Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the United States Coast Guard Component of the FY 2010 DHS Financial Statement Audit

OIG-11-80

May 2011

Office of Inspector General

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

Homeland Security

MAY 06 2011

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 component of the FY 2010 DHS financial statement audit as of September 30, 2010. It contains observations and recommendations related to information technology internal control that were summarized in the *Independent Auditors' Report,* dated November 12, 2010 and presents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit procedures at the Coast Guard component in support of the DHS FY 2010 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated March 22, 2011 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. We trust that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Frank Deffer
Assistant Inspector General
Office of Information Technology Audits

KPMG LLP
2001 M Street, NW
Washington, DC 20036-3389

March 22, 2011

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 balance sheet of the U.S. Department of Homeland Security (DHS or Department), as of September 30, 2010 and the related statement of custodial activity for the year then ended (herein after referred to as "financial statements"). We were also engaged to examine the Department's internal control over financial reporting of the balance sheet as of September 30, 2010 and the statement of custodial activity for the year then ended. We were not engaged to audit the statements of net cost, changes in net position, and budgetary resources as of September 30, 2010 (hereinafter referred to as "other fiscal year (FY) 2010 financial statements"), or to examine internal control over financial reporting over the other FY 2010 financial statements.

Because of matters discussed in our *Independent Auditors' Report,* dated November 12, 2010, the scope of our work was not sufficient to enable us to express, and we did not express, an opinion on the financial statements or on the effectiveness of DHS' internal control over financial reporting of the balance sheet as of September 30, 2010, and related statement of custodial activity for the year then ended. Additional deficiencies in internal control over financial reporting, potentially including additional material weaknesses and significant deficiencies, may have been identified and reported had we been able to perform all procedures necessary to express an opinion on the financial statements or on the effectiveness of DHS' internal control over financial reporting of the balance sheet as of September 30, 2010, and related statement of custodial activity for the year then ended; and had we been engaged to audit the other FY 2010 financial statements, and to examine internal control over financial reporting over the other FY 2010 financial statements.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

The United States Coast Guard (Coast Guard or USCG) is a component of DHS. During our audit engagement, we noted certain matters in the areas of information technology (IT) configuration management, security management, access controls, and segregation of duties with respect to Coast Guard's financial systems information technology (IT) general controls, which we believe contribute to an IT material weakness at the DHS level. These matters are described in the *IT General Control and Financial System Functionality Findings and Recommendations by Audit Area* section of this letter.

The material weakness described above is presented in our *Independent Auditors' Report*, dated November 12, 2010. This letter represents the separate limited distribution letter mentioned in that report.

The control deficiencies described herein have been discussed with the appropriate members of management, and communicated through a Notice of Finding and Recommendation (NFR).

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate. We aim to use our knowledge of Coast Guard gained during our audit engagement to make comments and suggestions that are intended to improve internal control over financial reporting or result in other operating efficiencies. 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. We have provided a description of key Coast Guard financial systems and IT infrastructure within the scope of our engagement to audit the FY 2010 DHS financial statements in Appendix A; a listing of the FY 2010 IT Notices of Findings and Recommendations at Coast Guard in Appendix B; and the status of the prior year NFRs and a comparison to current year NFRs in Appendix C; and Coast Guard management's written response in Appendix D. Our comments related to certain additional matters have been presented in a separate letter to the Office of Inspector General and the Coast Guard Chief Financial Officer.

Coast Guard's written response to our comments and recommendations, presented in Appendix D, has not been subjected to auditing procedures and, accordingly, we express no opinion on it.

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

Very truly yours,

KPMG LLP

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE, AND APPROACH

We were engaged to audit DHS' balance sheet as of September 30, 2010 and the related statement of custodial activity for the year then ended, we performed an evaluation of information technology general controls (ITGC) at Coast Guard, to assist in planning and performing our audit.

The *Federal Information System Controls Audit Manual* (FISCAM), issued by the Government Accountability Office (GAO), formed the basis of our ITGC evaluation procedures. The scope of the ITGC evaluation is further 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 five control functions to be essential to the effective operation of the ITGC environment.

