# Department of Homeland Security
## Office of Inspector General

# Information Technology Management Letter for the United States Coast Guard Component of the FY 2008 DHS Financial Statement Audit

# (Redacted)

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

OIG-09-47

March 2009

*Office of Inspector General*

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

Homeland Security

March 27, 2009

Preface

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

This report presents the information technology (IT) management letter for the United States Coast Guard (CG) component of the FY 2008 DHS financial statement audit as of September 30, 2008. It contains observations and recommendations related to information technology internal control that were not required to be reported in the financial statement audit report (OIG-09-09, November 2008) and represents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit of CG's FY 2008 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated December 5, 2008, and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control or make conclusion on compliance with laws and regulations.

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

**KPMG LLP**
2001 M Street, NW
Washington, DC 20036

December 5, 2008

Inspector General
U.S. Department of Homeland Security

Chief Information Officer
U.S. Coast Guard

Chief Financial Officer
U.S. Coast Guard

Ladies and Gentlemen:

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

In connection with our fiscal year (FY) 2008 engagement, we considered 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 Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements*. We did not test all internal controls relevant to operating objectives as broadly defined by the *Federal Managers' Financial Integrity Act of 1982* (FMFIA). The objective of our engagement was not to provide an opinion on the effectiveness of DHS' internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of DHS' internal control over financial reporting. Further, other matters involving internal control over financial reporting may have been identified and reported had we been able to perform all procedures necessary to express an opinion on the DHS balance sheet as of September 30, 2008, and the related statement of custodial activity for the year then ended, and had we been engaged to audit the other FY 2008 financial statements.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects DHS' ability to initiate, authorize, record, process, or report financial data reliably in accordance with U.S. generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of DHS' financial statements that is more than inconsequential will not be prevented or detected by DHS' internal control over financial reporting. A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control.

During our audit engagement, we noted certain matters in the area of application software development and change control with respect to Coast Guard's financial systems Information Technology (IT) general

controls which we believe contribute to a DHS-level significant deficiency that is considered a material weakness in IT general and application controls. These matters are described in the *IT General Control Findings by Audit Area* section of this letter.

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

Although not considered to be material weaknesses, we also noted certain other matters during our audit engagement which we would like to bring to your attention. These matters are also described in the *IT General Control Findings by Audit Area* section of this letter.

The material weakness and other comments described herein have been discussed with the appropriate members of management, or communicated through a Notice of Finding and Recommendation (NFR), and 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 2008 DHS financial statement audit in Appendix A; a description of each internal control finding in Appendix B; and the current status of the prior year NFRs in Appendix C. Our comments related to financial management and reporting internal controls have been presented in a separate letter to the Office of Inspector General and the DHS Chief Financial Officer dated December 5, 2008.

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

Very truly yours,

KPMG LLP

**Department of Homeland Security**
**United States Coast Guard**
*Information Technology Management Letter*
September 30, 2008

## INFORMATION TECHNOLOGY MANAGEMENT LETTER

### TABLE OF CONTENTS



### APPENDICES

# OBJECTIVE, SCOPE AND APPROACH

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

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

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

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

Application controls were not tested for the year ending September 30, 2008 due to the nature of prior-year audit findings.

# SUMMARY OF FINDINGS AND RECOMMENDATIONS

During fiscal year (FY) 2008, Coast Guard took corrective action to address nearly half of their prior year IT control weaknesses. For example, Coast Guard made improvements by implementing emergency response training for all Coast Guard personnel with data center access, verifying that all Coast Guard personnel have completed exit forms upon separation, and testing disaster recovery procedures. However, during FY 2008, we continued to identify IT general control weaknesses at Coast Guard. The most significant weaknesses from a financial statement audit perspective related to the development, implementation, and tracking of scripts at , and the design and implementation of configuration management policies and procedures at These IT control weaknesses limited Coast Guard's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impacted the internal controls over Coast Guard financial reporting and its operation and we consider them to collectively represent a material weakness for Coast Guard under standards established by the American Institute of Certified Public Accountants (AICPA). In addition, based upon the results of our test work we noted that the Coast Guard did not fully comply with the requirements of Federal Financial Management Improvement Act (FFMIA).

Of the 22 findings identified during our FY 2008 testing, 21 were repeat findings, either partially or in whole from the prior year, and 1 was a new IT finding. These findings represent weakness in four of the six FISCAM key control areas. The FISCAM areas impacted included Application Software Development and Change Controls, Access Controls, Service Continuity, and Entity-Wide Security Program Planning and Management. The majority of the findings were inherited from the lack of properly designed, detailed, and consistent guidance over financial system controls to enforce DHS Sensitive System Policy Directive 4300A requirements and National Institute of Standards and Technology (NIST) guidance. Specifically, the findings stem from 1) unverified access controls through the lack of user access privilege re-certifications, 2) entity-wide security program issues involving civilian and contractor background investigation weaknesses, 3) inadequately designed and operating change control policies and procedures, 4) patch and configuration management weaknesses within the system, and 5) the lack of updated disaster recovery plans which reflect the current environment identified through testing. These weaknesses may increase the risk that the confidentiality, integrity, and availability of system controls and Coast Guard financial data could be exploited thereby compromising the integrity of financial data used by management and reported in the DHS financial statements.

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

# IT GENERAL CONTROL FINDINGS BY AUDIT AREA

**Findings Contributing to a Material Weakness in IT General Controls**

*Conditions:* In FY 2008, the following IT and financial system control weaknesses were identified at the Coast Guard and contribute to a DHS-level significant deficiency that is considered a material weakness in IT general and application controls.

