently in development and not finalized. • We determined that FLETC has not completed a security assessment of the [redacted] installation.	• Finalize and implement the "FM 4300: Information Technology System Security Program and Policy," which provides policies for the use of [redacted] technologies. • Finalize and implement the [redacted] hardening guide and hardening SOP. • Conduct a security inspection of the [redacted] installations by completing the FLETC [redacted] Security Checklist.		**X**	**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
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.	• Perform timely background checks on all new and existing contractors and ensure that supporting documentation be maintained. • Document the status of ongoing and completed background checks in a central repository with critical details about the investigation documented, such as: date investigation was initiated or adjudicated, the type of investigation initiated or adjudicated, risk level of Contractors role, and current status of investigation.		**X**	**Medium**
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] application on an level.	• Finalize and implement "FM 4300: Information Technology System Security Program and Policy," which provides policies for the review of audit logs. • Continue with their projected plan for decommissioning the [redacted] application. Additionally, ensure that audit logs are maintained to capture actual or attempted unauthorized, unusual or sensitive application or operating system level access to [redacted].		**X**	**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
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 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.	This NFR will be issued without a recommendation as it was remediated during the audit period.	**X**		**Low**
FLETC-IT-07-20	We noted that the FLETC [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 4300A.	Configure the FLETC domain level inactivity threshold of the password protected screensaver to five (5) minutes to be in compliance with DHS 4300A.	**X**		**Low**
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 form.	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-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.	• Continue with their projected plan for decommissioning the [redacted] application and ensure that user access violation information is maintained at the [redacted] application level. • Ensure that [redacted] user access is only granted upon completion of a formal [redacted] User Access Control Form, and evidence of supervisory authorization. In addition, the access request forms should be retained for at least one year. • Configure [redacted] to permit users to reuse prior passwords after eight (8) iterations.	**X**		**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
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.	• Perform a recertification of all [redacted] user access and validating the existing [redacted] user access of individuals who stated they still need [redacted] access. • Remove [redacted] user access that is no longer needed. • Develop and implement procedures around the recertification of all [redacted] user access on an annual basis including verifying the access privileges granted to federal employees and contractors.	**X**		**Low**
FLETC-IT-07-24	We noted that copies of the [redacted] Contingency Plan are not securely stored off-site at the alternate processing facility.	Ensure that several updated copies of the [redacted] Contingency Plan is located at the [redacted] for use by contingency staff.	**X**		**Low**
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.	• Finalize and implement the FLETC SOP - Anti-Virus Software for Servers. • Finalize and implement the FLETC SOP - System Maintenance Policy and Procedures.	**X**		**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-07-26	During technical testing, configuration management weaknesses were identified on hosts and databases supporting the General Support System [redacted] applications.	• 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**
FLETC-IT-07-27	During technical testing, patch management weaknesses were identified on hosts and databases supporting the General Support System 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.	• 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-07-28	We noted that [redacted] server backup tape rotation logs are not consistently maintained.	Consistently complete and maintain backup tape rotation logs for [redacted] server backups.	**X**		**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
FLETC-IT-07-29	• We noted that [redacted] server level and [redacted] are not periodically tested. • We noted that procedures or a testing schedule are not in place for [redacted] server level and [redacted]	• Continue with the projected plan for decommissioning the [redacted] application. Develop and implement procedures to periodically test the [redacted] and [redacted] in compliance with DHS 4300A. • Periodically test the [redacted] server level and database backups at least annually in compliance with DHS 4300A.	**X**		**Medium**

Department of Homeland Security
FY2007 Information Technology
Notification of Findings and Recommendations – Detail

- **Transportation Security Administration**

Department of Homeland Security
FY2007 Information Technology
Notification of Findings and Recommendations – Detail

Transportation Security Administration

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT 07-01	The DRBC is in draft form and has not been tested for [redacted]. Additionally, FINCEN has drafted a MOU with the [redacted] for reciprocal services; however, the MOU is currently in draft form.	TSA ensure that [redacted] complete the following: • Finalize and implement the COOP and ensure that it addresses disaster recovery procedures for [redacted]. • Finalize the MOU with the [redacted] and document associated restoration procedures so that the [redacted] can serve as an alternate processing site in the event that the finance center is unavailable. • Periodically test the COOP and evaluate the results of the testwork so that the COOP can be adjusted to correct any deficiencies identified during testing.	X		Medium

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-02	The DRBC is in draft form and has not been tested for the Sunflower Application. Additionally, [redacted] has drafted a MOU with the [redacted] for reciprocal services; however, the MOU is currently in draft form.	TSA ensure that [redacted] complete the following: • Finalize and implement the COOP ensuring it addresses disaster recovery procedures for Sunflower as well as testing the COOP periodically, evaluating the results of the test work so the COOP can be adjusted to correct any deficiencies identified during testing. • Finalize the MOU with the [redacted] and document associated restoration procedures so that the [redacted] can serve as an alternate processing site in the event that the finance center is unavailable.	**X**		**Medium**
TSA-IT-07-03	The contract that 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.	TSA should ensure that CG reevaluates and revises the contract between CG and their software vendor or otherwise ensure that the security configurations associated with the builds, service packs, and software patches are in compliance with DHS and NIST standards for [redacted].	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-04	Although [redacted] has developed re-entry procedures, continued to limit entry into the data center and created a curriculum that must be completed annually by data center staff, weakness were noted in the process. Specifically, we determined that 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 KPMG with supporting evidence.	We recommend that TSA monitor [redacted]'s efforts to implement corrective action to ensure that all personnel with access to the data center have completed the data center emergency response training.	**X**		**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-05	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 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 should monitor CG's completion of the following corrective actions: • Implement procedures to ensure compliance with DHS policies for the background investigations of contracting personnel, such as DHS 4300A. • Ensure that all contracts procured by CG HQ, include the appropriate suitability designation for contracting personnel working on the contract and require completion of suitability checks specific to the position risk level prior to beginning work at CG. Additionally, ensure that all current contracts are updated with the required language. • Provide resources to CG Components to fully implement the developed procedures.	**X**		**High**
TSA-IT-07-06	CG IT Security Awareness Policies and Procedures lack 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 should monitor CG's completion of the following corrective actions: • Enhance current policies and procedures for IT role based training to require those with critical security responsibilities, such as network administrators, system administrators, senior managers and system owners, to complete the role based training on an annual basis. • Deploy the IT role-based training of civilian personnel with critical IT positions down to the CG component levels for implementation.	**X**		**Low**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-07	The following access control weakness surrounding [redacted] were identified: • TSA management did not receive a response from the 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 response was received. • Privileges associated with each user were not included in the May and July 2007 reviews performed. Additionally, 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 should complete the following: • Update the [redacted] policies and procedures to require that the privileges associated with each [redacted] user be included in each [redacted] access review. • Update the [redacted] policies and procedures to include steps to be followed in the event that a region or a division (such as FAMS) does not respond to the [redacted] access review request. • Notify and coordinate with [redacted] to implement the corrective actions that result from the [redacted] review, such as removing separated users from the system or modifying account privileges in a timely manner and in accordance with DHS guidance.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
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 DHS 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.	TSA should monitor [redacted]'s completion of the following: • Ensure that the [redacted] password configuration meets DHS requirements. For those requirements that cannot be implemented, due to system limitation, implement the use of mitigating controls to reduce the risk associated with weak passwords • Remove/end-date/disable the accounts of terminated individuals, both employees and contractors, from the system immediately upon their departure. • Develop and implement access control procedures for the [redacted] system and database accounts. These procedures should include, at a minimum, parties involved in the review, steps for reviewing the system and database user listings to ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked, and that privileges associated with each individual are still authorized and necessary.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
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.	TSA should monitor CG's completion of the following: • Configure the [redacted] password configuration to be in compliance with DHS guidance. For those requirements that cannot be implemented, due to system limitation, implement the use of mitigating controls to reduce the risk associated with weak passwords (i.e., review invalid logon attempts to the system, review audit logs, etc). • Configure the system to track and lock inactive [redacted] accounts in compliance with DHS requirements.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-10	An excessive number of individuals had user administration capabilities within [redacted] until the implementation of the centralized user management. Specifically, 78 individuals had [redacted] account management capabilities within the system. The privileges associated with these accounts permitted the user to create/delete/modify [redacted] user accounts for all of TSA including sites/locations that he/she was not responsible for. Thirteen of these accounts were end-dated (disabled) throughout the FY 2007 period; however, many of these individuals are part of the Financial Systems Branch and should not have such capabilities within the system. [redacted] became responsible for account creation/deletion/modification when the centralized user management was implemented. This effort reduced the number of individuals with account management capabilities to 16. However, we also noted the existence of two shared generic accounts with this privilege: [redacted] and [redacted]. These accounts have every privilege within the application, including the ability to create/delete/modify user accounts within [redacted].	TSA should monitor the following corrective action for [redacted]: • Remove all generic shared system accounts or establish individual accountability for these accounts. If these accounts cannot be removed, enable audit logging to capture the user's operating system logon ID so that individual accountability can be established for each instance of when these accounts are used. No recommendation required for the [redacted] excessive administrator access that existed from October 1, 2006 through August 19, 2007 as this weakness was remediated with the implementation of centralized user management.	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
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.	TSA should complete the following: • Immediately notify and coordinate with [redacted] when an employee or contractor separates from TSA so that his/her [redacted] account can be end-dated/disabled in a timely manner. • Modify the [redacted] Site Administrator Review Procedures to include, steps for reviewing the application and database user listings to ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked and that the privileges associated with each individual are still authorized and necessary. The procedures should note the parties that should be involved in the review process, the supporting documentation that should be retained, and procedures to notify [redacted] of corrective action that needs to be taken as a result of the review. • Complete an AAR or a Financial Systems Access Request Form for each individual requesting access to the [redacted] application or database.	X		Medium
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.	TSA should complete the following: • Develop and implement access control policies and procedures for the periodic review of [redacted] application and database accounts for TSA users. These procedures should include, at a minimum, the parties involved, steps for reviewing the application and database user listings to ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked and that the privileges associated with each	X		Medium