- *Security Management (SM)* – Controls that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related security controls.
- *Access control (AC)* – Controls that limit and/or monitor access to computer resources (data, programs, equipment, and facilities) to protect against unauthorized modification, loss, and disclosure.
- *Configuration Management (CM)* – Controls that help to prevent the implementation of unauthorized programs or modifications to existing programs.
- *Segregation of duties (SD)* – Controls that constitute policies, procedures, and an organizational structure to prevent one individual from controlling key aspects of computer-related operations, thus deterring unauthorized actions or access to assets or records.
- *Contingency Planning (CP)* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

To complement our ITGC audit procedures, we also performed technical security testing for key network and system devices. The technical security testing was performed 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. Limited social engineering and after-hours physical security testing was also included in the scope of technical security testing.

Application controls were not tested for the year ending September 30, 2010 due to the nature of prior-year audit findings.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During fiscal year (FY) 2010, Coast Guard took corrective action to address nearly half of the prior year IT control weaknesses. For example, Coast Guard made improvements by strengthening its system security settings over some of its systems at the USCG Finance Center, strengthening account management and configuration management controls over the Workflow Imaging Network System (WINS), and improved the data center controls at the USCG Finance Center (FINCEN). However, during FY 2010, we continued to identify IT general control weaknesses at Coast Guard. The most significant weaknesses from a financial statement audit perspective are related to the controls over authorization, development, implementation, and tracking of IT scripts at FINCEN. These IT control deficiencies 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 deficiencies negatively impacted the internal controls over Coast Guard financial reporting and its operation and we consider them to contribute to a material weakness at the Department level under standards established by the American Institute of Certified Public Accountants. In addition, based upon the results of our test work, we noted that the Coast Guard did not fully comply with the Department's requirements under the *Federal Financial Management Improvement Act* (FFMIA).

In FY 2010, our IT audit work identified 28 IT findings, of which ten were repeat findings from the prior year and 18 were new findings. In addition, we determined that Coast Guard remediated eight IT findings identified in previous years. Specifically, the Coast Guard took actions to improve aspects of its user recertification process, data center physical security, and scanning for system vulnerabilities. The Coast Guard's remediation efforts have enabled us to expand our test work into areas that previously were not practical to test, considering management's acknowledgment of the existence of control deficiencies. Most of the new findings relate to IT systems that were added to our examination scope this year.

Collectively, these findings represent deficiencies in four of the five FISCAM key control areas. The FISCAM areas impacted included Security Management, Access Control, Segregation of Duties, and Configuration Management. We also considered the effects of financial systems functionality when testing internal controls since key Coast Guard financial systems are not compliant with FFMIA and are no longer supported by the original software provider. Financial system functionality limitations add to the challenge of addressing systemic internal control weaknesses and strengthening the control environment at the Coast Guard.

The majority of the findings indicate a 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) poorly, but improving, designed and operating IT script change control policies and procedures, 2) unverified access controls through the lack of user access privilege re-certifications, 3) entity-wide security program issues involving civilian and contractor background investigation weaknesses, 4) inadequately designed and operating audit log review policies and procedures, 5) physical security and security awareness, and 6) role-based training for individuals with elevated responsibilities.

These deficiencies 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 DHS' consolidated financial statements.

While the recommendations made by us 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 CONTROLS AND FINANCIAL SYSTEM FUNCTIONALITY FINDINGS

Findings and Recommendations:

Conditions: During the FY 2010 DHS Financial Statement Audit, Coast Guard segment, we identified the following IT and financial system control deficiencies that in the aggregate significantly contribute to the material weakness at the department level. Our findings are divided into two groupings: 1) financial systems controls and 2) IT system functionality.

