DEPARTMENT OF HOMELAND SECURITY
Office of Inspector General

Information Technology Management Letter for the United States Coast Guard Component of the FY 2007 DHS Financial Statement Audit (Redacted)

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

OIG-08-69

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 United States Coast Guard (CG) component of the FY 2007 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 CG'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

Chief Financial Officer
U.S. Coast Guard

Chief Information Officer
U.S. Coast Guard,

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 ended 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 2007 engagement, we considered Coast Guard's internal control over financial reporting by obtaining an understanding of Coast Guard's 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 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 fiscal year (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 Coast Guard 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

United States Coast Guard
Information Technology Management Letter
For the FY 2007 DHS Financial Statement Audit Engagement

INFORMATION TECHNOLOGY MANAGEMENT LETTER

Table of Contents

Appendices

United States Coast Guard
Information Technology Management Letter
For the FY 2007 DHS Financial Statement Audit Engagement

OBJECTIVE, SCOPE AND APPROACH

We performed audit procedures over Coast Guard's general controls in support of the Audit of the DHS balance sheet as of September 30, 2007 and related statement of custodial activity for the year then ended. The overall objective of our audit procedures was to evaluate the effectiveness of information technology (IT) general controls of Coast Guard's financial processing environment and related IT infrastructure as necessary to support the engagement. The Federal Information System Controls Audit Manual (FISCAM), issued by the Government Accountability Office, formed the basis of our audit procedures. Further information related to the scope of the Coast Guard's IT general controls assessment is described in Appendix A.

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

- *Entity-wide security program planning and management* – 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* – 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* – Controls that help to prevent the implementation of unauthorized programs or modifications to existing programs.
- *System software* – Controls that limit and monitor access to powerful programs that operate computer hardware.
- *Segregation of duties* – 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* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

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

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

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

ensure that security settings, once instituted, remain in place and to identify vulnerabilities that require correction.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

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

During the fiscal year 2006 DHS Financial Statement Audit, 44 IT general and application control NFRs were identified and issued. During fiscal year 2007, Coast Guard took actions to improve aspects of their IT general and application control environment and to address prior year IT control issues. Coast Guard did take corrective action in the areas of implementing incident response procedures, ensuring that back-up of key financial data is being conducted, and exit and entrance procedures have been implemented at Coast Guard's Financial Center. However, Coast Guard did not make all of necessary improvements that they had planned to during the year. During the 2007 IT testing, we identified a total of 42 findings, of these 40 are repeated findings, either partially or in whole, from the prior year and 6 were new IT findings.

All six general control areas included control deficiencies (IT NFRs) that present a reasonably possible chance of impacting financial data integrity. The deficiencies included: 1) excessive access to key Coast Guard financial applications, 2) application change control processes that are not adequately designed nor operating effectively, 3) entity-wide security program issues involving personnel background issues, 4) system software weaknesses involving patch management and configuration management, 5) segregation of duties involving lack of policies and procedures and excessive privilege access issues, and 6) service continuity issues involving the lack of disaster recovery testing. The continued and the new additional internal control weaknesses were the result of a lack of organization and prioritization in taking the necessary corrective actions and a mis-understanding of the necessary steps to identify and address the root cause of prior-year weaknesses and implement appropriate corrective action plans. Several significant and serious IT general control weaknesses remain that collectively limit Coast Guard's ability to ensure that critical financial and operational data is maintained in a manner to ensure confidentiality, integrity, and availability.

IT FINDINGS BY AUDIT AREA

Conditions: In fiscal year 2007, the following IT and financial system control weaknesses were identified at Coast Guard. Many of the issues identified during our fiscal year 2007 engagement were also identified during fiscal year 2006. These following IT and financial system control weaknesses result in IT being reported as a material weakness in the DHS Internal Control report.

1. Access controls – we noted:
   - A large number of instances of weak password configurations for key financial applications that do not meet DHS requirements.
   - A large number of instances of missing and weak user passwords on key servers and databases which process and house financial data.
   - A large number of instances where user account lists were not periodically reviewed for appropriateness, and inappropriate authorizations and excessive user access privileges were allowed.
   - Instances where workstations, servers, or network devices were configured without necessary security patches or were not configured securely.
   - Instances where application and database accounts are not immediately disabled upon an employee or contractor's termination.
   - Excessive access existed within financial applications. 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.
   - Coast Guard systems are not compliant with DHS requirements. Coast Guard systems have 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.
2. Application software development and change control – we noted:
   - The Coast Guard Finance Center ([redacted]), critical to the management of financial systems, 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. These deficiencies contribute directly to Coast Guard's inability to support their financial reporting assertions related to reported financial statement balances.
   - The contract that Coast Guard has with their software vendor does not include security configuration requirements that must be adhered to during the configuration management process thereby causing security vulnerabilities to be present on key [redacted] financial systems.
   - 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.