Application software development and change controls – we noted:

- For the data scripts run at Coast Guard's , procedures over approval, testing, and documentation requirements remain in draft form. The does not consistently include all testing, approval, and implementation documentation for all scripts. In addition, Coast Guard does not monitor scripts run in the database through audit logging and has not developed a technical solution to monitor who accesses the database through to run scripts or review what scripts are run.
- Coast Guard conducted an examination of the data scripts run with an external, independent organization; however, due to the many limitations over scope, the analysis was incomplete. Furthermore, the analysis did not properly evaluate scripts as to financial statement impact, including current versus prior year effect.
- Coast Guard lacks a formal process to distinguish between the module lead approvers for script approval requests.
- Procedures over software changes for the key financial applications during the development and testing processes include multiple weaknesses.

*Recommendations:* We recommend that the Coast Guard Chief Information Officer and Chief Financial Officer, in coordination with the DHS Office of Chief Financial Officer and the DHS Office of the Chief Information Officer**,** make the following improvements to Coast Guard's financial management systems and associated information technology security program:

- Implement and document in detail, a single, integrated script change control process that includes clear lines of authority to Coast Guard financial and IT management personnel, enforced responsibilities of all participants in the process, and documentation requirements.
- Continue efforts to complete an in-depth analysis of active scripts, with the following objectives: All changes to active scripts and new scripts should be subject to an appropriate software change control process, to include testing, reviews, and approvals, and should be reviewed for impact on financial statement balances.
- Develop and implement change control policies and procedures to verify that all software changes are approved, tested, documented, tracked, and reviewed prior to deploying the changes into the production environment in accordance with DHS Sensitive System Policy Directive 4300A.

**Other Findings in IT General Controls**

Although not considered to be a material weakness, we also noted the following other matters related to IT and financial system control deficiencies during the FY08 audit engagement:

1. Access controls – we noted:
    - Procedures surrounding the system used to track contracted personnel data have not been formally documented.
    - Procedures over the process of finalizing and implementing entity-wide processes for account terminations and related notifications are still in draft and have not been implemented or communicated.
    - Security configuration management weaknesses exist on hosts supporting the key financial applications and the underlying general support systems.
    - Security patch management weaknesses exist on hosts supporting the key financial applications and general support systems.
    - Policies and procedures have not been developed and implemented for the manual periodic review of audit logs for key financial systems.
    - Access review procedures for key financial applications do not include the review of all user accounts to ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked, and that privileges associated with each individual are still authorized and necessary.
    - Access control weaknesses identified during our IT testing also contributed to numerous instances where access to data could lead to various incompatible function issues.
    - Access request forms are not being completed for all financial system users on a consistent basis.

2. Entity-wide security program planning and management – we noted:
    - Security configuration requirements were not implemented into contract language of a support contractor.
    - Policies or procedures have not been implemented to require that a favorably adjudicated background investigation be completed for all contractor personnel.
    - Background investigations for all civilian employees have not been completed and civilian position sensitivity designations have not been determined in accordance with DHS guidance.
    - A risk assessment for a major financial application has not been completed and the associated System Security Plan remains in draft form.

3. Service continuity – we noted:

- The [redacted] Continuity of Operations (COOP) Plan has not been updated to reflect the results of testing and the division Business Continuity Plans have not been finalized.

*Recommendations:* We recommend that the Coast Guard Chief Information Officer and Chief Financial Officer, in coordination with the DHS Office of Chief Financial Officer and the DHS Office of the Chief Information Officer**,** make the following improvements to Coast Guard's financial management systems and associated information technology security program.

For access controls:

- Develop procedures for the periodic review of the manual audit logs. In addition, ensure audit log files are configured, retained, and archived in compliance with DHS policy.
- Develop and implement procedures to require a periodic review by supervisors of all financial application and database user accounts and their associated privileges. These procedures should include steps to verify that all terminated individuals no longer have active accounts, that inactive accounts are locked and that privileges associated with each individual are still authorized and necessary.
- Finalize the procedural documentation over contractor tracking and communicate/distribute the procedures. In addition, continuously monitor controls over the contractor tracking system to verify that contractor data within the system remains current and accurate.
- Actively monitor the use of and changes related to operating systems and other sensitive utility software and hardware. Additionally, perform corrective actions on the specific patch and configuration weaknesses identified.
- Implement an automated process/system that will notify system owners of terminated contractor, military, and civilian personnel.
- Finalize and implement entity management policies and procedures for verifying that terminated user accounts have been successfully removed.
- Develop and implement procedures to require an annual review of all financial application and database user account privileges to verify that privileges remain up to date and proper segregation of duties exists.
- Update procedures to ensure that a documented and approved access authorization request is completed for each individual prior to granting him/her access to the key financial applications or databases.

For entity-wide security program planning and management:

- Create and implement contractor background investigation policies and procedures in order to establish requirements and ensure compliance with DHS Sensitive System Policy Directive 4300A. This includes the verification that all contracts issued by the Coast Guard include the appropriate Coast Guard position sensitivity designation requirements for contracted personnel.
- Perform initial background investigations and re-investigations for civilian employees in accordance with position sensitivity designations at no less than the Moderate level as required by DHS directives. In addition, conduct civilian background re-investigations every ten (10) years, as required by DHS directives, to ensure that each employee has a favorably adjudicated and valid Minimum Background Investigation.
- Finalize and implement the certification and accreditation C&A package for the key financial systems in accordance with DHS and NIST guidance.

For service continuity:

- Update the COOP to include the results of its testing and finalize the applicable supporting business continuity plans.

*Cause/Effect:* Many of these weaknesses were inherited from a system implementation in 2003 that did not properly take into account all of the key Coast Guard business and functional processes, operational support procedures, and IT security requirements; policies and procedures that were outdated, lacking, or contradictory; and a lack of consistent and proper monitoring and enforcement by Coast Guard management of the IT policies and procedures that are in place.