Related to IT Financial Systems Controls

Configuration Management

We noted that Coast Guard's core financial system configuration management process controls are not operating effectively, and continue to present risks to DHS financial data confidentiality, integrity, and availability. Financial data in the general ledger may be compromised by automated and manual changes that are not adequately controlled. For example, the Coast Guard uses an IT scripting process to make updates to its core general ledger software as necessary to process financial data. During our FY 2010 testing, we noted that some previously identified control deficiencies were remediated (particularly with the implementation of a new script change management tool in the second half of FY 2010), while other deficiencies continued to exist. The remaining control deficiencies vary in significance. However, three key areas that impact the Coast Guard IT script control environment are:

- Script testing requirements – Limited testing requirements exist to guide FINCEN staff in the development of test plans and guidance over the functional testing that should be performed;
- Script testing environment – Not all script changes were tested in the appropriate test environments, as required; and
- Script audit logging process – The Coast Guard's core system databases are logging changes to tables as well as successful and unsuccessful logins. However, no reconciliation between the scripts run and the changes made to the database tables is being performed to monitor the script activities and ensure that all scripts run have been approved.

In addition, we noted weaknesses in the script change management process as it relates to the Internal Control over Financial Reporting (ICOFR) process (e.g., the financial statement impact of the changes to FINCEN core accounting system through the script change management process). The Coast Guard has not fully developed and implemented procedures to ensure that a script, planned to be run in production, has been through an appropriate level of review by a group of individuals thoroughly assessing if the script would have a financial statement impact. Furthermore, the rationale documenting the impact of the script, whether deemed as having financial impact or not, is not documented and retained for internal assessment or audit purposes. Internal controls that ensure the reliability of the scripting process must be effective throughout the year, but most importantly during the year-end close-out and financial reporting process.

Access Controls

- Procedures surrounding the use of monitoring reports over 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.
- Audit log reviews for key financial systems are not being conducted on all key information, and are not being retained for self-assessment and audit purposes.
- New user access forms are not retained for self-assessment and audit purposes. In addition, evidence of supervisory approval of new users was also not available for review.
- 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.
- Account re-certifications are not being retained for self-assessment and audit purposes.

Segregation of Duties

- Audit log reviews are being performed by the system administrator, who is not considered an independent party as required by DHS MD 4300A.

Security Management

- Background investigations for all civilian employees have not been completed and Coast Guard's civilian position sensitivity designation process is not in compliance with DHS guidance.
- Coast Guard procedures do not include specific guidance for the program managers on how to set the correct and consistent risk levels and position sensitivity designations for contract employees.
- Policies and procedures for key control areas are not adequately detailed to provide clear and complete control descriptions.
- There is a lack of a consistent contractor, civilian and military account termination notification process for Coast Guard systems.
- During our after-hours physical security and social engineering testing, we identified exceptions in the protection of sensitive user account information. The table on page 6 details the exceptions identified at the various locations tested.

After-Hours Physical Security Testing

We performed after-hours physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects include physical access to media and equipment that houses financial data and information residing on a Coast Guard employee's/contractor's desk, which could be used by others to gain unauthorized access to systems housing financial information. The testing was performed at various Coast Guard locations that process and/or maintain financial data. The table on the following page provides a summary of our testing results.

Security Weaknesses Observed During After Hours Physical Security Testing					
	Coast Guard Locations Tested				
Exceptions Noted	**Coast Guard Headquarters (HQ) – Jemal (CG-6)**	**Coast Guard HQ – Transpoint (CG-84)**	**Coast Guard Finance Center – Main**	**Coast Guard Finance Center - Annex**	**Total Exceptions by Type**
Passwords	3	4	2	0	**9**
For Official Use Only (FOUO) Documents	11	0	0	2	**13**
Keys/Badges	0	1	0	0	**1**
Personally Identifiable Information (PII)	0	1	3	0	**4**
Server Names/IP Addresses	0	0	0	3	**3**
Unsecured Laptops	1	2	0	0	**3**
Unsecured External Drives	4	10	0	2	**16**
Terminal root command left unattended	0	0	0	1	**1**
Directory structure map unsecured	0	0	0	1	**1**
Common Access Cards (CAC)	0	1	1	0	**2**
Secure ID Token PIN	2	0	0	0	**2**
Active computer left unattended	0	0	0	1	**1**
Total Exceptions by Location	**21**	**19**	**6**	**10**	**56**
Source: Coast Guard management, OIG, and KPMG direct observation and inspection of work areas. Note: Approximately 20-25 desks/offices were examined for each one of the columns in the above table.					