- Instances where changes made to the configuration of the system were not always documented through System Change Requests (SCRs), test plans, test results, or software modifications at [redacted] and at Coast Guard's Personnel Service Center ([redacted]). 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.
- Changes to a financial application were implemented in the production environment prior to management approval.

3. Entity-wide security program planning and management – we noted:
   - Despite continued improvements in the process of performing Certification and Accreditation (C&A) of IT systems, a major financial application was not properly certified and accredited, in compliance with DHS' *Information Technology Security Program Sensitive Systems Handbook, 4300A* (DHS 4300A) and National Institute of Standards and Technology (NIST) guidance.
   - Instances where background investigations of contractors employed to operate, manage and provide security over IT systems were not being properly conducted related to Coast Guard Headquarters and [redacted]. Additionally at the [redacted], thirteen (13) contractors were foreign nationals with sensitive IT security positions such as database administrators and system administrators. These contractors did not have a completed waiver from DHS and the [redacted] was in the process of initiating background investigations for them this fiscal year.
   - Background investigations and reinvestigations for civilian personnel have not been performed in accordance with DHS guidance.
4. System software – we noted:
   - Patch management weaknesses continue to exist on host supporting Coast Guard financial systems.
   - Configuration management weaknesses continue to exist on Coast Guard financial systems.
5. Segregation of duties – we noted:
   - An instance where the policy and procedures to define and implement segregation of duties were not properly developed and/or implemented at the [redacted].
   - 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.
   - Database administration accounts are shared and activities performed with these accounts are not logged and reviewed.
   - One developer for a financial system had access to an elevated privilege in production.
6. Service continuity – we noted:
   - Disaster Recovery Planning (DRP) has not been completed. Specifically, DRPs for the [redacted] and Coast Guard's Operations Supply Center ([redacted]) are in draft form and have not been tested. In addition, the Memorandum of Understandings (MOUs) to finalize the plans are not complete.

Application Controls:

- We did not identify any findings during our testing of the Coast Guard application controls. However, it should be noted that our application testing was limited due to the seriousness of audit findings that limited the completion of planned audit procedures.

Cause/Effect: Many of these weaknesses were inherited from system development activities that did not incorporate strong security controls during the initial implementation of the system and will take several years to fully address. These weaknesses exist both in the design and 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 stringent security practices. Consequently, as policies and procedures are updated many Coast Guard components have struggled to move away from previous methodologies and fully implement and enforce these new controls.

Furthermore, there is no consistent and thorough testing of IT controls by Coast Guard to identify and mitigate weaknesses. 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 primary example of this is the second change control process that was implemented to address functionality weaknesses in the Coast Guard financial systems. Instead of implementing corrective actions to address the functionality issues identified in the application, workarounds were implemented so that the system could continue functioning. The effect of these numerous IT weaknesses identified during our testing impacts the reliability, confidentiality and integrity of Coast Guard's financial data. Many of these weaknesses, especially those in the area of change control, may result in material errors in Coast Guard's financial data that are not detected, in a timely manner, in the normal course of business. In addition, as a result of the continuous presence of serious IT deficiencies, there is added pressure on the mitigating manual controls to be operating effectively at all times. Since manual controls are operated by people, there cannot be a reasonable expectation that they would be able to be in place at all times and in all areas.

Criteria: The *Federal Information Security Management Act* (FISMA) passed as part of the *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.

Recommendations: We recommend that the DHS Office of Chief Information Officer in coordination with the OCFO and the Coast Guard make the following improvements to the Coast Guard's financial management systems:

1. For access control:
   a) Enforce password controls that meet DHS' password requirements on all key financial systems;
   b) Implement an account management certification process within all the Coast Guard components to ensure the periodic review of user accounts for appropriate access and to ensure that generic accounts do not exist on the system;

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

d) 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;

e) Implement a periodic review process of accounts that have been inactive by the specified period of time outlined in DHS guidance;

f) Configure financial applications settings to be compliant with DHS guidance to ensure that account sessions are locked out after 20 minutes of inactivity and that accounts are locked after 90 days of inactivity;

g) Implement a patch and security configuration process, and enforce the requirement that systems are periodically tested by Coast Guard; and

h) 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.