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		individual are still authorized and necessary. • Retain supporting documentation associated with the review • Notify and coordinate with the [redacted] to implement the corrective actions that result from the review, such as removing separated users from the system or modifying account privileges.			
TSA-IT-07-13	[redacted] had not adequately completed the [redacted] C&A package to include the Sunflower system. Specifically [redacted] management stated that Sunflower is a subsystem of [redacted] and a separate C&A does not need to be completed since it is covered by the CAS C&A Package. However, we determined that there is no documentation within the [redacted] SSP that defines Sunflower as a subsystem and specifically addresses the appropriate security controls for Sunflower in this capacity.	TSA should monitor [redacted] completion of the following corrective actions: • Further define and justify the classification of Sunflower as a subsystem to [redacted] in accordance to NIST guidance. • Once recommendation one is complete, update the [redacted] C&A package to include that each subsystem component is fully described in the system security plan, an appropriate security categorization is assigned, and an appropriate set of security controls are identified in accordance with NIST guidance.	X		Medium
TSA-IT-07-14	[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.	TSA should monitor [redacted]'s efforts to track and end-date/disable [redacted] accounts in compliance with DHS requirements.	X		Low
TSA-IT-07-15	TSA sanctioning policies and procedures have not been fully developed and implemented to include consequences for individuals who do not sign the computer access agreements or complete initial or refresher security awareness training. Additionally, we determined that TSA allows individuals to complete security awareness training within sixty days of beginning work and gaining access to their LAN	TSA should perform the following corrective action: • Review and revise the current TSA policies and procedures for the on-boarding of both contractors and TSA employees according to DHS 4300A and NIST guidance. • Continue to develop and implement the policies and procedures for the	X		Low

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	and application accounts. However DHS guidance requires that all individuals complete security awareness training prior to gaining access to the Information systems. Furthermore, security awareness training and Computer Access Agreements are not consistently completed.	requirements surrounding the completion of security awareness and training, and computer access agreements for both TSA employees and contractors. • Address the weakness surrounding the development and implementation of a sanctioning process for both TSA employees and contractors if these requirements are not met.			
TSA-IT-07-16	Procedures are not formally documented requiring the review of the activities of the Linux system administrators. We also noted that reviews of the audit logs that document the actions of Linux administrators in the [redacted] operating environment are not being performed.	TSA should monitor [redacted]'s completion of the development and implementation of detailed procedures requiring the periodic review of Linux audit logs for unauthorized and suspicious activity as well as the performance of periodic audit log reviews of the Linux operating system.	**X**		**Medium**
TSA-IT-07-017	Procedures are not formally documented identifying how change control should be performed when applying system software changes, including software patches, to the Linux operating system according to a standard schedule or in an emergency situation.	TSA should monitor [redacted]'s efforts to develop and implement detailed procedures for the performance of standard and emergency system software change controls for the Linux operating environment.	**X**		**Medium**
TSA-IT-07-18	Technical testing identified patch management weaknesses on hosts supporting the [redacted] and [redacted] applications which could allow for a remote attacker to gain full control of the affected host and could lead to the compromise of the availability, confidentiality and integrity of [redacted] data.	TSA should monitor [redacted]'s completion of corrective actions surrounding the vulnerabilities identified and implement policies and procedures to ensure that the software builds created by the CG software developer are tested, prior to implementation, to ensure that all software security configurations, such as software patches and non-compliant settings, are up to date.	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-19	Technical testing identified configuration management weaknesses on hosts supporting the [redacted] applications. Specifically, servers were identified with excessive access privileges, and password and auditing configuration weaknesses.	TSA should monitor [redacted]'s completion of corrective actions surrounding the vulnerabilities identified and implement policies and procedures to ensure that the software builds created by the CG software developer are tested, prior to implementation, to ensure that all software security configurations, such as software patches and non-compliant settings, are up to date.	**X**		**High**
TSA-IT-07-20	The IT off-boarding process for Non-Screeners and Contractors, is not consistently completed for terminated personnel. 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.	TSA should review the current policies and procedures for the exit process of both TSA contractors and employees and develop corrective action plans to remediate the identified weaknesses according to DHS 4300A and NIST guidance.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-21	The following weaknesses were identified in the TSA [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 TSA and [redacted] or guidance for ensuring that changes that are 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] changes • Policies and procedures for the emergency change control process are not documented.	TSA should complete the following: • Continue to develop and implement a more detailed change control policy and procedure to formally define the TSA change control to include different roles and responsibilities that personnel within TSA must complete and include instructions for the monitoring [redacted]. • Develop and implement policies and procedures to specifically address the documentation of the testing performed in different phases of testing as well as testing performed by [redacted]. • Continue to develop and implement a formalized process for the retention of documentation. • Ensure that the policies and procedures developed include the emergency change control process for [redacted].	X		High

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-22	Policies and procedures for the overall change control process surrounding [redacted] and [redacted] changes and emergency changes are inadequate. Specifically procedures detail the overall process and phases for [redacted] and [redacted] change control, but lack detailed guidance for the roles and responsibilities executed by [redacted] personnel and do not address emergency changes. Additionally, [redacted] is not consistently retaining documentation to support the change control and emergency change control process.	TSA should monitor [redacted]'s completion of the following: • Continue to develop and implement a more detailed change control policy and procedure to formally define the change control process for [redacted] to include the different roles and responsibilities that personnel within CG-[redacted] must complete. Additionally, ensure that the policies and procedures developed include the emergency change control. • Develop and implement policies and procedures to specifically address initial approvals of the changes proposed by the software vendor, including technical changes, testing involved, and additional testing performed by [redacted]. • Continue to develop and implement a formalized process for the retention of documentation throughout the change control process.	**X**		**High**
TSA-IT-07-23	CG has and continues to operate a separate, informal and largely undocumented change development and implementation process effecting CG Financial Systems, outside of and conflicting with the formal change control process. This informal script development and implementation process began with the implementation of [redacted] in June of 2003. [redacted] reports that the documentation and tracking of the scripts was not developed until June of 2005 but is unable to provide a complete population of implemented scripts, to include the type, purpose and intended	TSA should monitor CG's completion of the following: • Immediately implement a single, integrated change control process over CG Financial Systems with appropriate internal controls to in include clear lines of authority to CG financial management personnel, enforced responsibilities of all participants in the process and documentation requirements • Continue with plans to further commence an in depth examination of the CG Financial Systems with an external	**X**		**High**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	effect on financial data. The implemented process is ineffective as the approval, testing and documentation procedures of the script changes are not appropriately designed and the current process is ineffective to control the intended and actual effect on financial data.	independent organization trained in financial information systems, process analysis and with a demonstrated understanding of the federal accounting environment to determine the root causes and specific, detailed actions necessary to correct the conditions that caused scripts as well as manual adjustments to be implemented. CG's root cause analysis needs to specifically determined if the causes are process or system driven to determine the appropriate corrective actions. • In conjunction with item number two above, begin an in depth examination to determine and document, in detail, the effects of the identified root causes and implemented automated and manual adjustments on financial data and affected financial statements for prior reporting periods and make appropriate restatements, if necessary.			
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 MBI per DHS 4300A. Additionally, 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 should monitor CG's completion of performing initial background investigations and reinvestigations for civilian employees in accordance with DHS directives.	**X**		**Medium**

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
TSA-IT-07-25	TSA has not documented policies and procedures surrounding the change control process for [redacted], formalized a tracking process of its own change requests submitted to [redacted], or retained documentation associated with the requests (i.e., initial approvals, testing and final approvals). Additionally, KPMG noted that testing was not fully completed by TSA prior to passing the change for testing for three of the changes.	TSA should complete the following: • Develop and implement a more detailed change control policy and procedure to formally define the change control process for [redacted]. This documentation should detail the different roles and responsibilities that personnel within TSA Property Division must complete. • Develop and implement policies and procedures to specifically address initial approvals of the changes proposed by the software vendor, including technical changes, testing involved, and additional testing performed by [redacted]. • Develop and implement a formalized process for the retention of documentation throughout the change control process for [redacted]. • Ensure that the policies and procedures developed include the emergency change control process for [redacted]. • Ensure that all changes are fully tested and have passed prior to approving the change.	**X**		**High**

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, 2007

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
CIS	06-01	The [redacted] has not defined or documented the appropriate user permissions for the various roles granted to [redacted].		**07-01**
CIS	06-02	NBC does not perform periodic [redacted] user access reviews to ensure that users' level of access remains appropriate.		**07-02**
CIS	06-03	Management at the CIS [redacted] has not completed or inadequately completed access forms for [redacted] and [redacted] system users.		**07-03**
CIS	06-04	Access control weaknesses such as account management, password length, and a lack of review over audit records were identified for the [redacted] system.	**X**	
ICE	06-01	ICE OCIO management has not defined or documented a formal plan to monitor security control compliance of third party providers of [redacted] services.	**X**	
ICE	06-02	The [redacted] System Security Plan does not include procedures for distributing, maintaining, or tracking a user's signed ROB document. Additionally, not all [redacted] users have signed the current ROB document reflecting DHS policies and procedures.	**X**	
ICE	06-03	At the time our procedures were performed, OCIO Management had not reviewed and updated the list of ICE users with wireless access. Several wireless broadband cards were issued to ICE users, but the OCIO was unaware of who the users are or where they are located.	**X**	
ICE	06-04	ICE network traffic for the [redacted] client/server application does not pass through the ICE firewall, but rather goes directly to the ICE router at the [redacted]) and then is handed off to [redacted]	**X**	
ICE	06-05	Users are not locked out of [redacted] or the ICE Network after 20 minutes of inactivity.	**X**	
ICE	06-06	The [redacted] security audit log for the mainframe system housing the [redacted] databases can be modified by the [redacted] Security Administrator.	**X**	
ICE	06-07	ICE CIO has not completed and authorized remote access forms for two of the five ICE users we selected for testing.	**X**	
ICE	06-08	Two of the five [redacted] users we selected for testing have two accounts (eg - Jsmith, Jsmith1, same person with 2 accounts), but only one access form on file.		**07-01**
ICE	06-09	User profiles are not properly segregated within [redacted]. We noted the following: • 3 users can enter, approve, and make payments; • 157 users can create obligations and payments; and • 7 contractors have access to the Desk Approving Official and Desk Funding Official profiles.	**X**	