Reasonable assurance should be provided that financial system user access levels are limited and monitored for appropriateness and that all user accounts belong to current employees. The weaknesses identified within Coast Guard's access controls increase the risk that employees and contractors may have access to a system that is outside the realm of their job responsibilities or that a separated individual, or another person with knowledge of an active account of a terminated employee, could use the account to alter the data contained within the application or database. This may also increase the risk that the confidentiality, integrity, and availability of system controls and the financial data could be exploited thereby compromising the integrity of financial data used by management and reported in the DHS financial statements.

Furthermore, the lack of documented security configuration management controls may result in security responsibilities communicated to system developers improperly as well as the improper implementation and monitoring of system changes. This also increases the risk of unsubstantiated changes as well as changes that may introduce errors or data integrity issues that are not easily traceable back to the changes. In addition, it increases the risk of undocumented and unauthorized changes to critical or sensitive information and systems. This may reduce the reliability of information produced by these systems.

*Criteria:* The *Federal Information Security Management Act* (FISMA) passed as part of the *Electronic Government Act of 2002,* mandates that Federal entities maintain IT security programs in accordance with OMB and NIST guidance. OMB Circular No. A-130, *Management of Federal Information Resources,* and various NIST guidelines describe specific essential criteria for maintaining effective general IT controls. In addition, OMB Circular No. A-127 prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems. FFMIA sets forth legislation prescribing policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems. The purpose of FFMIA is: (1) to provide for consistency of accounting by an agency from one fiscal year to the next, and uniform accounting standards throughout the Federal Government; (2) require Federal financial management systems to support full disclosure of Federal financial data, including the full costs of Federal programs and activities; (3) increase the accountability and credibility of federal financial management; (4) improve performance, productivity and efficiency of Federal Government financial management; and (5) establish financial management systems to support controlling the cost of Federal Government. In closing, for this year's IT audit we assessed the DHS component's compliance with DHS Sensitive System Policy Directive 4300A.

## APPLICATION CONTROL FINDINGS

Application controls were not tested for the year ending September 30, 2008 due to the nature of the prior-year audit findings.

## MANAGEMENT COMMENTS AND OIG RESPONSE

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

### OIG Response

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

**Department of Homeland Security**
**United States Coast Guard**
*Information Technology Management Letter*
September 30, 2008

# Appendix A

# Description of Key Coast Guard Financial Systems and IT Infrastructure within the Scope of the FY 2008 DHS Financial Statement Audit

**Department of Homeland Security**
**United States Coast Guard**
*Information Technology Management Letter*
September 30, 2008

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

Locations of Audit: Coast Guard ; the Coast Guard ; the in ; and the ( ) in .

Key Systems Subject to Audit:

- that is the principal general ledger for recording financial transactions for the Coast Guard. is hosted at the Coast Guard's primary data center. It is a customized version of Financials.
- Used to create and post obligations to the . It allows users to enter funding, create purchase requests, issue procurement documents, perform system administration responsibilities, and reconcile weekly program element status reports. is interconnected with the system and is hosted at .
- Document image processing system, which is integrated with an relational database. allows electronic data and scanned paper documents to be imaged and processed for data verification, reconciliation and payment. utilizes software to scan documents and to view the images of scanned documents and to render images of electronic data received. This system is hosted at
- 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 at .
- Database maintained at . Information from is uploaded to this instance monthly with other Coast Guard general ledger balances. After reconciliation and adjustment, balancing information is uploaded into .
- application, hosted at , used for paying Coast Guard active and reserve personnel payroll.
- Formerly named the , is hosted at is the primary financial application for the the , and the Coast Guard .

- Web-based application, hosted at designed to automate the management of Coast Guard's vessel logistics by supporting the following functions: configuration, maintenance, supply and finance.

**Department of Homeland Security**
**United States Coast Guard**
*Information Technology Management Letter*
September 30, 2008

# Appendix B

# FY2008 Notices of IT Findings and Recommendations – Coast Guard

**Department of Homeland Security**
**United States Coast Guard**
*Information Technology Management Letter*
September 30, 2008

**Notice of Findings and Recommendations – Definition of Risk Ratings**:**

The Notices of Findings and Recommendations (NFR) were risk ranked as High, Medium, and Low** based upon the potential impact that each weakness could have on Coast Guard's information technology (IT) general control environment and the integrity of the financial data residing on Coast Guard's financial systems, and the pervasiveness of the weakness.

** **The risk ratings are intended only to assist management in prioritizing corrective actions**, considering the potential benefit of the corrective action to strengthen the IT general control environment and/or the integrity of the DHS consolidated financial statements. The risk ratings, used in this context, are not defined by *Government Auditing Standards*, issued by the Comptroller General of the United States, or the American Institute of Certified Public Accountants (AICPA) Professional Standards, and do not necessarily correlate to a significant deficiency, as defined by the AICPA Standards and reported in our *Independent Auditors' Report* on the consolidated balance sheet of DHS as of September 30, 2008, dated November 14, 2008.

Correction of some higher risk findings may help mitigate the severity of lower risk findings, and possibly function as a compensating control. In addition, analysis was conducted collectively on all NFRs to assess connections between individual NFRs, which when joined together could lead to a control weakness occurring with more likelihood and/or higher impact potential.