2. For application software development and change control:

   a) Reevaluate and revise the contract between Coast Guard 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 NIST guidance for financial applications;

   b) Implement a single, integrated change control process over the Coast Guard's financial systems with appropriate internal controls to include clear lines of authority to the financial management personnel and to enforce responsibilities of all participants in the process and documentation requirements; and

   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.

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

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

   b) Enforce DHS' policy to ensure that all contractors and civilian personnel go through the appropriate background/suitability check and periodic reinvestigations.

4. For system software, actively monitor the use of and changes related to operating systems and other sensitive utility software and hardware. Additionally perform corrective actions on weaknesses identified.

5. For segregation of duties:

   a) 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;

   b) Implement policies and procedures developed to enforce segregation of duties; and

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

6. For service continuity:
   a) Develop and implement complete current business continuity plans and system disaster recovery plans;
   b) Perform testing of key service continuity capabilities; and
   c) Finalize MOUs pertaining to current business continuity plans and system disaster recovery plans.

Management Comments and OIG Evaluation

We obtained written comments on a draft of this report from the CG CIO. Generally, the CG CIO agreed with all of the report's findings and recommendations. We have incorporated the comments where appropriate and included a copy of the comments in their entirety at Appendix D.

OIG Response

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

Appendix A

DESCRIPTION OF FINANCIAL SYSTEMS AND IT INFRASTRUCTURE

Below is a description of significant Coast Guard financial management systems and supporting IT infrastructure included in the scope of the FY 2007 balance sheet audit engagement.

Locations of Audit: Coast Guard Headquarters in [redacted] the Coast Guard Finance Center ([redacted]) in [redacted] the [redacted] in [redacted] and the [redacted] in [redacted]

Key Systems Subject to Audit:

- [redacted] is the [redacted] that is the principal general ledger for recording financial transactions 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]) - [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. It reconciles transaction items that Treasury has processed to transaction items Coast Guard has sent 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 with other Coast Guard general ledger balances. After reconciliation and adjustment, balancing information is uploaded into DHS TIER.
- [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] ([redacted]) – Formerly named the Supply Center Computer Replacement System, [redacted] is hosted at [redacted]. [redacted] is the primary financial application for the [redacted] ([redacted]), the Supply Fund, and the Coast Guard Yard fund.
- [redacted] ([redacted]) - [redacted], is a web-based application designed to automate the management of Coast Guard's vessel logistics by supporting the following functions: configuration, maintenance, supply and finance.

Appendix B

COAST GUARD IT NOTICES OF FINDINGS AND RECOMMENDATIONS THAT CONTRIBUTED TO THE DEPARTMENT'S MATERIAL WEAKNESS OVER FINANCIAL SYSTEMS SECURITY

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 control environment and on the integrity of the financial data residing on the DHS component's financial systems. 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.

High Risk: A control weakness serious in nature to create a potential material misstatement to the financial statements.

Medium Risk: A control weakness, in conjunction with other events, less severe - in nature than a high risk issue, which could lead to a misstatement to the financial statements.

Low Risk: A control weakness minimal in impact to the financial statements.

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

Appendix B

COAST GUARD IT NOTICES OF FINDINGS AND RECOMMENDATIONS THAT CONTRIBUTED TO THE DEPARTMENT'S MATERIAL WEAKNESS OVER FINANCIAL SYSTEMS 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.	• Finalize and implement the 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 OSC 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. 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	• Modify the current policies and procedures to reflect the change control and emergency change control process for [redacted] in accordance with DHS and NIST guidance. Specifically, develop and implement a formalized process for the initial approval, testing, and final approval of all system changes. Additionally, this documentation should include roles and responsibilities of [redacted] personnel in this process. • Develop and implement a formalized		X	Medium

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	to service packs, data fixes and the testing procedures completed.	process for the retention of documentation throughout the change control process.			
CG-IT-07-03	Personnel Service Center ([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. • 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	[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