Department of Homeland Security
Information Technology Management Letter
September 30, 2007

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
ICE	06-10	User profiles have not been updated across all instances of [redacted] for the entities in which ICE, OFM provides accounting services to address the principles of least privilege and separation of duties.	**X**	
MGT	06-01	During our testing we noted that the user account for an individual who separated from MGT on May 24, 2006 had not been removed from [redacted] as of September 8, 2006. Although the user account was made inactive in [redacted]S upon the employee's departure, the inactive account was not removed from [redacted].	**X**	
CBP	06-01	Due to the design of [redacted], certain controls can be 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.		**07-01**
CBP	06-02	CBP management has not established ISAs for legacy connections with [redacted]. Additionally, the majority of financial institutions connecting with [redacted] do not have ISAs.		**07-02**
CBP	06-03	CBP management has not performed a formal certification and accreditation on the [redacted] as a whole. Specifically, a formal security control assessment and a formal risk assessment have not been performed for components of the [redacted].	**X**	
CBP	06-04	CBP does not maintain a centralized listing of separated contract personnel. The only method CBP employs to track terminated contractors is the use of a report of users that had their mainframe account deleted.		**07-03**
CBP	06-05	CBP management has not performed a formal review of individuals with physical access to the data center. Additionally, CBP management has not established formal procedures for revoking physical access to [redacted] buildings.		**07-10**
CBP	06-06	CBP has not performed a separate certification and accreditation for the applications remaining in the seven business process areas defined in the Administrative Applications C&A.	**X**	
CBP	06-07	[redacted] does not have an automated mechanism to detect and deactivate users that have not logged on for 90 days per DHS policy.	**X**	
CBP	06-08	Field offices are not consistently reporting the completion of [redacted] re-certifications at their ports to the OFO HQ. Email confirmation of completion of [redacted] re-certifications were not available for [redacted] office only provided an email stating that re-certification process exists, but did not confirm that [redacted] re-certifications had been completed.		**07-24**

Department of Homeland Security
Information Technology Management Letter
September 30, 2007

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
CBP	06-09	We could not obtain the requested evidence of [redacted] recertifications from CBP for any of the 44 selected field level ports to determine whether [redacted] accounts with sensitive and high-risk combination of functions are reviewed for appropriateness.		**07-31**
CBP	06-10	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. Specifically, we noted the following issues: • [redacted] will not be installed on all workstations for the majority of the fiscal year. • 3 of 8 selected system flaw notifications did not have an associated Service Center ticket.		**07-12**
CBP	06-11	We noted that the process for deletion of [redacted] accounts for terminated government and contractor personnel may be utilizing erroneous data. Specifically, we noted that the files being sent from the Mainframe Security group to the [redacted] Security team to terminate [redacted] accounts of separated employees do not display the true status of employees. The mainframe query producing the separated contractor file includes individuals with Mainframe accounts that have been locked after 30 days of inactivity. Additionally, the separated government employees file is not accurate due to the fact that many government employees are separated and return to CBP as contractors. Consequently, the [redacted] Security Group does not deactivate the accounts for these instances.	**X**	
CBP	06-12	We noted that 24 out of 45 selected individuals did not have formally documented VPN access authorization forms. Additionally, CBP has not implemented formal procedures for VPN recertification for the majority of FY 2006.		**07-20**
CBP	06-13	CBP System Security does not conduct reviews of powerful system utilities. Specifically, the utilities [redacted] for [redacted] are not reviewed by management.		**07-17**
CBP	06-14	Multiple methods of termination of [redacted] accounts are used by Systems Security personnel (i.e. electronic mail, phone calls, and termination checklists). We selected 45 terminated employees to determine whether termination checklists had been consistently completed. Of the 45 employees, only 30 forms were provided. Of these 30 forms, we noted that 9 out of 30 forms did not have supervisory signature, which signifies completion of the form to include notification sent to System Security for removal of logical access to applications. We noted that termination checklists (CF-241) are not consistently completed for separating employees throughout the organization.		**07-29**
CBP	06-15	Backup tapes do not have affixed external labels to indicate the sensitivity of the data contained in the tapes.		**07-04**
CBP	06-16	CBP System Security does not have formal policies and procedures in place for monitoring powerful/sensitive system utilities		**07-17**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
CBP	06-17	Improvements still needed in CBP's technical security controls. Related to issues reported in FY02, FY03 and FY04 findings regarding host and network based security system access deficiencies, we noted the following: • CBP has confirmed that they will not be implementing the Passfilt.dll system control program to enforce strong passwords or the Windows NT password protection feature enhancement upgrade referred to as NT [redacted] • CBP has not made the configuration changes to the Windows NT [redacted] Domain Controller that was compromised in FY03 intrusion tests. • Discovered key systems' domains in targeting for potential unauthorized access attempts where we were able to identify major CBP network domains. • Exploited a system vulnerability that had not been corrected. • We confirmed that the number of Domain Administrators on selected Domains has increased since 2005. • Identified weak passwords, expired passwords, misconfigurations, and missing patches. • Identified vulnerabilities on an Oracle database which had critical patches missing, week passwords and auditing is not enabled.		**07-35 and 07-36**
CBP	06-18	We noted the following issues related to password parameters: • [redacted] minimum password length is set to six characters • [redacted] LAN minimum password length is set to six characters • Password complexity is not set on the [redacted] • Password complexity is not set on [redacted] • Password complexity is not set on the [redacted]		**07-05**
CBP	06-19	We noted the following issues related to automatic session disconnection: • CBP's policy states that sessions should be automatically disconnected after 30 minutes of inactivity, which is not consistent with DHS' policy. • CBP's policy states that the workstation should log off from all connections after 5 minutes of inactivity, which is a documentation error. According to applicable guidance, all system connections do not have to be terminated after 5 minutes of inactivity on the workstation. • [redacted] sessions are configured to terminate after 60 minutes of inactivity. • CBP workstations cannot enforce the activation of a password-protected screensaver after 5 minutes of inactivity. The settings		**07-06**

Department of Homeland Security
Information Technology Management Letter
September 30, 2007

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		can be disabled or changed by individual users.		
CBP	06-20	[redacted] is not configured to disable user accounts after 3 consecutive failed logon attempts. Additionally, per observation, we noted [redacted] accounts were not locked after three consecutive failed login attempts.	**X**	
CBP	06-21	CBP does not document formal approval of system changes for the [redacted] system. We selected 8 [redacted] regularly scheduled changes to determine if formal approval was given and documented. Per inspection of documentation, we were informed that there is no formally documented approval for the 8 selected changes.	**X**	
CBP	06-22	We noted weaknesses related to the deposit and withdrawal of backup tapes: • Tape deposit receipts for 2 of 25 selected dates were not available. • Withdrawal of backup tapes from the off-site storage facility is not logged.		**07-14**
CBP	06-23	CBP System Security does not consistently retain audit logs of powerful [redacted] system utilities. Specifically, we selected 25 [redacted] reports to determine if powerful [redacted] system utilities are being consistently logged. We determined that 5 out of the 25 selected logs were missing.		**07-11**
CBP	06-24	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.		**07-07**
CBP	06-25	Accounts are not deactivated after 90 days of inactivity with respect to the [redacted] system. We determined through inspection of audit evidence acquired from [redacted] that the defined deactivation period is, in fact, 180 days.		**07-15**
CBP	06-26	[redacted] Security Administrators do not keep audit logs for the prescribed period of time. Audit logs are only available for, at the most, the past three months. Logs are not maintained beyond the configured space for the log file. We also noted that [redacted] LAN Security Administrators do not review audit logs.		**07-08**
CBP	06-27	We noted that accounts are not deactivated after 90 days of inactivity on the [redacted] LAN. We determined that the removal of inactive [redacted] LAN accounts is a manual process.		**7-09**
CBP	06-28	[redacted] ISAs are not fully documented for [redacted]. The ISA documenting the connection between [redacted] America and CBP is currently out of date. In addition, the connection that exists between Treasury and CBP is currently not officially documented.	**X**	