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

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

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

**Department of Homeland Security**
**United States Coast Guard**
*Information Technology Management Letter*
September 30, 2008

# United States Coast Guard
# FY2008 Information Technology
# Notification of Findings and Recommendations – Detail

**Department of Homeland Security**
**United States Coast Guard**
*Information Technology Management Letter*
September 30, 2008

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

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|---|---|---|---|---|---|
| CG-IT-08-01 | The ) Continuity of Operations Plan (COOP) has not been updated to reflect the results of testing the COOP, and the Business Continuity Plans for each division have not been finalized. | Update the COOP as the result of its testing and finalize the applicable supporting Business Continuity Plans. | | X | Low |
| CG-IT-08-06 | During the first half of the fiscal year the contract with the software vendor was still in place, and no corrective action had taken place related to the prior year recommendation. Therefore, the risk exists that the condition was present for the majority of the fiscal year (October 1, 2007 through April 1, 2008). However, due to the Coast Guard decision to terminate the contract with their software vendor and the Coast Guard decision to suspend all Software Problem Reports (SPRs) and Software Change Requests (SCRs), the condition did not exist beyond the date of these 2 events. | • Enhance existing Configuration Management/Change Management policies and procedures to explicitly address security configurations and software patches (e.g., those associated with system/application "builds", service packs, and maintenance releases) to better ensure compliance with DHS requirements and NIST guidance.<br>• Communicate with and educate affected staff regarding these improved policies and procedures.<br>• Develop, communicate, and implement procedures to periodically review system changes and system baselines. | | X | High |
| CG-IT-08-07 | We determined that Coast Guard's has not implemented the following password requirements:<br>• Passwords shall contain special characters<br>• Passwords shall not contain any dictionary word<br>• Passwords shall not contain any proper noun or the | • Continue with the plans to upgrade the operating system in order to enforce password complexity requirements to meet DHS Sensitive System Policy Directive 4300A.<br>• Continue to implement mitigating controls to | | X | Low |

**Department of Homeland Security**
**United States Coast Guard**
*Information Technology Management Letter*
September 30, 2008

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|---|---|---|---|---|---|
| | name of any person, pet, child, or fictional character<br>• 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<br>• Passwords shall not contain any simple pattern of letters or numbers, such as "qwerty" or "xyz123"<br>• 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<br>• Passwords shall not be the same as the User ID<br><br>While compensating controls were implemented to reduce the risk of unauthorized access, they unto themselves do not remove the potential risk from occurring. | reduce the risk of unauthorized individuals gaining access to the system.<br>• Educate all employees and contractors of DHS Sensitive System Policy Directive 4300A password requirements so they can set their passwords in accordance with policy despite the systems inability to enforce them. | | | |
| CG-IT-08-10 | Coast Guard has developed but not yet implemented policies and procedures to require that a favorably adjudicated background investigation be completed for all contractor personnel. | Create and implement contractor background investigation policies and procedures in order to establish requirements and ensure compliance with DHS Sensitive System Policy Directive 4300A. This includes the verification that all contracts issued by the Coast Guard include the appropriate Coast Guard position sensitivity designation requirements for contracted personnel. | | X | High |
| CG-IT-08-14 | Coast Guard has not finalized the Role-Based Training for Coast Guard Information Assurance Professionals Commandant Instruction, which will require all Coast Guard members, employees, and contractors with significant IT security responsibilities to receive initial specialized training and annual refresher training thereafter. The online Training Management Tool, which will track compliance, will not be implemented until the Role-Based | • Continue efforts to finalize and implement the Role-Based Training for Coast Guard Information Assurance Professionals Commandant Instruction which would require personnel with significant information security responsibilities to complete specialized role-based training on an annual basis. | | X | Medium |

**Department of Homeland Security**
**United States Coast Guard**
*Information Technology Management Letter*
September 30, 2008

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|---|---|---|---|---|---|
| | Training is implemented. | • Develop and deploy this specialized role-based training throughout the Coast Guard.<br>• Implement the use of the Training Management Tool in order to track and verify specialized role-based training requirements compliance. | | | |
| CG-IT-08-15 | Until August 2008, configuration management weaknesses continue to exist on hosts supporting the Naval Electronics | Through our test work, we determined that the prior year control weakness has been remediated prior to the fiscal year-end; therefore, no recommendation is required. | | | Low |
| CG-IT-08-17 | Although has made significant progress in remediation, we were unable to verify that is consistently remediating the vulnerabilities identified by the scans in order to make it an effective mitigating control for the application. | Continue to use the currently implemented mitigating controls for those DHS password requirements that cannot be enforced by the system. Specifically, should continue to routinely use the scanner and remediate any identified password weakness vulnerabilities. | | | Low |
| CG-IT-08-22 | Until August 15, 2008, when corrective actions were successfully implemented, password rules had not been appropriately configured for the database. We noted that:<br>• does not require passwords to be a minimum of eight characters;<br>• does not require a combination of alphabetic, numeric, and special characters;<br>• does not restrict dictionary words;<br>• does not restrict simple pattern passwords;<br>• does not restrict dictionary words spelled | Through our test work, we determined that the prior year control weaknesses was remediated prior to the fiscal year-end, therefore, no recommendation is required for this NFR. | | | Medium |

**Department of Homeland Security**
**United States Coast Guard**
*Information Technology Management Letter*
September 30, 2008

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|---|---|---|---|---|---|
| | backwards;<br>• does not restrict the use of proper names; and<br>• does not restrict the use of the employee's user ID | | | | |
| CG-IT-08-23 | Policies and procedures have not been developed and implemented for the manual periodic review of audit logs. As a result, audit logs are not periodically reviewed. | • Develop procedures for the periodic review of the manual audit logs in accordance with DHS policy.<br>• Ensure that an entity independent of the personnel administering the application reviews system audit trails on a regular basis as part of a more comprehensive continuous monitoring program.<br>• Ensure audit log files are configured, retained, and archived in compliance with DHS policy. | | X | Medium |
| CG-IT-08-25 | We determined the following weaknesses associated with the change controls:<br>• Procedures have been created and implemented for the quarterly review of developer and analyst roles. However, the procedures do not include the review of all other user accounts to ensure that all terminated individuals no longer have active accounts, that inactive accounts are locked, and that privileges associated with each individual are still authorized and | • Develop and implement procedures to require a periodic review of all accounts and their associated privileges. These procedures should include steps to verify that all terminated individuals no longer have active accounts, that inactive accounts are locked and that privileges associated with each individual are still authorized and necessary.<br>• Continue to reduce the number of tables that can be updated to ensure that each user has a business need to update each table.<br>• Document a mapping between the flow roles and the associated database tables | | X | Medium |