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	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 existing Systems Development Lifecycle Document (SDLC) 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 checklist and requiring that the checklist be completed each time a change is made. • Establish procedures to be followed		X	Medium

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		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 Coast Guard 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. Coast Guard 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 Coast Guard HQ and corrective actions will be taken at that time.	CG-841 should reevaluate and revise the contract between Coast Guard 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 guidance 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 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	[redacted] should: • Continue to seek improvements to [redacted] sign-on technology that would enforce password complexity requirements to meet 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

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	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 NON[redacted] and the [redacted] is not enabled. [redacted] enables the activities of users with the OPERATIONS 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] and [redacted] 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] should: • Set [redacted] security settings to the most restrictive modes possible. Specifically, the following [redacted] settings should be changed: - [redacted]o - Enable PROTECTALL 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 determined to have excessive privileges, revoke unneeded privileges. • Revoke the [redacted]ccount in [redacted]. • Revoke the [redacted] in		X	Medium

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	[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..	[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 Coast Guard Headquarters to address DHS requirements surrounding the suitability screening of contractors accessing DHS IT systems. DHS directives and policies require Coast Guard and other DHS components to ensure the completion of background investigations for all contractors accessing IT systems. The type of background investigations should be based on the risk level of their future position at Coast Guard and are required to be completed prior to the start of work. However, no Coast Guard guidance exists to require Coast	• 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 Coast Guard 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		X	High

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Guard components to clear their contractors for suitability, especially those with sensitive IT positions.	work at Coast Guard. Additionally, ensure that all current contracts are updated with the required language. • Provide resources to Coast Guard 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.		X	Low

CG-IT-07-12	• [redacted] was tested and the [redacted] DRP was tested at the [redacted] ([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 domain name system (DNS) 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	Medium

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	[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

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	approvals) was not available for each change selected for testing.				
CG-IT-07-14	Coast Guard 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 Coast Guard 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 ORACLE_HOME/bin chmod o-x oracle. • 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		X	Medium

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		parameter. • Document the current process used for both performing vulnerability scans of the [redacted] network environment as required by DHS Sensitive Systems Policy Directive 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 • 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] 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 are utilizing and will utilize a password in compliance with DHS guidance.		X	Low

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
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 not being reviewed for appropriateness.	• 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 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		X	Medium

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		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 Coast Guard 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 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], [redacted], [redacted] TSA, and [redacted]. These accounts have every privilege within	• 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] 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,		X	High

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	the application, including the ability to create/delete/modify user accounts within [redacted].	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 [redacted] 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 [redacted] 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 [redacted] 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 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 Coast Guard. 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	[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

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	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; • SAM 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 USCG to address the DHS requirement that systems disable idle accounts after 20 minutes. No determination was made on the waiver for this NFR.	• Modify the [redacted] application password configurations to be compliant with DHS and Coast Guard 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 Coast Guard policy.		X	Medium
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 USCG to address the DHS requirement that audit logs over the use of sensitive system utilities be reviewed. No	• Develop and implement procedures to monitor the actions of the DBAs 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		X	High

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	determination was made on the waiver for this NFR.	performing operations in the system and determine whether the actions taken by [redacted] end users are appropriate to their job function.			
CG-IT-07-24	End user computing procedures have been developed, but that they are currently in draft form. At the time of testing, Coast Guard 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.	Coast Guard 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]_USER_R 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 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], [redacted] and	• Continue with efforts to reduce the number of users associated with the [redacted]_USER_R 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 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		X	Medium

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	[redacted] profiles do not meet DHS password requirements. (Although the [redacted] profile was not assigned to any new [redacted] users during FY 2007, users with this profile were transferred to the SECURE_LOGON 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.	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] and [redacted] systems have been configured to automatically end date accounts that have not been used in six months; however, DHS guidance requires accounts that have been inactive for 30 days be disabled.	[redacted] should track and end-date/disable [redacted] and [redacted] accounts in compliance with DHS requirements.	X		Low
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	• 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		X	Medium

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	after 90 days.	timely manner so that access to the [redacted] system can be removed in a timely manner.			
CG-IT-07-28	• One developer had access to an elevated privilege in [redacted] production. • We also noted that [redacted] privileges in [redacted] 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 an applicant by the same individual. Specifically, the individual who enters an applicant's data into the [redacted] system also has the ability to hire the applicant in the system.	Segregate the roles by requiring that the person who enters an applicant's data is 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 [redacted] audit trails on a regular basis to ensure that activities are authorized.)		X	Medium
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	• 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		X	Medium