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
CBP	06-29	The documentation of completed initial security awareness training is not properly maintained. We selected security awareness training documentation for 45 users. Per inspection of documentation, and noted that 13 of 45 did not have security awareness training certificates documented.		**07-19**
CBP	06-30	Contractor access request forms for the [redacted] could not be adequately tested. We noted that no list of contractors hired to work at CBP is maintained, accordingly audit procedures requiring a sample of contractor access request forms could not be requested.		**07-03**
CBP	06-31	[redacted] has excessive access to emergency processing capabilities. We noted that after an initial authorization to be added to an emergency user table in [redacted], a user can repeatedly request that their emergency access be reinstated, without being reauthorized. While emergency access in [redacted] can expire in no more than nine days, some users renew their emergency access every nine days. We noted that CBP has not implemented an effective method of controlling this access, as users are not required to reauthorize their emergency access each time it is requested.		**07-16**
CBP	06-32	Access change audit logs are not reviewed in [redacted] or [redacted]. CBP management does not independently review the changes that are put into place by the [redacted] or [redacted] security administrators.		**07-21**
CBP	06-34	An administrator account on the [redacted] ("CMO [redacted] Administrator") is shared by four [redacted] administrators.	**X**	
CBP	06-36	We determined that the following documents have not been formally approved: • SDLC Configuration Management Plan – No approval • Configuration Management Code Migration Procedures for [redacted] has no authorization • Acquisition Planning and Selection and Development Process has no authorization • Configuration Management Code Migration Procedure for Systems, Applications, and Products has no authorization • Production Management Team Procedures – No approval, no change history • [redacted] Operations: Standard Operating Procedures – No approval	**X**	
CBP	06-37	User acceptance testing for Employee Self Service Solution (ESSS)/Remedy was not formally documented	**X**	
CBP	06-38	We noted that one individual with [redacted] administrator privileges did not have justified access. We noted that there are instances where [redacted] locks security administrator accounts due to various reasons that do not require documented approvals for reinstating the user account. Additionally, we noted that instances where the [redacted] security administrator is new or		**07-22**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		reinstatement of suspended/deleted accounts is needed, a documented approval is required. We noted that due to a system limitation within [redacted], management cannot produce a system-generated list of field [redacted] security administrators that differentiates between the two cases.		
CBP	06-39	We noted that 1 out of 3 selected batch job schedule changes did not have documented approval.	**X**	
CG	06-01	The [redacted] Business Contingency and Disaster Recovery Plan is still in draft form and has not yet been tested.		**07-01**
CG	06-02	A comprehensive incident capability that includes designated response team members and procedures for incident handling to help ensure that the incident is properly handled has not been documented and implemented.	**X**	
CG	06-03	Configuration weaknesses over [redacted] workstations allowed users to modify sensitive workstation system and security settings. During our test work, using a [redacted] network user account provided with ordinary privileges, we were able to successfully: • Disable the desktop's anti-virus; • Change the screen saver setting to remove the password-locking feature; and • Increase the time period for the screen saver activation significantly.	**X**	
CG	06-04	Although backup tapes for [redacted] are created on a regular basis, testing procedures have not been documented in accordance with [redacted] Instruction. Additionally, although [redacted] backup tapes are rotated offsite to the [redacted], GSS backups have not been included in the tape rotation process to the [redacted]. Although a tape rotation schedule and tape rotation procedures have been documented, the tape transfer logs are not being completed in their entirety to note the tape numbers and the number of tapes being rotated offsite.	**X**	
CG	06-05	Although a change control process has been established and documented for [redacted], the process is not consistently followed. The appropriate approvals are not consistently documented within PVCS Tracker prior to implementation. Out of a selection of 30 [redacted] changes, 2 approvals were not documented. Additionally, evidence of testing, either through attached test plans and results or emails were not consistently attached to the selected SCRs within Tracker. As a result, evidence of testing for 7 out of the 30 selected changes were not available.		**07-34**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		Additionally, although criticality levels for [redacted] changes have been defined, procedures for making emergency changes to [redacted] have not been developed.		
CG	06-06	• [redacted] emergency procedures are in place for the evacuation of [redacted] and its Data Center. However, no emergency re-entry procedures exist within this directive. • No policies and procedures are in place to guide and document the emergency training of Data Center personnel. • Weaknesses exist in the implementation of least privilege regarding granting access to the Data Center personnel. Specifically, two out of the fifteen personnel forms selected, granted twenty-four hour access to individuals on the janitorial staff.		**07-09**
CG	06-07	The passwords for [redacted] are not required by the system to be 8 characters in length or contain a combination of alphabetic, numeric and/or special characters. Due to lack of vendor support, there is uncertainty to the feasibility of implementing stronger password controls.		**07-03**
CG	06-08	A periodic review of [redacted] access lists was not conducted to ensure that users had the correct access privileges. Additionally, we determined that an applicant could be entered and hired by the same individual. The process of transitioning an applicant to an employee is in an audit trail; however this audit trail is not reviewed on a regular basis.		**07-20 and 07-29**
CG	06-09	Access authorization requests for [redacted] ids did not indicate the roles or menus necessary for the user to perform job functions; rather access authorizations identified a current user with similar privileges that could be copied to create the privileges for the new [redacted] id. Additionally, requests for new accounts are accomplished via email, and the system administrator did not routinely retain these emails prior to January 2006.		**07-21**
CG	06-10	• Formal documented procedures are not in place over system software changes, related to z/OS, DB2, and [redacted]; • A testing baseline for system software changes has not been established and documented; • [redacted] does not formally document and maintain the following for each system software change: - System software change request and authorization of the request; - Test plan documentation and test results;		**07-05**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		- Approval for migration of system software changes into production; and • The audit trail of system software changes is not periodically reviewed.		
CG	06-11	Test plans and test results for [redacted] application changes were not consistently documented and maintained. Specifically, 28 out of 30 selected application changes did not have test plans or test results documented. In addition, 11 out of 30 changes were not approved by the business sponsor (user acceptance approval) and 4 out of 30 changes were not approved by the peer reviewers prior to migration into production, as required by the [redacted] Systems Development Life Cycle		**07-13**
CG	06-12	[redacted] passwords are not in compliance with the DHS password policy. The [redacted] systems does not enforce the following password rules: • passwords are to be eight characters in length • passwords are to include alphabetic, numeric, and special characters • passwords are not be the same as the previous eight passwords We determined that [redacted] sessions are not timed out following 20 minutes of inactivity and accounts are not disabled following a period of 90 days of inactivity. During our testing of [redacted] accounts with special attributes, we determined that two generic accounts have access to [redacted] and [redacted] Additionally, we determined that the [redacted] settings were not enabled. Furthermore, four accounts assigned to [redacted] personnel had both [redacted], two of which were system programmers.		**07-07** **07-08** **07-11**
CG	06-13	Outgoing Personnel forms were not documented for two out of nine selected users. These two individuals retained access to the [redacted] system with read only access.		**07-04**
CG	06-14	• Excessive access privileges have been granted 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		**07-25**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		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	06-15	Weaknesses were noted in regard to these [redacted] personnel entrance and exit procedures for civilian, contractor and military personnel. Specifically, out of fifteen entrance check-in sheets inspected, thirteen were incomplete or did not exist. Additionally, out of fifteen exit check-out sheets inspected, only four were received from our sample selection, and none of which were complete.	**X**	
CG	06-16	• Password configurations for [redacted] have been not configured to maintain the password history for each account. • Users are not locked out of their [redacted] accounts after three invalid logon attempts. • Policies and procedures for application and database audit log management have not been documented. • Documented access request forms could not be located for three out of nine new [redacted] users granted access to the application. • [redacted] accounts are not immediately disabled upon an employee's termination. Specifically three civilians terminated employment with [redacted]. • [redacted] has not been configured to track and deactivate accounts that have not been used in 90 days. • [redacted] account reviews have not been performed on a periodic basis and results of the reviews are not maintained. • An excessive number of individuals have user administrator capabilities within [redacted].		**07-19**
CG	06-17	• Password configurations for application and database have been configured to permit passwords to be a minimum of six characters in length. • Users are not locked out of their [redacted] application accounts after three invalid logon attempts. • Audit logging has not been enabled within the [redacted] application or database. • Individuals who are no longer employed with [redacted] were		**07-18**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		found to have active accounts within [redacted]. • [redacted] account reviews have not been performed on a periodic basis.		
CG	06-18	• Password configurations for the application and database have been configured to permit passwords to be a minimum of six characters in length • Policies and procedures for application and database audit log management have not been documented. • [redacted] account reviews have not been performed on a periodic basis.		**07-17**
CG	06-19	• Manager Review of System Administration Monitor Procedures have been developed that guide managers in performing periodic system administration monitoring reviews. However, the procedures do not note the periods of review that are being monitored, who is responsible for performing the reviews and evidence that the manager review was performed could only be obtained for March 2006. Additionally, although the manager reviews were implemented in March 2006, for the first half of the fiscal year, October through March, [redacted] system administration monitoring was not performed by a manager or group outside of the three systems administrators during that time period. • The access request form for one out of four individuals granted access to [redacted] since October 1, 2005, did not contain the supervisor's approval. • The account of a contractor that left [redacted] in October 2005 remained active until May 2006.	**X**	
CG	06-20	A [redacted] Security Configuration Management Plan does not exist that clearly delineates the roles and responsibilities between Global Computer Enterprises (GCE), and the [redacted]. GCE is the organization under contract by CG to manage the [redacted] and [redacted] software programs. Consequently, the SSPs for the [redacted] and [redacted] applications do not include key security control information. Specifically, the plans do not include information on the current security configuration management process, including delineation of responsibilities for all involved parties. The SSPs otherwise compliant with current NIST standards.	**X**	
CG	06-21	CG HQ is in the process of developing policy that addresses role-based training requirements for individuals with critical IT positions. However, currently this Training and Education Plan is still in draft		**07-14**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		form and no policies and procedures exist that require critical IT personnel to continue their education through role-based training.		
CG	06-22	National Oceanic and Atmospheric Administration (NOAA) forgotten widows, member type 1384, are not designed to be excluded from the actuarial data file created annually to estimate the pension liability for the CG. Forgotten widows are the survivors of retired personnel who died before any survivor benefit program was enacted. The program is designed to exclude those member types included in the [redacted] group identified in the [redacted] Cobol program, which does not contain member type 1384. All member types not in the [redacted] group are included in the actuarial liability file.	**X**	
CG	06-23	Not used.		
CG	06-24	A security test and evaluation has not been conducted on the [redacted]. In addition, the final Certification and Accreditation package has not been created and an Authorization to Operate has not been requested or approved for the [redacted].	**X**	
CG	06-25	No documentation exists for the change control process, including the emergency changes process, surrounding the [redacted] application. Although a development server exists for the application, [redacted] management indicated that the application version 6.0.13 was the only version implemented for [redacted] in 2003 and no changes or updates have been made since.		**07-02**
CG	06-26	During technical testing patch management weaknesses were identified on hosts supporting the [redacted] applications. Many of these vulnerabilities could allow a remote attacker to gain full control of the affected host and could lead to the compromise of the availability, confidentiality and integrity of [redacted] data.		**07-36**
CG	06-27	During technical testing configuration management weaknesses were identified on hosts supporting the [redacted] applications. Specifically, servers were identified with excessive access privileges, and password and auditing configuration weaknesses.		**07-37**
CG	06-28	• CG has not completed the process of filing the records that were recovered and recreating of the records that were not found during the migration of records from the Department of Transportation to DHS. • Civilian background investigations and reinvestigations are not being consistently performed. Specifically, three (3) out of seven (7) newly hired civilian employees at [redacted] did not have any record of a background investigation on file. Additionally, for the re-investigation of [redacted] employees, four (4) out of five		**07-39** **07-40**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		(5) employees selected did not have a current investigation on file. • Position sensitivity level distinctions for civilian personnel with access to DHS information systems at [redacted] are not accurately depicted. Specifically, of the selection of position descriptions received, nine (9) out of ten (10) had non-critical position sensitivities although their job functions were that of IT personnel with advanced access to the DHS system.		
CG	06-29	CG has and continues to operate a separate, informal and largely undocumented change development and implementation process effecting CG Financial Systems, outside of and conflicting with the formal change control process. This informal script development and implementation process began with the implementation of [redacted] in June of 2003. [redacted] reports that the documentation and tracking of the scripts was not developed until June of 2005 but is unable to provide a complete population of implemented scripts, to include the type, purpose and intended effect on financial data. The implemented process is ineffective as the approval, testing and documentation procedures of the script changes are not appropriately designed and the current process is ineffective to control the intended and actual effect on financial data.		**07-31**
CG	06-30	• A copy of the [redacted] Disaster Recovery Plan has been completed. However, the plan has not been tested. • The DRP for [redacted] has been completed. However, testing of the [redacted] DRP has not taken place. The projected completion date is October 2006. • The DRP for the [redacted] has been completed. However, testing of the [redacted] DRP is scheduled to take place by the end of the year. • A copy of the MOU between [redacted] and two other CG components who the [redacted] must rely on for various reasons at the off-site facility was cited in the Disaster Recovery Plan • A finalized contract with the off-site facility was cited in the Disaster Recovery Plan. However, we were unable to obtain the signature page for it during our audit field work.		**07-12**
CG	06-31	During our FY 2006 follow-up testing, we determined that [redacted] had taken corrective action on several of the previously noted vulnerabilities, however several remained. The remaining vulnerabilities are in the following four areas: • Account management - 2 high-risk vulnerabilities and 4 medium-risk vulnerabilities		**07-15**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		• Configuration management – 2 medium-risk vulnerabilities • Patch management – 3 high-risk vulnerabilities		
CG	06-32	During our FY 2006 testing, we determined that none of the [redacted] prior year vulnerabilities were corrected. As a result, the vulnerabilities present in FY 2006 are in the following four areas: • Audit management – 2 medium risk vulnerabilities • Configuration management – 3 high, 6 medium and 11 low risk vulnerabilities • Password management – 1 high and 5 medium risk vulnerabilities • Patch management- 11 high, 12 medium and 12 low risk vulnerabilities		**07-15**
CG	06-33	[redacted] contracts the maintenance of their information systems software and hardware for the Superdome supercomputer, which houses the four production databases including the [redacted] production database, to Hewlett Packard through two separate service agreements. One of the service contracts is valid until 2007 for a segment of their computer software and hardware. However, the second portion of [redacted]'s Superdome equipment is covered under a maintenance contract that expired on May 31, 2006. [redacted] has requested a renewal of this contract however the request is still pending and there is no other contractual agreement to cover the maintenance of their software and hardware during this lapse in service contracts.	**X**	
CG	06-34	• [redacted] does not perform background investigations or verify that background investigations have been performed for contractors working at [redacted], especially those with sensitive IT positions. Specifically, [redacted] employs 150 contractors; however, We were unable to obtain the status of a background investigation on any of them. • No risk levels for contractor personnel with access to DHS information systems at [redacted] exist. Contracting personnel with IT job functions which require advanced access to the DHS system are not categorized at a higher risk level then an individual who uses the system with basic privileges.		**07-10**
CG	06-35	The MOU developed between CG [redacted] and Treasury Financial Management Service addresses the development, management, operation, and security of a connection between systems owned by both parties. The previous agreement expired in April of 2006 and a current MOU between [redacted] and Treasury has not been completed.	**X**	