**Department of Homeland Security**
**United States Coast Guard**
*Information Technology Management Letter*
September 30, 2008

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|---|---|---|---|---|---|
| | necessary.<br>• 529 users have unlocked database accounts with access to the . Therefore, the number of users with the role has increased by 141 users from the 388 users noted during FY 2007. Additionally, a mapping of flow roles within the application to the tables that can be updated within the database has not been created. Therefore, we are unable to perform an analysis of the flow roles and the associated tables that are affected to determine whether access is appropriately restricted.<br>• The password configurations for the and profiles will not be updated to be in compliance with DHS guidance until after the database upgrade. Since no improvements have been made in regards to the password configuration, we determined that the password configurations continue to not meet the following DHS requirement of having a user password contain at least one special character. | that are affected.<br>• Continue with plans to complete the database upgrade and configure the password requirements to be in compliance with DHS guidance. | | | |
| CG-IT-08-27 | We noted that Coast Guard was unable to provide sufficient evidence of the following:<br>- access request forms are documented and approved;<br>- user accounts are revalidated annually; and<br>- access is revoked in a timely manner for employees or contractors that have left Coast Guard or are reassigned to other duties. | • Establish and enforce procedures to ensure access request forms are documented, approved, and provided to prior to establishing user account.<br>• Continue to develop and implement policy and procedures for re-validating user accounts in order to meet the requirements of | | X | Medium |

**Department of Homeland Security**
**United States Coast Guard**
*Information Technology Management Letter*
September 30, 2008

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|---|---|---|---|---|---|
| | | DHS Sensitive System Policy Directive 4300A.<br>• Establish and enforce procedures to ensure access is revoked for employees or contractors who leave the Coast Guard or are reassigned to other duties in order to meet the requirements of DHS Sensitive System Policy Directive 4300A. | | | |
| CG-IT-08-31 | Coast Guard's controls over the scripting process remain ineffective. Weaknesses were noted in controls over script implementation, approvals and testing, as well as active script modification. In addition, Coast Guard has not maintained or developed a population of scripts run since the inception of in 2003 nor has it performed a historical analysis of script impact on the cumulative balances in permanent accounts of the financial statements. Specifically:<br>• Coast Guard lacks a formal process to distinguish between the module lead approvers for script approval requests;<br>• The Procedures for Data Scripts do not specifically state the testing and documentation requirements for blanket approval scripts and this policy remains in draft form;<br>• Coast Guard does not monitor scripts run in the database through audit logging and has not developed a technical solution to monitor who accesses the database through to run scripts or | In order for management to assert to any financial statement line items, Coast Guard should:<br>• Continue to design, document, implement, and demonstrate the effectiveness of internal controls associated with the active (current and future) scripts.<br>• Identify and evaluate the historical scripts (all those implemented prior to those identified in recommendation 1 above) to determine the financial statement impact on cumulative balances in permanent accounts; and develop and maintain supporting procedures related to each script.<br>With respect to procedures already in place, Coast Guard should:<br>• Continue to update script policies and procedures to include clear guidance over module lead approvers, testing and documentation requirements, monitoring/audit log reviews, and blanket approval | | X | High |

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|---|---|---|---|---|---|
| | review what scripts are run;<br>• The [redacted] does not consistently include all testing, approval, and implementation documentation for all scripts; and<br>• Coast Guard has not completed [redacted] documentation for all scripts executed since their implementation. | requirements<br>• Finalize and implement policies and procedures governing the script change control process including completing records within the [redacted] for all executed scripts and ensuring that all scripts are tested in an appropriate test environment prior to being put into production.<br>Regarding the actual scripts themselves, Coast Guard should:<br>• Determine the root causes and specific detailed actions necessary to correct the conditions that resulted in scripts, for the total population of scripts run at [redacted] in order to develop system upgrades that would eliminate the use of some of the scripts.<br>• Continue efforts to complete an in-depth analysis of active scripts, with the following objectives:<br>o All changes to active scripts and new scripts should be subject to an appropriate software change control process to include testing, reviews, and approvals.<br>o All active scripts should be reviewed for impact on financial statement balances. | | | |
| CG-IT-08-32 | Although Coast Guard [redacted] has mandated the use of [redacted] to maintain and track contracted personnel data, procedures surrounding | • Finalize the procedure documentation and communicate/distribute the procedures | | X | Medium |

**Department of Homeland Security**
**United States Coast Guard**
*Information Technology Management Letter*
September 30, 2008

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|---|---|---|---|---|---|
| | this process have not been formally documented. As a result, we were unable to determine the effectiveness of the controls in place for contractor tracking. | • Continuously monitor controls over to verify that contractor data within the system remains current and accurate. | | | |
| CG-IT-08-33 | Coast Guard does not consistently notify system owners that individuals are terminating from the Coast Guard so that system accounts can be updated timely. | • Implement an automated process/system that will notify system owners of terminated contractor, military, and civilian personnel.<br>• Finalize and implement entity management policies and procedures for verifying that terminated user accounts have been successfully removed. | X | | Medium |
| CG-IT-08-34 | All are not being appropriately reviewed and approved by management prior to development/deployment. In addition, developers and testers are not updating information in the tool in a timely manner. | • Reconfigure the tool to not allow the automatic approval of upon creation.<br>• Enforce established change control policies and procedures by reviewing and approving: a) all software change requests prior to developing the changes; b) test results; and c) all test-developed changes prior to deploying the changes into the production environment.<br>• Ensure that the development and test staff adheres to the policies and procedures for updating software change control information within the tool. | X | | Medium |
| CG-IT-08-35 | We noted that control weaknesses still exist within the design of 's Configuration Management policies and procedures for and , as well as the operating effectiveness of those controls. Our test work over the design of the change controls covered both periods of the change control environment; however, our | • : Develop, implement, communicate, and enforce procedures regarding how changes are to be controlled, documented, tracked, and reviewed as these changes progress through testing and into production. | | X | High |