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	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.	responsibilities. • Develop and implement a formalized process for the retention of documentation throughout the change control process for [redacted] functional changes.			
CG-IT-07-31	Coast Guard has and continues to operate a separate, informal and largely undocumented change development and implementation process effecting Coast Guard Financial Systems, outside of and conflicting with the formal change control process. This informal script development and implementation process began with the implementation of [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.	• Immediately implement a single, integrated change control process over Coast Guard Financial Systems with appropriate internal controls to in include clear lines of authority to Coast Guard 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 Coast Guard Financial Systems with an external independent organization trained in financial information systems, process analysis and with a demonstrated understanding of the federal accounting environment 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. Coast Guard's root cause analysis		X	High

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		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	Coast Guard 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.	Coast Guard Headquarters should implement policies and procedures to track the status of Coast Guard contractors.	X		**Medium**
CG-IT-07-33	Coast Guard does not consistently notify system owners that individuals are terminating from the Coast Guard so that system accounts can be updated timely.	Coast Guard Headquarters should develop a method to inform system owners that individuals are terminating from the Coast Guard and that their systems access should be locked and/or removed upon their termination from the Coast Guard.	X		**Medium**
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,	[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		X	**Medium**

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	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.	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.			
CG-IT-07-35	Policies and procedures for the overall change control process surrounding [redacted], [redacted] and [redacted] changes and emergency changes are inadequate. Specifically procedures detail the overall process and phases for [redacted], [redacted] and [redacted] change control, but lack detailed guidance for the roles and responsibilities executed by [redacted] personnel and do not address emergency changes. Additionally, [redacted] is not consistently retaining documentation to support the change control and emergency change control process.	[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], [redacted] and [redacted] to include the different roles and responsibilities that personnel within Coast Guard-[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		X	High

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		of documentation throughout the change control process.			
CG-IT-07-36	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] and [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 Coast Guard 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
CG-IT-07-37	Technical testing identified configuration management weaknesses on hosts supporting the [redacted] and [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 Coast Guard 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
CG-IT-07-38	[redacted] has taken corrective actions surrounding the [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.	[redacted] should complete the following: • Ensure that personnel involved in the [redacted] change control process follow the policies and procedures set forth in [redacted]'s Financial Reporting Procedures for Changes to [redacted]. • Ensure that all [redacted] changes are tested and that the test results are reviewed and approved by the appropriate [redacted] management prior to		X	Medium

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	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.	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 TIER Database form.			
CG-IT-07-39	Coast Guard is making progress in the number of background investigation records that remain to be restored. However, Coast Guard has not completed the process of filing the records that were recovered and recreating of the records that were not found during the migration of records from the Department of Transportation to DHS.	Coast Guard 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. 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.	Coast Guard should completion of performing initial background investigations and reinvestigations for civilian employees in accordance with DHS directives.		X	Medium
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	[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] build..	X		Low

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
	Coast Guard operates; • C&A does not reflect system changes made in the [redacted] upgrade; and • [redacted] is classified by Coast Guard as a subsystem of [redacted]. However, we noted that there is no documentation within the [redacted] system security plan (SSP) that defines [redacted] as 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] build. However, the process has not yet been completed.				
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 Coast Guard is non-compliant with the Federal Financial Management Improvement Act (FFMIA) in an information technology perspective and in the following areas:. • Computer Security Act Requirements, including aspects of the Federal Information Security Management Act (FISMA) • System Documentation • Internal Controls • Training and User Support • System Maintenance • System Information Flow	• Continue to implement and monitor compliance with DHS, Coast Guard and Federal security policies and procedures in the areas of: • Change Controls • 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		X	High

Appendix B

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating
		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.			