Department of Homeland Security
Information Technology Management Letter
September 30, 2007

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
CG	06-36	• Seven developers out of 15 personnel in the Business Services Section had inappropriate access to [redacted] function in the Production and Development environments allowing them to potentially circumvent the change control process at [redacted] from October 1, 2005 through August 10, 2006. • We further note that 5 out of 15 personnel in the Business Services Section had inappropriate access to functions containing elevated privileges in the Production and Development environments allowing them to update production and potentially circumvent the change control process at [redacted].		**07-28**
CG	06-37	The following password configuration weaknesses associated with the [redacted] application: • Passwords were not configured to require password changes every 90 days from October 1, 2005 to February 14, 2006. • Passwords were not configured to require minimum length of six instead of eight. • Passwords were not configured to maintain a history of six passwords. • Passwords were not configured to require a combination of alphabetic, numeric, and special characters. • Passwords were not configured to restrict dictionary words including dictionary words spelled backwards. • Passwords were not configured to restrict simple pattern passwords; such as “qwerty” or “xyz123”. • Passwords were not configured to check that two identical characters in any position exist from the previous password. Additionally, we identified that the [redacted] application is configured to terminate idle sessions after 30 minutes of inactivity instead of 20 minutes.		**07-22**
CG	06-38	The following segregation of duties weaknesses associated with the [redacted] application. Application Audit Trails/Monitoring • The [redacted] application does not have the capacity to maintain audit trails for management review. Incompatible Duties • There is only one individual performing all [redacted] DBA duties. The lone [redacted] DBA actions are not reviewed for appropriateness, including changes to data and/or security profiles.		**07-23**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		• Users in the "[redacted]" group have privilege to insert data at the database level. • There are 17 accounts associated with the DBA role in Oracle.		
CG	06-39	There are no documented policies and procedures on the calculation of the environmental liability reported on the DHS Consolidated balance sheet. The environmental liability is adjusted quarterly based on the data stored in the [redacted] application.		**07-24**
CG	06-40	We identified the following account management weaknesses associated with the [redacted] application. Inactive Accounts • A planned monthly review of inactive [redacted] application user accounts has not been implemented. • There are 315 active accounts that have not logged into the [redacted] application for 90 days. Access Authorizations • Access authorization documentation was not made available for 17 out of 60 selected new [redacted] application users. Logical/Physical Access Reviews • The [redacted] application accounts are not recertified annually to validate that the accounts belong to appropriate personnel. • Management is not reviewing failed logon attempts to the [redacted] application. Termination Procedures • Five separated civilian personnel had active accounts in the [redacted] application. • Nine separated military personnel had active accounts in the [redacted] application. • CG does not maintain a centralized listing of separated contractors.		**07-27**
CG	06-41	System change request to modify transaction code 136-2 to automatically reestablish the funds as obligated was implemented in March 2006 within the [redacted] 3.2 build. Currently, the automated process appeared to be operating effectively. However, from October 2005 through March 2006, no mitigating controls such as procedures for training of staff and/or manual reviews were established to determine whether or not the re-obligation should be established to the associated undelivered orders balance. Additionally, [redacted] management indicated that transaction code 230 should not be automatically reestablishing the funds in the system. However, as we could not perform a complete analysis of the [redacted] posting logic in FY 2006 as noted in NFR CG IT-06-029, transaction code 230, as well as other codes, may still contain errors as of September 30, 2006.	**X**	

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
CG	06-42	[redacted] had not developed formal change control procedures documenting the requirements for altering the criteria used in [redacted] to match transactions. Functional changes are required when initially establishing a matching process or when the accounting operations team identifies that transactions that should be matching are not correctly matching in the system.		**07-30**
CG	06-43	Policies and procedures surrounding the change control process for CG [redacted] needs improvement. Specifically, no policies and procedures exist for: • the testing/verification the functionality of the change in pre-production before the change is implemented in production • the final approval of the change by [redacted] management Additionally, change control test results, as well as approvals, are not consistently documented. Specifically, documentation for the two formula changes requested, did not include evidence of testing in a pre-production instance and the final approvals of the changes when they are implemented in production. Furthermore, of the five remained changes selected, we were unable to obtain documentation of final of final approvals for each of the five sample items approvals for five out of the five items.		**07-38**
CG	06-44	Policies and procedures for the overall change control process surrounding [redacted] changes and 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.		**07-35**
CG	06-45	As a result of our audit test work and supported by all the IT NFRs issued during the current year, we determined that CG is non-compliant with the following laws and regulations: • FISMA • FFMIA • Office of Management and Budget (OMB) Circular A-130		**07-42**
CONS	06-01	Two members of DHS OFM had excessive [redacted] within DHS [redacted]. We informed DHS OFM of the excessive [redacted] access and noted that DHS OFM removed both users with excessive [redacted] access. We noted that corrective action has been taken and completed in the current fiscal year; however, this issue posed a risk for a majority of the fiscal year and therefore will be		**07-03**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		reported as a weakness for FY 2006.		
CONS	06-02	[redacted] new user access request forms were not consistently completed prior to granting access to [redacted]. Specifically, one (1) out of a sample of eleven (11) did not have a supervisor's approval. Additionally, five (5) out of a sample of eleven (11) did not have [redacted] security manager review.		**07-02**
CONS	06-03	OFM has not developed procedures to periodically review [redacted] access lists in order to determine whether user access is valid, consistent with job responsibilities and in accordance with the principle of least privilege	**X**	
CONS	06-04	During our audit, the following configuration management weaknesses were noted • Segregation of duties violations exists for twelve (12) out of twenty-five (25) system changes made outside of the scheduled [redacted] Quarterly Releases. • Segregation of duties violations exists for four (4) out of ten (10) emergency system changes made outside of the scheduled [redacted] Quarterly Releases. • Test documentation is not available for changes implemented outside of the scheduled [redacted] Quarterly Releases.		**07-11**
CONS	06-05	There are no documented procedures in place for DHS components to perform a formal review, by a separate approving individual, to verify the [redacted] financial data to the general ledger before moving the [redacted] file from the Holding Area into the [redacted] Repository.		**07-05**
CONS	06-06	There are no individual user accounts for DBA access and that the generic [redacted]" account is shared amongst the two DBAs.		**07-7**
CONS	06-07	The DHS OFM is not requiring [redacted] users to formally acknowledge and sign the FARS ROB prior to being granted access to [redacted]. We noted that eighteen (18) out of a sample of (20) [redacted] users had not formally acknowledged and signed the FARS ROB document.	**X**	
CONS	06-08	• Password configurations for the [redacted] application have been configured to permit passwords to be a minimum of six (6) characters in length which is not in compliance with DHS 4300A, which requires passwords to be a minimum of eight (8) characters in length. • [redacted] application administrators lock out accounts if a user has not accessed the account after 180 days which is not in compliance with DHS 4300A, which requires administrators to lock out		**07-06**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		accounts if a user has not accessed the account after 90 days.		
CONS	06-09	The password configurations for the [redacted] application have been configured to not enforce passwords to have a combination of alphanumeric characters and special characters which is not in compliance with DHS 4300A, which requires that passwords contain a combination of alphabetic, numeric, and special characters.		**07-01**
CONS	06-10	Personnel with physical access to the [redacted] production server, housed in the Department of Treasury Data Center are not periodically reviewed for appropriateness of access.	**X**	
CONS	06-11	OFM does not maintain a termination/separated employee listing of OFM employees. As a result we were unable to perform a control test to determine if terminated/separated OFM employees have access to [redacted].	**X**	
CONS	06-12	Department of Treasury media sanitization policies and procedures have not been developed for [redacted]. We noted that media sanitization services are provided by Iron Mountain through Qwest; however, there are no specific media sanitization policies and procedures in place for the Department of Treasury to sanitize [redacted] media.	**X**	
CONS	06-13	Not used.		
CONS	06-14	Department of Treasury media sanitization policies and procedures have not been finalized or implemented. We noted that the Department of Treasury policy entitled, "Memorandum: Destroying and Sanitizing Media" is currently in draft form.	**X**	
CONS	06-15	Discrepancies exist between the DHS Performance and Accountability Report (PAR) Guidance and the Analytical Report		**07-10**
CONS	06-16	[redacted] We determined that normal balance type indicated on the DHS SGL for Account 4132 and Account 7280 differ from the normal balance type indicated on the [redacted]. • We determined that 101 DHS [redacted] accounts were not found in the US SGL and reported a zero balance for period 9. These accounts do not appear to be currently used by DHS and/or do not appear to be related to DHS operations.		**CONS-07-18 (Issued by the Audit Team)**
CONS	06-17	Access to waive fatal errors using the [redacted]_ZAP role appears excessive for two employees per OFM policy.		**07-04**
CONS	06-18	DHS is non-compliant with FISMA.		**07-13**