**Department of Homeland Security**
**United States Coast Guard**
*Information Technology Management Letter*
September 30, 2008

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|---|---|---|---|---|---|
| | testing of operating effectiveness covered only the period of start of the fiscal year through March 2008, since no changes were made to and from April through the remainder of the fiscal year. | • Coast Guard Develop, implement, communicate, and enforce procedures regarding how change control documentation will be maintained, reviewed, and validated in accordance with DHS Sensitive System Policy Directive 4300A. | | | |
| CG-IT-08-36 | Configuration management weaknesses continue to exist on hosts supporting the applications and the underlying .<br><br>Note: Due to the nature of this testing, see the tables in the NFR for the specific conditions. | • Implement the corrective actions for the recommendations listed within the NFR.<br><br>• Continue to implement policies and procedures to ensure that the tested and deployed software builds include required software patches and have current, correct, and compliant security configuration settings. | | X | Medium |
| CG-IT-08-37 | Security patch management weaknesses continue to exist on hosts supporting the applications and<br><br>Note: Due to the nature of this testing, see the tables in the NFR for the specific conditions. | • Implement the corrective actions for the recommendations listed within the NFR.<br><br>• Continue to implement polices and procedures to ensure that the tested and deployed software builds include required software patches and have current, correct, and compliant security configuration settings. | | X | Medium |
| CG-IT-08-40 | Although Coast Guard is in the process of completing background investigations for all civilian employees, this has not been completed. Additionally, Coast Guard has set its position sensitivity designations to Low for the majority of its employees. However, DHS requires position sensitivity designations no less than Moderate which equates to a Minimum Background Investigation (MBI). Therefore, we determined that the | • Perform initial background investigations and re-investigations for civilian employees in accordance with position sensitivity designations at no less than the Moderate level as required by DHS directives; and<br><br>• Conduct civilian background re-investigations every ten (10) years, as required by DHS directives, to ensure that each employee has a | | X | Medium |

**Department of Homeland Security**
**United States Coast Guard**
*Information Technology Management Letter*
September 30, 2008

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|---|---|---|---|---|---|
| | conditions noted in prior year NFR CG-IT-07-40 have not been remediated. | favorably adjudicated and valid MBI. | | | |
| CG-IT-08-41 | has not completed the risk assessment for the , and the is still in draft form. | Finalize and implement the Certification and Accreditation Package for the in accordance with DHS and NIST guidance. | | X | Low |
| CG-IT-08-42 | During prior financial statement audits dating back to FY 2003, we noted that implementation and oversight of the Coast Guard's information security policy and procedures was fragmented among the organizations responsible for operating various applications/systems. In FY 2008, significant improvements have been made in some areas; however, improvements are still warranted at the Coast Guard data centers/locations that operate and process key Coast Guard financial information. Improvements are needed especially in the areas of change control and to a lesser extent, access to data and programs. These two key areas were the subject of significant findings identified and recommendations that were made during the audit.<br><br>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.* | • Continue to implement, improve, and monitor compliance with DHS, Coast Guard, and Federal security policies and procedures in the areas of:<br>- Change Controls<br>• Continue to improve and monitor compliance with DHS, Coast Guard, and Federal security policies and procedures in the areas of:<br>- Access Controls<br>- Entity-wide Security Planning<br>- Service Continuity<br>- Segregation of Duties<br>- System Software<br>- Application Controls<br>• Develop and implement corrective action plans to address and remediate the NFRs issued during the FY 2008 audit. These corrective action plans should be developed from the perspective of the identified root cause of the weakness. In addition, the IT NFRs should not be assessed as individual issues to fix, but instead, should be assessed collectively based upon the area where the weakness was identified. This approach | | X | High |

**Department of Homeland Security**
**United States Coast Guard**
*Information Technology Management Letter*
September 30, 2008

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|---|---|---|---|---|---|
| | | would enable a corrective action that would be more holistic in nature, thereby leading to a more efficient and effective process of fixing those controls which are not operating effectively. | | | |
| CG-IT-08-43 | During our testwork over and access accounts, we noted that controls over user account authorizations and controls over user account reviews were not operating effectively. | • Implement and document the ( ) user access review procedures to include all access privileges and include supervisors in each review.<br>• Update procedures to ensure that a documented and approved access authorization request is completed for each individual prior to granting him/her access to the and applications or databases. | X | | Medium |

*** Risk ratings are only intended to assist management in prioritizing corrective actions. Risk ratings in this context do not correlate to definitions of control deficiencies as identified by the AICPA.**

# Appendix C

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

| | | | Disposition | |
|---|---|---|---|---|
| **Component** | **NFR #** | **Description** | **Closed** | **Repeat** |
| CG | 07-01 | has replaced the Disaster Recovery Business Continuity concept with the development of a Continuity of Operations Plan (COOP) which addresses disaster recovery, business continuity and continuity of government. However, the COOP is in draft form and has not yet been tested and the Memorandum of Understanding with the for reciprocal services is still in draft form as well. | | 08-01 |
| CG | 07-02 | The change control policy does not detail requirements for requesting, testing, and approving changes. Furthermore, there are no formalized requirements pertaining to retention of supporting documentation and the roles and responsibilities of personnel in the process. Additionally, the policy does not adequately reflect the environment and change control process that was utilized during the upgrade performed during FY07. Examples of inconsistencies include the references to service packs, data fixes, and the testing procedures completed. | X | |
| CG | 07-03 | The system does not meet DHS password complexity requirements, and the system is not scheduled for decommissioning until December 2007. | X | |
| CG | 07-04 | We identified the following account terminations weaknesses at :<br><br>• From October 1, 2006 through July 24, 2007, had not yet implemented policies and procedures for use in managing terminations, including the use of the Outgoing Personnel Form.<br><br>• Outgoing Personnel Forms were not completed for one of five individuals selected for testing.<br><br>• One terminated individual remained active within until 90 days after his last logon before his account was revoked as part of the account review process.<br><br>• 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 | X | |