Appendix C

STATUS OF PRIOR YEAR COAST GUARD IT NOTICES OF FINDINGS AND RECOMMENDATIONS

			Disposition	
Component	NFR No.	Description	Closed	Repeat
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] and the [redacted] are created on a regular basis, testing procedures have not been documented in accordance with [redacted] Instruction. Additionally, although [redacted] backup tapes are rotated offsite to the [redacted] 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. Additionally, although criticality levels for [redacted] changes have been defined, procedures for making emergency changes to [redacted] have not been developed.		07-34

Appendix C

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
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; - Approval for migration of system software changes into production; and • The audit trail of system software changes is not periodically reviewed.		**07-05**
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		**07-13**

Component	NFR No.	Description	Disposition	
			Closed	Repeat
		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		
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] and [redacted] settings were not enabled. Furthermore, four accounts assigned to [redacted] personnel had both [redacted] and [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 SECURE_LOGON and SECURE_LOGON2 profiles have been configured to permit passwords to be a minimum of six characters in length. Additionally, the password history requirement is the only password requirement that has been configured for the [redacted] profile. • Audit logging has not been enabled within the [redacted] application or database. • Documented access request forms could not be located for nine out of 22 new [redacted] users granted access to the application. Additionally, although the automated access request forms for the other 13 out of 22 new [redacted] users granted access to the application were approved, the level of access/privileges associated with the new user were not documented on the access request form. • Individuals who are no longer employed with [redacted] were found to have active accounts within [redacted]. • [redacted] account reviews have not been performed on a periodic basis.		**07-25**

Appendix C

			Disposition	
Component	NFR No.	Description	Closed	Repeat
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 found to have active accounts within [redacted]. • [redacted] account reviews have not been performed on a periodic basis.		07-18
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	X	

Component	NFR No.	Description	Disposition	
			Closed	Repeat
		procedures do not note the periods of review that are being monitored, who is responsible for performing the reviews and evidence that the manager review was performed could only be obtained for March 2006. Additionally, although the manager reviews were implemented in March 2006, for the first half of the fiscal year, October through March, [redacted] system administration monitoring was not performed by a manager or group outside of the three systems administrators during that time period. • The access request form for one out of four individuals granted access to [redacted] since October 1, 2005, did not contain the supervisor's approval. • The account of a contractor that left [redacted] in October 2005 remained active until May 2006.		
CG	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 Coast Guard to manage the [redacted] and [redacted] software programs. Consequently, the System Security Plans for the [redacted] and [redacted] applications do not include key security control information. Specifically, the plans do not include information on the current security configuration management process, including delineation of responsibilities for all involved parties. The System Security Plans were otherwise compliant with current NIST guidance.	X	
CG	06-21	Coast Guard Headquarters is in the process of developing policy that addresses role-based training requirements for individuals with critical IT positions. However, currently this Training and Education Plan is still in draft form and no policies and procedures exist that require critical IT personnel to continue their education through role-based training.		07-14
CG	06-22	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 Coast Guard. Forgotten widows are the survivors of retired personnel who died before any survivor benefit program was enacted. The program is designed to exclude those member types included in the [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	

Appendix C

			Disposition	
Component	**NFR No.**	**Description**	**Closed**	**Repeat**
		[redacted].		
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], [redacted] and [redacted] applications. Many of these vulnerabilities could allow a remote attacker to gain full control of the affected host and could lead to the compromise of the availability, confidentiality and integrity of [redacted], [redacted] and [redacted] data.		**07-36**
CG	06-27	During technical testing configuration management weaknesses were identified on hosts supporting the [redacted], [redacted] and [redacted] applications. Specifically, servers were identified with excessive access privileges, and password and auditing configuration weaknesses.		**07-37**
CG	06-28	• Coast Guard has not completed the process of filing the records that were recovered and recreating of the records that were not found during the migration of records from the Department of Transportation to DHS. • Civilian background investigations and reinvestigations are not being consistently performed. Specifically, three (3) out of seven (7) newly hired civilian employees at [redacted] did not have any record of a background investigation on file. Additionally, for the re-investigation of [redacted] employees, four (4) out of five (5) GS employees selected did not have a current investigation on file. • Position sensitivity level distinctions for civilian personnel with access to DHS information systems at [redacted] are not accurately depicted. Specifically, of the selection of position descriptions received, nine (9) out of ten (10) had non-critical position sensitivities although their job functions were that of IT personnel with advanced access to the DHS system.		**07-39** **07-40**
CG	06-29	Coast Guard has and continues to operate a separate, informal and largely undocumented change development and implementation process effecting Coast Guard Financial Systems, outside of and conflicting with the formal change control process. This informal script development and implementation process began with the implementation of [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**