Department of Homeland Security
Information Technology Management Letter
September 30, 2007

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
FEMA	06-01	During our technical testing, patch management weaknesses were identified on [redacted] servers. Specifically, as a result of missing patches, the [redacted] servers were vulnerable to buffer overflow vulnerabilities.		**07-01**
FEMA	06-02	During our technical testing, configuration management weaknesses were identified on [redacted], and key support servers. Specifically, servers were identified with password and auditing configuration weaknesses, and version weaknesses.		**07-02**
FEMA	06-03	There are no procedures are in place to periodically review [redacted] user access lists to determine if access is still needed, including the development of a master listing of all employees and contractors developed and maintained by FSB.		**07-03**
FEMA	06-04	The [redacted] production and test servers are located in very close proximity of each other, which is not conducive to effective contingency planning efforts. We note that upon the implementation of the [redacted] Data Center's "real-time" back-up facility, both the [redacted] test and production servers will be redundant, alleviating the current condition. However, the [redacted] back-up facility does not currently have that capability in place.		**07-04**
FEMA	06-05	• The [redacted] ST&E did not provide adequate documentation of the results to the accrediting authority. The [redacted] ST&E included thorough testing of managerial, operational and technical controls and identified 88 vulnerabilities; however, the vulnerabilities listed in the ST&E report were only identified as one Plan of Action and Milestones (POA&M) weakness in the [redacted] POA&M • Of the 10 systems deemed critical for which the C&A process was completed, we noted that the following four systems did not include any documentation of their ST&E results in the ATO package: [redacted] • FEMA has completed a majority of the [redacted] migration from Microsoft Windows 2000 Professional to Linux except for a few aspects of the migration dealing with Individual Assistance and various regional sites. We noted that these major changes to the system warrant that the [redacted] C&A process be re-performed.		**07-05**
FEMA	06-06	There is not formal, documented procedures are in place to require updates to the [redacted] system documentation as [redacted] functions are added, deleted, or modified.		**07-06**
FEMA	06-07	• FEMA did not adequately document testing of the Contingency Plan for [redacted]. Although a table-top test of the [redacted] Contingency Plan was completed on February 10, 2006, the [redacted] table top test did not adequately test the IT components of the system/processes. • FEMA does not have an accurate Contingency Plan for [redacted]. The most recent version of the [redacted] Contingency Plan is dated		**07-07**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		July 19, 2004. However, since that time, FEMA has nearly completed its migration of [redacted] from Microsoft Windows 2000 Professional to the Linux operating system and is adding a Small Business Administration web interface.		
FEMA	06-08	The FEMA COOP has prioritized each of its 12 critical IT systems according to criticality of the systems; however, the FEMA COOP has not been updated to take into account the new listing of FEMA critical IT systems. We confirmed with the Office of Cyber Security (OCS) and Office of National Security (ONSC) that the updated listing of FEMA mission critical IT systems should be represented in the FEMA COOP.		**07-08**
FEMA	06-09	• [redacted] users are not locked out of the system after three invalid logon attempts. In addition, we determined that upon locking a user account out of the system after three invalid logon attempts at the domain level, the user account becomes unlocked and active again after fifteen (15) minutes of inactivity. • [redacted] settings on machines running Microsoft Windows 2000 Professional disabled the user's ability to disable the password protected screensaver; however the [redacted] settings did not disable the user's ability to change the inactivity threshold greater than the FEMA standard of fifteen minutes. This weakness impacts [redacted].		**07-09**
FEMA	06-10	[redacted] settings on machines running Microsoft Windows 2000 Professional prevented the user's ability to disable the password protected screensaver; however the [redacted] settings did not prevent the user's ability to change the inactivity threshold. The implementation of a password protected screensaver as a mitigating control for lacking a second form of authentication is not sufficient if users have the ability to change the inactivity threshold greater than the FEMA standard of fifteen minutes. This weakness impacts [redacted]		**07-10**
FEMA	06-11	• Password configurations for the [redacted] application have been configured to permit passwords to be a minimum of six characters in length which is not in compliance with DHS 4300A. • Access authorizations for [redacted] are not consistently documented and maintained on file. We noted that FEMA Form 20-24, User Access Control Form, was not completed for three (3) out of a sample of twenty-five (25) new user access request forms for [redacted].		**07-11**
FEMA	06-12	No policies or procedures exist to periodically review [redacted] access listings to determine if access is still required or if access levels commensurate with users' job responsibilities. We noted that [redacted] user access lists have not been reviewed to determine if access is still required or if access levels commensurate with users' job responsibilities.		**07-12**
FEMA	06-13	Twenty-nine (29) terminated or separated FEMA employees and contractors maintain active [redacted] user accounts. Additionally, we		**07-13**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		noted that two (2) terminated or separated FEMA employees maintain active [redacted] user accounts. The implementation of FEMA Instruction 1540.3 as a form of access controls review is not sufficient because FEMA is only performing reviews over current year terminations and separations, and has not performed reviews over legacy users to ensure that all users have valid access.		
FEMA	06-14	[redacted] software request forms were not consistently approved by supervisors. We noted that FEMA Software Tracking Form, did not have supervisor approval prior to receiving software for eight (8) out of a sample of fifteen (15) [redacted] software request tickets, which is not in compliance with the FEMA Policy – Procedures for Removal and Return of Storage Media from and to the Library, as well as DHS 4300A.	**X**	
FEMA	06-15	• Deposits and withdrawals of [redacted] backup tapes are not authorized or logged. • [redacted] backup tapes are not rotated to an offsite location.		**07-14**
FEMA	06-16	FEMA Policy - Sanitization and Release of Electronic Storage Media has not been finalized or implemented and is currently in draft form.	**X**	
FEMA	06-17	No formally documented configuration management plan is in place for [redacted]. FEMA has informal configuration management procedures for [redacted]; however they have not been formally documented.	**X**	
FEMA	06-18	• A documented configuration management plan is in place for [redacted]; however, it is currently in draft form. We noted that the plan has multiple sections where input from FEMA personnel is requested by the Contractor who created the plan, however, FEMA has not responded back to these requests. Additionally, the [redacted] configuration management plan was created in 1998 and needs to be updated to reflect the current [redacted] environment. • No documented policies and procedures are in place for restricting access to system software. • No documented [redacted] Patch Management Policy has been documented.		**07-15**
FEMA	06-19	No formally documented policies and procedures are in place for restricting access to [redacted] system software		**07-16**
FEMA	06-20	[redacted] application programmers/configuration management group responsible for maintaining and developing changes for IFMIS are also responsible for migrating application code changes into the production environment. We noted that the Contractor uses the username, "ifmiscm" within the [redacted] Unix environment to deploy application code changes into the [redacted] production environment.		**07-17**
FEMA	06-21	No formal investigation procedures are in place to review suspicious		**07-18**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		system software activities or suspicious access activities for [redacted].		
FEMA	06-22	• No documented policies and procedures exist to monitor sensitive access and system software utilities for [redacted] • No formal investigation procedures are in place to review suspicious system software activities or suspicious access activities for [redacted]		**07-19**
FEMA	06-23	No documented SDLC has been developed for [redacted]		**07-20**
FEMA	06-24	No documented SDLC has been developed for [redacted].		**07-21**
FEMA	06-25	Emergency exit and re-entry procedures are not effective for the data center housing the [redacted] production and test servers. The current procedures do not provide detailed information regarding the exact procedures needed to re-enter the data center after leaving the facility for an emergency.	**X**	
FEMA	06-26	Excessive access has been granted to Group 0001 in [redacted]. We identified one member of Group 0001 who does not have a real business need to have access to this function. We informed the FSB of the excessive Group 0001 access and noted that FSB removed the user with excessive access. We noted that corrective action has been taken and completed in the current fiscal year; however, this issue posed a risk for a majority of the fiscal year and therefore will be reported as a weakness for FY 2006.	**X**	
FEMA	06-27	Twenty-one (21) users in Group 0002 and eight (8) users in Group 0003 have the ability to gain access to the account mapping functions and make changes to the account tables. Of the 21 users in Group 0002, nine (9) users do not have a real business need to have access to this function. The 9 users that appear to have excessive access consist of [redacted] developers or others with system administrative access. Additionally, of the 8 users in Group 0003, six (6) users do not have a real business need to have access to this function. Additionally, excessive access is designed to be permitted within [redacted] to make offline changes to the general ledger account tables via the FMFTP Group. Currently, we identified five (5) users in the FMFTP group that have the ability to make offline changes to the general ledger account tables. Of the five users, four (4) users do not have a real business need to have access to this function.		**07-30**
FEMA	06-28	[redacted] user access request forms were not consistently completed prior to granting access to [redacted]. Specifically, two (2) out of a sample of thirteen (13) did not have a supervisor's approval.	**X**	
FEMA	06-29	• An applicant's homeowner's insurance status is not verified prior to granting disaster housing assistance. • The automated home ownership verification check within [redacted] failed by (a) misidentifying a renter as a homeowner and (b) failing to verify home ownership status for a valid homeowner.		**FEMA-07-16 (Issued by the Audit Team)**