| | | | Disposition | |
|---|---|---|---|---|
| **Component** | **NFR #** | **Description** | **Closed** | **Repeat** |
| | | potential risk to the data. | | |
| CG | 07-05 | Policies and procedures regarding requesting, authorizing, testing, and approving operating system changes are not consistently followed. Additionally, a testing baseline standard has not been established to ensure that operating system changes have not adversely affected portions of the system that were not intended to be affected. Lastly, was unable to reconcile changes to the operating system to a listing of authorized operating system changes to ensure that all changes have been appropriately approved. | X | |
| CG | 07-06 | The contract Coast Guard has with the and software vendor does not include security configuration requirements that must be adhered to during the configuration management process. Consequently, and builds and maintenance packs may not be configured and implemented with comprehensive security configuration requirements. CG recognizes the absence of security requirements and indicated that the contract with the vendor will be reassessed in 2008 during the contract renewal process with Coast Guard and corrective actions will be taken at that time. | | 08-06 |
| CG | 07-07 | has not implemented the following password requirements:<br>• Passwords shall contain special characters<br>• Passwords shall not contain any dictionary word<br>• Passwords shall not contain any proper noun or name of any person, pet, child, or fictional character<br>• 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<br>• Passwords shall not contain any simple pattern of letters or numbers, such as qwerty or xyz123<br>• 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<br>• Passwords shall not be the same as the User ID | | 08-07 |

**Department of Homeland Security**
**United States Coast Guard**
*Information Technology Management Letter*
September 30, 2008

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

| | | | Disposition | |
|---|---|---|---|---|
| **Component** | **NFR #** | **Description** | **Closed** | **Repeat** |
| | | scope of security responsibilities addressed in DHS requirements. | | |
| CG | 07-15 | The application database ( ) is using version , which is no longer supported by the vendor. Additionally, an account on the database has a password the same as account name ( ). The database also has a directory manipulation vulnerability in the binary file . | | 08-15 |
| CG | 07-16 | has developed and implemented policies and procedures that address the review of inactive accounts and lock those that have been inactive for 90 days. However, DHS guidance requires that inactive accounts be locked after 30 days. | X | |
| CG | 07-17 | access control weaknesses were noted:<br>• Passwords shall contain special characters<br>• Passwords shall not contain any dictionary word<br>• Passwords shall not contain any proper noun or name of any person, pet, child, or fictional character<br>• 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<br>• Passwords shall not contain any simple pattern of letters or numbers, such as qwerty or xyz123<br>• 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 | | 08-17 |
| CG | 07-18 | access control weaknesses were noted:<br>• Passwords shall contain special characters<br>• Passwords shall not contain any dictionary word<br>• Passwords shall not contain any proper noun or name of any person, pet, child, or fictional character<br>• Passwords shall not contain any employee serial number, social | X | |

| | | | Disposition | |
|---|---|---|---|---|
| **Component** | **NFR #** | **Description** | **Closed** | **Repeat** |
| | | security number, birth date, phone number, or any information that could be readily guessed about the creator of the password<br><br>• Passwords shall not contain any simple pattern of letters or numbers, such as qwerty or xyz123<br><br>• 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<br><br>• accounts of terminated individuals are not removed in a timely manner, including one individual who had user account management capabilities within the system. Additionally, application and database accounts are not being reviewed for appropriateness. | | |
| CG | 07-19 | access control weaknesses were noted:<br><br>• Documented access request forms could not be located for two new users granted access to the application.<br><br>• accounts are not immediately disabled upon an employee's termination.<br><br>• Procedures have not been developed to require periodic account reviews to be performed to ensure that all users and their associated privileges are appropriate.<br><br>• has not been configured to track and deactivate accounts that have not been used in 30 days.<br><br>• An excessive number of individuals have user administrator capabilities within until the implementation of the centralized user management (August 19, 2007).<br><br>• Password configuration is not in compliance with DHS guidance. | X | |
| CG | 07-20 | The periodic review of accounts only covers 1% of all user accounts with roles greater than and that have been modified within the last 90 days. The population that is validated during this review was found to be insufficient as the user population of the system is approximately 60,000 user | X | |

| | | | Disposition | |
|---|---|---|---|---|
| **Component** | **NFR #** | **Description** | **Closed** | **Repeat** |
| | | accounts. | | |
| CG | 07-21 | The procedures for the periodic review of user accounts does not require a review of all active user accounts and privileges to be performed and validated. | X | |
| CG | 07-22 | Password configuration weaknesses associated with the application. Also, the application is configured to terminate idle sessions after 30 minutes of inactivity instead of 20 minutes. | | 08-22 |
| CG | 07-23 | While audit logging has been turned on for the database, reviews of actions being taken on that database are still not being performed. | | 08-23 |
| CG | 07-24 | Policies and procedures regarding data used for the Coast Guard environmental liability report on the DHS Consolidated balance sheet have been developed but are currently in draft form and have not been implemented. | X | |
| CG | 07-25 | The following access control weaknesses were identified within :<br>• Excessive access exists within the database;<br>• Password configurations for the and 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 profile.<br>• Audit logging has not been enabled within the application or database.<br>• Documented access request forms could not be located for nine out of 22 new users granted access to the application. Additionally, although the automated access request forms for the other 13 out of 22 new 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.<br>• Individuals who are no longer employed with were | | 08-25 |