			Disposition	
Component	NFR No.	Description	Closed	Repeat
CG	06-30	• A copy of the [redacted] Disaster Recovery Plan has been completed. However, the plan has not been tested. • The DRP for the Naval Engineering Supply Support System ([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 Memorandum of Understanding (MOU) between [redacted] and two other Coast Guard 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 • Configuration management – 2 medium-risk vulnerabilities • Patch management – 3 high-risk vulnerabilities		07-15
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 (HP) through two separate service agreements. One of the service contracts is valid until 2007 for a segment of their computer software and hardware. However, the	X	

			Disposition	
Component	NFR No.	Description	Closed	Repeat
		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.		
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 Memorandum of Understanding (MOU) developed between Coast Guard [redacted] and Treasury Financial Management Service addresses the development, management, operation, and security of a connection between systems owned by both parties. The previous agreement expired in April of 2006 and a current MOU between [redacted] and Treasury has not been completed.	X	
CG	06-36	• Seven developers out of 15 personnel in the Business Services Section had inappropriate access to [redacted]_DEVELOPER_R 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		07-22

			Disposition	
Component	NFR No.	Description	Closed	Repeat
		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.		
CG	06-38	The following segregation of duties weaknesses associated with the [redacted] application. <u>Application Audit Trails/Monitoring</u> • The [redacted] application does not have the capacity to maintain audit trails for management review. <u>Incompatible Duties</u> • There is only one individual performing all [redacted] DBA duties. The lone [redacted] DBA actions are not reviewed for appropriateness, including changes to data and/or security profiles. • Users in the "CSDHLPDSK" group have privilege to insert data at the database level. • There are 17 accounts associated with the DBA role in Oracle.		**07-23**
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. <u>Inactive Accounts</u> • 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. <u>Access Authorizations</u> • Access authorization documentation was not made available for 17 out of 60 selected new [redacted] application users. <u>Logical/Physical Access Reviews</u> • 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. <u>Termination Procedures</u> • Five separated civilian personnel had active accounts in the [redacted]		**07-27**

Component	NFR No.	Description	Disposition	
			Closed	Repeat
		application. • Nine separated military personnel had active accounts in the [redacted] application. • Coast Guard does not maintain a centralized listing of separated contractors.		
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 UDO 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 Coast Guard IT-06-029, transaction code 230, as well as other codes, may still contain errors as of September 30, 2006.	X	
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 [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] and [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		**07-35**

			Disposition	
Component	NFR No.	Description	Closed	Repeat
		approvals, [redacted] testing, final approvals and documentation retention requirements for changes made to the system.		
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 Coast Guard is non-compliant with the following laws and regulations: • Federal Information Security Management Act of 2002 (FISMA) • Federal Financial Management Improvement Act (FFMIA) • Office of Management and Budget (OMB) Circular A-130		**07-42**

U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: CG-621
Phone: (202) 475-3638
Fax: (202) 475-3928
Email: kurt.e.steiner@uscg.mil

7100
MAR 11 2008

MEMORANDUM

From: RDML D. T. Glenn
COMDT (CG-6)

Reply to Attn of: CG-621
LT K. Steiner
(202) 475-3638

To: Mr. Frank Deffer, Assistant Inspector General, Information Technology Audits
U.S. Department of Homeland Security

Subj: DRAFT AUDIT REPORT - INFORMATION TECHNOLOGY MANAGEMENT LETTER FOR THE U.S.COAST GUARD COMPONENT OF THE FY 2007 DHS FINANCIAL STATEMENT AUDIT REPSONSE

Ref: (a) DHS Draft Audit Report Memorandum of 11 Feb 2008

1. The Coast Guard has reviewed reference (a) and concurs with the findings and recommendations. The Coast Guard will continue working with the DHS OCFO in pursuing the strategy that was briefed on 7 January 2008, and will incorporate the results of this audit.

2. Thank you for the opportunity to comment on your draft audit report.

#

Copy: COMDT (CG-8)

United States Coast Guard
Information Technology Management Letter
For the FY 2007 DHS Financial Statement Audit Engagement

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Chief of Staff
Deputy Chief of Staff
Executive Secretariat
Under Secretary, Management
Commandant of the USCG
DHS Chief Information Officer
DHS Chief Financial Officer
Chief Financial Officer, USCG
Chief Information Officer, USCG
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
Director, Audit Coordination

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.