Department of Homeland Security
Information Technology Management Letter
September 30, 2007

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
FEMA	06-30	• Visitor logs are not maintained to the LAN room at [redacted] Bureau LAN Data Center in [redacted] • One separated CSC personnel retained physical access to the [redacted] facility; however, this individual did not have access privileges to the [redacted] room. • Management does not periodically review physical access listings to determine if access is still required or if access levels are commensurate with users' job responsibilities.		**07-42**
FEMA	06-31	• The [redacted] application does not require password authentication separate from an initia [redacted] password authentication to identify and authenticate user access. • No audit trails documenting user actions or actual or attempted access are maintained or reviewed. • The [redacted] application does not timeout after a period of inactivity. • Password protected screensavers are not operating on al [redacted] desktops. • Information owners do not periodically review access authorization listings to determine if access is still required or if access levels commensurate with users' job responsibilities. • [redacted] does not disable accounts after a period of inactivity, such as 90 days.		**07-31**
FEMA	06-32	• Information owners do not periodically review access authorization listings to determine if access is still required or if access levels commensurate with users' job responsibilities. • Does not disable accounts after a period of inactivity, such as 90 days. • Does not enforce the DHS password requirements beyond the use of 8 characters. • Does not have a session timeout after the DHS required period of inactivity. • Audit trails are not reviewed in accordance with [redacted]) and DHS policy.		**07-41**
FEMA	06-33	Segregation of duties controls were not implemented for the [redacted] General Ledger application, such as establishing user roles and groups.		**07-38**
FEMA	06-34	The current program build of Symantec Anti-Virus Corporate Edition for the NFIP [redacted] program build had Security Advisory SYM06-010 issued about it on June 6, 2006, indicating that a security flaw had been identified allowing a remote or local attacker to execute code on an affected system.	**X**	
FEMA	06-35	• [redacted] change management procedures are not documented. • Installation of the new version of [redacted] in FY 2006 was not formally approved by users. • Installation of the operating system upgrade in FY 2006 was not		**07-32**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		formally documented or approved.		
FEMA	06-36	• Five of 15 selected mainframe changes did not have documented requestor's change approval on the OSR forms. • NFIP mainframe baseline configuration document has not been updated to reflect the current environment.		**07-34**
FEMA	06-37	Excess access was identified to following Transaction Record Reporting and Processing accounts: • [redacted] – Bureau Production • [redacted] production member.		**07-35**
FEMA	06-38	There are no individual user accounts for [redacted] administrator access and that the generic "Administrator" account is shared amongst the three administrators. Furthermore, the [redacted] has the capability to maintain system activity logs; however, system administrators do not regularly review the logs.		**07-33**
FEMA	06-39	Access to the excel files that calculate the Loss and Loss Adjustment Expense appears excessive. Specifically, we identified that modify and write access permissions to the excel files appear inappropriate for six people of the Bureau of Finance and Statistical Control group.		**07-36**
FEMA	06-40	No formal change control procedures are in place to authorize, test, verify, and approve program changes made to the Loss and Loss Adjustment Expense Reserves excel files.	**X**	
FEMA	06-41	• [redacted] Visitor logs are not maintained to the Technology Management Group (TMG) raised floor data center in [redacted] • Two separated CSC personnel retained physical access to the TMG facility.	**X**	
FEMA	06-42	• Information owners do not periodically review access authorization listings to determine if access is still required or if access levels are commensurate with users' job responsibilities. • Audit trails are not reviewed in accordance with DHS policy. • Excessive access to the sensitive system utilities dataset [redacted]) on the [redacted] was provided to 1 security administrator and 31 operations personnel.	**X**	
FEMA	06-43	One of the eight requested exit checklists used to ensure that all physical and logical access of terminated personnel is removed was not provided.	**X**	
FLETC	06-01	• No documented configuration management plan is in place for [redacted] including the following: - Lack of documented test plan standards and procedures; - Lack of a documented comprehensive set of test transactions;		**07-01**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		- Test results are not maintained and a documented approval for the test results does not exist; and - Lack of a description for the emergency change process. • We were unable to verify that an independent control group performed the migration of tested and approved [redacted] system software to the production environment. • We were unable to verify that access to [redacted] program libraries is restricted.		
FLETC	06-02	• No documented configuration management plan is in place for [redacted] including the following: - Lack of documented test plan standards and procedures; - Lack of a documented comprehensive set of test transactions; - Test results are not maintained and a documented approval for the test results does not exist; and - Lack of a description for the emergency change process. • We were unable to verify that access to [redacted] program libraries is restricted. We noted that a listing of users with access to the [redacted] production environment was unavailable.		**07-02**
FLETC	06-03	The installation of [redacted] system software is not logged or reviewed by FLETC management.		**07-03**
FLETC	06-04	The SDLC for [redacted] is currently in draft form.		**07-04**
FLETC	06-05	• [redacted] backups maintained onsite are not periodically tested. • FLETC does not utilize external labels to indicate the sensitivity of the information on the [redacted] backup compact discs.		**07-05**
FLETC	06-06	The [redacted] contingency plan has not been tested.		**07-06**
FLETC	06-07	FM11041: Safeguarding Sensitive But Unclassified (For Official Use Only) Information is currently in draft form and has not been finalized or implemented.	**X**	
FLETC	06-08	We noted that incidents are not tracked from inception to resolution in an incident response management system.		**07-07**
FLETC	06-09	We noted that there are five (5) generic/shared [redacted] accounts shared amongst the two DBAs.		**07-08**
FLETC	06-10	The following [redacted] control weaknesses were identified: • No policies and procedures are in place to request access to the [redacted]. • No policies and procedures are in place to periodically review the list of persons with physical access to the [redacted]. • No emergency policies and procedures are in place for the evacuation and re-entry of the [redacted]. • No policies and procedures are in place to guide and document		**07-09**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		the emergency training of [redacted] personnel.		
FLETC	06-11	• No policies and procedures are in place over access authorizations to [redacted] and the general support system hosting these applications. • No policies and procedures are in place to periodically review the list of [redacted] user accounts. • No policies and procedures are in place to immediately notify [redacted] System administrators when users are terminated or transferred. • Password configurations for [redacted] have been configured to permit passwords to be a minimum of six characters in length with no complexity requirements. • [redacted] users are locked out of the system after five (5) invalid logon.		**07-10**
FLETC	06-12	FD 43220: IT System Security Awareness and Training is currently in draft form and has not been finalized or implemented.		**07-11**
FLETC	06-13	There are no established policies and procedures in place for the authorization and use of mobile code technologies. Currently, FLETC uses client side Java Applets in connection with [redacted]		**07-12**
FLETC	06-14	There are no policies and procedures in place to review [redacted] audit logs for actual or attempted unauthorized or unusual access to sensitive data.		**07-13**
FLETC	06-15	There are no documented policies and procedures in place for restricting access to [redacted] system software.		**07-14**
FLETC	06-16	Incompatible duties and roles identified within the [redacted] application have not been documented and no policies and procedures exist to segregate incompatible duties and roles.		**07-15**
FLETC	06-17	An established sanctions process for personnel failing to comply with established information security policies and procedures does not exist. However, we noted that FM 4900, Information Technology System ROB and Use Agreements, was finalized in August 2006 and establishes disciplinary actions they could be subject to if the ROB are not followed. We noted that the policy is finalized but has yet to be implemented.	**X**	
FLETC	06-18	There are no FLETC specific established policies and procedures in place for the use and installation of [redacted] technologies. We noted that FLETC is currently using the Defense Information Systems Agency (DISA) [redacted] and the FLETC [redacted] Security Checklist for the use and installation of [redacted] technologies. Currently, this technology is used at three FLETC sites and is all interconnected through the FLETC [redacted] which has a direct connection with [redacted].		**07-16**

Department of Homeland Security
Information Technology Management Letter
September 30, 2007

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
FLETC	06-19	We noted that twelve (12) out of a sample of (15) FLETC contractors did not have evidence that a background investigation was initiated or completed.		**07-17**
FLETC	06-20	We noted that a user of the [redacted] Fixed Assets module has the ability to change the useful life field during the asset entering process.		**Issued by the Audit Team**
FLETC	06-21	The following [redacted] access control weaknesses were identified: • No policies and procedures are in place to [redacted] server level system software audit logs for successful or unsuccessful access attempts. • No audit logs are maintained to capture actual or attempted unauthorized, unusual or sensitive access within the [redacted] application level.		**07-18**
FLETC	06-22	During technical testing, configuration management weaknesses were identified on the databases supporting the [redacted] applications, as well as supporting servers. Specifically, databases and servers were identified with account management, auditing, database configuration and password management weaknesses.		**07-26**
FLETC	06-23	During technical testing, patch management weaknesses were identified on hosts and databases supporting the [redacted] applications. The fact that these vendor supplied patches have not been applied in a timely manner could allow a remote attacker to gain unauthorized access on the host or database.		**07-27**
G&T	06-01	The POA&M report for G&T does not identify the scheduled completion date, and/or the status of corrective action taken for each IT weakness listed on the POA&M report.	**X**	
G&T	06-02	G&T does not have a signed waiver in place as part of their Interagency Agreement (i.e. MOU) to mitigate the issue of their lack of compliance with NIST SP 800-53 "Recommended Security Controls for Federal Information Systems" security controls.	**X**	
G&T	06-03	We identified that all 45 G&T users (17 GMS, 11 IFMIS, and 17 Web 269) recertification forms contained one of the following weaknesses; original access level/privileges assigned were not documented on the form, and the user privileges were notated as deleted on the form but still active on the access listing. In addition, the recertification process was not performed on a semi-annual basis as stipulated by the OJP's recertification process.	**X**	
G&T	06-04	We identified 14 out of 15 remote users, did not have an authorized remote access form on file. Specifically, we noted that the forms were missing signatures from the employee and his/her supervisor.	**X**	