| | | | Disposition | |
|---|---|---|---|---|
| **Component** | **NFR #** | **Description** | **Closed** | **Repeat** |
| | | found to have active accounts within .<br>• account reviews have not been performed on a periodic basis. | | |
| CG | 07-26 | has been configured to automatically end date accounts that have been inactive for six months. However, DHS requirements require accounts to be disabled after 30 days of inactivity. | X | |
| CG | 07-27 | Accounts within that have been inactive for more than 90 days have not been disabled, access request authorization forms were unavailable for 19 of the 30 individuals who had accounts created during FY07, a recertification of accounts is not performed, and terminated employees are not deactivated in a timely manner. | | 08-27 |
| CG | 07-28 | From the sample selected, a developer had elevated production privileges in . Also, two procedures/packages were added to privileges. | X | |
| CG | 07-29 | The individual who enters an applicant's data into the also has the ability to hire the applicant in the system | NFR transferred to Audit Team. See Financial NFR 08-32. | |
| CG | 07-30 | functional change control policies and procedures did not reflect the change control process for the changes and did not adequately detail guidance for the change control process. Specifically, the policy does not include requirements for requesting, testing, and approving changes prior to implementing the functional change into the production environment. | X | |
| CG | 07-31 | Coast Guard has only eliminated a small number of the scripts used on a consistent basis and is projecting that this approach will continue into the delivery of and beyond. Additionally, we noted that as of April 27, 2007, 240 scripts were run during a week long period. The number and type of scripts that are executed during any one period in time varies from week to week depending on the issues encountered. Of the 240 scripts noted during this particular week, several were run numerous times for the same software gap. Consequently, has not fully integrated the two change control processes or eliminated the need for the scripts. | | 08-31 |
| CG | 07-32 | Coast Guard does not maintain a centralized listing of contracted personnel, including employment status, such as start date and | | 08-32 |

| | | | Disposition | |
|---|---|---|---|---|
| **Component** | **NFR #** | **Description** | **Closed** | **Repeat** |
| | | termination date, so that system accounts can be timely updated. | | |
| CG | 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. | | 08-33 |
| CG | 07-34 | is not consistently implementing policies and procedures regarding the change control process. Specifically, supporting documentation is not maintained for all changes and emergency changes. Additionally, changes may be approved prior to the change being tested and passing the test. | | 08-34 |
| CG | 07-35 | Policies and procedures for the overall change control process surrounding and changes and emergency changes are inadequate. Specifically, the policies and procedures do not fully include guidance for the roles and responsibilities possesses in the change control process. Additionally, they do not include detailed requirements and guidance on requesting changes, initial approvals, testing, final approvals and documentation retention requirements for changes made to the system. | | 08-35 |
| CG | 07-36 | Configuration management weaknesses exist on hosts supporting the , , and applications and . | | 08-36 |
| CG | 07-37 | Patch management weaknesses exist on hosts supporting the , , and applications and . | | 08-37 |
| CG | 07-38 | Coast Guard's ) program changes are implemented in production prior to approval from the Financial Reports & Analysis Branch Chief or the Financial Control & Information Division Chief as required by policy and procedures. Additionally, systems personnel move program changes into production without signing off on the Request Change to Database form as required by the procedures. | X | |
| CG | 07-39 | Coast Guard has not completed the process of filing the background investigation records that were recovered and recreating the records that were not found during the migration of records from the Department of Transportation to DHS. | X | |
| CG | 07-40 | Civilian background investigations and reinvestigations are not being performed in accordance with DHS Minimum Background Investigation standards per DHS Sensitive System Policy Directive | | 08-40 |

| | | | Disposition | |
|---|---|---|---|---|
| **Component** | **NFR #** | **Description** | **Closed** | **Repeat** |
| | | 4300A. | | |
| CG | 07-41 | Per review of the Certification and Accreditation (C&A) package, we noted that system boundary definitions do not fully reflect the systems environment in which Coast Guard operates, C&A does not reflect system changes made in the upgrade, and is classified by Coast Guard as a subsystem of , however, there is no documentation within the that defines as a subsystem and addresses the appropriate security controls for in this capacity according to NIST requirements for subsystems | | 08-41 |
| CG | 07-42 | Coast Guard is not compliant with the *Federal Financial Management Improvement Act* from an information technology perspective and in the following areas:<br>• Computer Security Act Requirements, including aspects of the *Federal Information Security Management Act*<br>• System Documentation<br>• Internal Controls<br>• Training and User Support<br>• System Maintenance<br>• System Information Flow | | 08-42 |

# Appendix D

# Management Comments

**Department of Homeland Security**
**United States Coast Guard**
*Information Technology Management Letter*
September 30, 2008

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 2 2009

**MEMORANDUM**

From: D. T. Glenn, RADM
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 2008 DHS FINANCIAL STATEMENT AUDIT REPSONSE

Ref: (a) Draft Audit Report Memorandum of 13 Feb 2009

1. The Coast Guard has reviewed reference (a) and concurs with the findings and recommendations. The Coast Guard will continue work with DHS OCFO in pursuing the strategy that will be briefed April 2009 to DHS OCFO that will incorporate the results of this audit.

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

#

Copy: COMDT (CG-8)

**Department of Homeland Security**
**United States Coast Guard**
*Information Technology Management Letter*
September 30, 2008

**Report Distribution**

**Department of Homeland Security**

Secretary
Acting Deputy Secretary
Chief of Staff for Operations
Chief of Staff for Policy
Acting General Counsel
Executive Secretariat
Under Secretary, Management
Acting Assistant Commissioner, USCG
DHS Chief Information Officer
DHS Chief Financial Officer
Chief Financial Officer, USCG
Chief Information Officer, USCG
DHS 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
USCG Audit Liaison

**Office of Management and Budget**

Chief, Homeland Security Branch
DHS OIG Budget Examiner

**Congress**

Congressional Oversight and Appropriations Committees as Appropriate

## ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

## OIG HOTLINE

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

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigations - Hotline,
  245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

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