Department of Homeland Security
Information Technology Management Letter
September 30, 2007

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
G&T	06-05	We identified 1 out of 6 terminated employees who had a missing requestor signature on their SF-52 form. In addition, we identified 6 out of 6 terminated employees who did not sign their DHS 400-2 exit clearance form upon departure.	**X**	
G&T	06-06	Weaknesses were identified as a part of the FY 2006 Department of Justice, OJP Financial Statement Audit and impact the reliance G&T has on OJP's IT control environment.	**X**	
G&T	06-07	1 out of 6 G&T terminated employees access was not removed from the [redacted] application within a timely manner (i.e. two business days).	**X**	
G&T	06-12	Three users who have been assigned privileges that allow them to enter, modify, and approve journal vouchers. According to their job functions and responsibilities, these users should only have the ability to enter journal vouchers. In addition, two users who have been assigned privileges (e.g. [redacted] that allow them to modify vendor tables, and allow them to open and close fiscal years.	**X**	
TSA	06-01	Service continuity weaknesses for [redacted] including outdated Business Continuity Contingency Plan (BCCP), lack of disaster recovery procedure details, an off-site storage location in close proximity to the data center, and lack of BCCP testing exist.		**07-01**
TSA	06-02	A comprehensive incident capability that includes designated response team members and procedures for incident handling to help ensure that the incident is properly handed has not been documented and implemented.	**X**	
TSA	06-03	[redacted] emergency procedures are in place for the evacuation of [redacted] and its data center; however, no emergency re-entry procedures exist within this directive. Additionally, no policies and procedures are in place to guide and document the emergency training of data center personnel. Lastly, the concept of "least privilege" has not been implemented with regard to the data center.		**07-04**
TSA	06-04	Although backup tapes for [redacted] and GSS are created on a regular basis, testing procedures have not been documented in accordance with [redacted] Instruction. Additionally, although [redacted] backup tapes are rotated off-site to the [redacted] GSS backups have not been included in the rotation process. Lastly, tape transfer logs are not being completed in their entirety.	**X**	
TSA	06-05	Configuration weaknesses over [redacted] workstations allowed users to modify sensitive workstation system and security settings. Upon notification, [redacted] management took immediate action to correct the configuration settings.	**X**	
TSA	06-06	Weaknesses were noted regarding [redacted] personnel entrance and exit procedures for civilian, contractor and military personnel.	**X**	
TSA	06-07	A [redacted] Security Configuration Management Plan does not exist that clearly delineates the roles and responsibilities between CG's support contractor, and the [redacted]. CG's support contractor is the	**X**	

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		organization under contract by CG to manage the [redacted] software programs. Consequently, the System Security Plans for the [redacted] applications do not include key security control information such as the current security configuration management process, including delineation of responsibilities for all involved parties.		
TSA	06-08	Technical testing identified patch management weaknesses on hosts supporting the [redacted] applications which could allow for a remote attacker to gain full control of the affected host and could lead to the compromise of the availability, confidentiality and integrity of [redacted] data.		**07-18**
TSA	06-09	Technical testing identified configuration management weaknesses on hosts supporting the [redacted] applications. Specifically, servers were identified with excessive access privileges, and password and auditing configuration weaknesses.		**07-19**
TSA	06-10	Not Used.		
TSA	06-11	The MOU between [redacted] and Treasury Financial Management Service expired during FY 2006.	**X**	
TSA	06-12	An agreement for system software and hardware support for the four production databases including the [redacted] production database expired on May 31, 2006. A request to renew the contract is pending; however, there is no other contractual agreement to cover the maintenance of their software and hardware during this lapse in service contracts.	**X**	
TSA	06-13	Manager Review of System Administration Monitor Procedures do not note the periods of review that are being monitored and who is responsible for performing the reviews, and evidence that the manager review was performed could only be obtained for March 2006. Additionally, for the first half of the fiscal year, Unix system administration monitoring was not performed by a manager or group outside of the three systems administrators. Additionally, Unix access request forms are not consistently maintained and the account of a contractor that left [redacted] remained active for eight months after the contractor's departure.	**X**	
TSA	06-14	The following [redacted] access control weaknesses were identified: 1. Password configurations for the application and database were not in compliance with the [redacted] Password Policy SOP. 2. Users are not locked out of their [redacted] application accounts after three invalid logon attempts. 3. Audit logging has not been enabled within the [redacted] application or database. 4. Individuals who were no longer employed with [redacted] were found to have active accounts within [redacted]. 5. [redacted] account reviews have not been performed on a periodic basis for [redacted] personnel.		**07-08**
TSA	06-15	The following [redacted] access control weaknesses were identified: 1. Password configurations for the application and database were not		**07-09**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		in compliance with the [redacted] Password Policy SOP. 2. Users are not locked out of their [redacted] accounts after three invalid logon attempts. 3. Policies and procedures for application and database audit log management have not been documented, and audit logs that are generated are being reviewed by the database administrators, not by an external party.		
TSA	06-16	The following Sunflower access control weaknesses were identified: 1. Password configurations for the application and database were not in compliance with the [redacted] Password Policy SOP. 2. Users are not locked out of the Sunflower application after three invalid logon attempts. 3. Audit logging has not been enabled within the Sunflower application or database.	**X**	
TSA	06-17	[redacted] accounts are not immediately disabled upon an employee's termination, and no policies and procedures exist for the periodic review of TSA personnel with access to [redacted].		**07-12**
TSA	06-18	[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.		**07-11**
TSA	06-19	[redacted] accounts are not immediately disabled upon an employee's termination. Additionally, policies and procedures do not exist requiring the periodic review of TSA personnel with access to [redacted].		**07-07**
TSA	06-20	The TSA Form 1402, IT off-boarding form for Non-Screeners and Contractors, is not consistently completed for terminated personnel. Specifically, we identified that the form was unavailable for thirty-eight (38) of sixty (60) terminated employees selected for testing. Additionally, eight (8) out of the twenty-two (22) forms received were incomplete.		**07-20**
TSA	06-21	Security awareness training and Computer Access Agreements are not consistently completed. Additionally, TSA has not documented sanctioning procedures to be enforced when users of TSA information systems are in violation of the computer access agreements and security policies.		**07-15**
TSA	06-22	TSA has not documented policies and procedures surrounding the change control process for [redacted], formalized a tracking process of its own change requests submitted to [redacted], or retained documentation associated with the requests (i.e., initial approvals, testing and final approvals).		**07-21 and 07-25**
TSA	06-23	Guidance for performing suitability screening for all contractors is considered interim and not final; therefore, CG will wait until the policy is finalized before moving forward on conducting background investigations on contractors. Additionally, [redacted] does not perform background investigations or verify that outside background		**07-05**

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		investigations have been performed for contractors working at [redacted]. Lastly, risk levels for contractor personnel with access to DHS information systems have not been assigned.		
TSA	06-24	Excessive access has been granted within Markview. Specifically, of the 27 individuals that have been granted Authorized Certifying Officer privileges to approve invoices of any dollar value, four were not justified in having such privileged access.	**X**	

Appendix D

Management's Response to the Draft Department of Homeland Security Information Technology Management Letter

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

Homeland Security

JUN 18 2008

MEMORANDUM FOR: Richard Skinner
Inspector General

FROM: David Norquist
Chief Financial Officer

Robert West
Chief Information Security Officer

SUBJECT: *Draft Report Office of the Inspector General Fiscal Year 2007 Information Technology Management Letter*

We have reviewed the Office of the Inspector General's (OIG) FY07 Information Technology Management Letter (ITML) report dated, December 14, 2007. We concur with the Financial Systems Security findings contained within your audit report.

Per the report's recommendation, the DHS Office of the Chief Information Officer (OCIO) and the Office of the Chief Financial Officer (OCFO) have expanded their collaboration in FY08 to address the detailed recommendations regarding information security controls and processes.

Some of the activities completed so far in FY08, include:

- Published the FY08 *Internal Control Playbook*, including the Financial Systems Security section to better integrate OCIO and OCFO security requirements;
- Aligned the DHS Federal Information Security Management Act (FISMA) and Financial Systems Inventories;
- Developed DHS policies and procedures for a compliance model for OCFO designated systems based on key National Institute of Standards and Technology (NIST) SP 800-53 controls (4300A, Attachment R);
- Updated DHS Information Assurance tools to account for the additional security requirements associated with OCFO-designated systems; and
- Provided direct Component field support for remediation activities where necessary.

In addition, the OCFO released an exposure draft Addendum to the DHS FY08 *Internal Control Playbook*, Track Two, Management Assurance Guide, to assist DHS in its efforts to comply with the internal control provisions of A-123. This document outlines how:

CFO Audit Management Letter Continued
Page 2 of 2

- DHS will begin incorporating the OCIO Compliance Framework into the OMB A-123, Appendix A Assessment and
- Existing CIO and CFO assessment approaches will be leveraged.

These efforts will enable the Department to provide a consistent and comprehensive approach to resolving and ensuring the security of CFO-financial designated systems. 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.

Report Distribution

Department of Homeland Security

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

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

Additional Information and Copies

To obtain additional copies of this report, 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.