Social Engineering Testing

Social engineering is defined as the act of attempting to manipulate or deceive individuals into taking action that is inconsistent with DHS policies, such as divulging sensitive information or allowing/enabling computer system access. The term typically applies to deception for the purpose of information gathering, or gaining computer system access, as shown in the following table.

Location	Total Called	Total Answered	Number of people who provided a password
Coast Guard HQ	45	11	1
Coast Guard FINCEN	50	23	7

Recommendations: We recommend that the Coast Guard Chief Information Officer (CIO) 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.

Configuration Management:

We recommend that the Coast Guard CIO update the scripting policies and procedures to include additional and more detailed test documentation, develop training that addresses all aspects of script testing (including documentation of test documents) and provide training to appropriate CM staff, develop a resource plan (RP) with associated supporting business case(s) to address the database audit logging requirements, develop procedures and perform regular account revalidations for the Serena

application to ensure privileges remain appropriate, and conduct an assessment over the ICOFR process related to identifying and evaluating scripts that have a financial statement impact.

Access Controls:

- Update account management procedures to effectively track and retain user access documentation;
- Update account management procedures to provide clear guidance regarding the use of user access forms and update the access form to include an approval signature line;
- Configure Coast Guard applications to enforce the strong password and password history requirements described in the DHS MD 4300A Policy Directive and update all impacted system documentation accordingly;
- Update standard operating procedures to address the audit log review and retention procedures;
- Update audit log review procedures within specific procedures to include more detail in recording the results of the review of the audit logs;
- Continue with ongoing efforts for identifying, designing, and implementing automated tools to assist in audit log collection, storage, analysis, and reporting which will further improve consistency, timeliness, and accuracy of the reviews when compared with labor and time intensive manual processes;
- Develop and document an enterprise-wide process that will notify all impacted system owners of terminated, transferred, or retired contractor, military, and civilian personnel;
- Continue to update procedures to require an annual review of 100% of user accounts for the key financial systems and their associated privileges that are greater than read-only to ensure access is still required;
- Develop a RP with associated supporting business case(s) to address the installation of Service Pack 3 on all applicable workstations and/or upgrade the operating systems of these workstations to the Coast Guard's Standard Image; and
- Develop a RP with associated supporting business case(s) to address the server operating system upgrades to include a technical analysis to ensure server upgrades do not adversely affect system operation.

Segregation of Duties:

- Implement separation of duties for Coast Guard System audit log reviews.

Security Management:

- Update the policies and procedures currently in place to include clear guidance for Program Managers and Contracting Officers to assign contractor risk level(s) and position sensitivity designation requirements in order to verify that all contracts issued by the Coast Guard include the appropriate investigation level requirements;
- Perform initial background investigations and re-investigations for civilian employees in accordance with DHS directives;

- Update the annual Information Assurance (IA) training to include more robust office "physical security" and "clean desk" guidance and instruction and explicitly test individuals during the training on these topic areas;
- Implement enterprise-wide and site-specific processes for verifying the effectiveness of this training via mechanisms such as scheduled and ad hoc desk checks, training follow-ups, and other management controls;
- Develop, document, communicate, train, test, and continuously maintain policies and procedures for the cited IT control and process areas;
- Continue to implement Commandant Instruction *Information Assurance Professional Certification*; and
- Improve and utilize its manual tracking process until such time that the Direct Access implementation is in place.

Related to Financial System Functionality

Conditions: We noted that certain financial system functionality limitations are contributing to control deficiencies, inhibiting progress on corrective actions for Coast Guard, and preventing the Coast Guard from improving the efficiency and reliability of its financial reporting processes. Some of the financial system limitations lead to extensive manual and redundant procedures to process transactions, to verify the accuracy of data, and to prepare financial statements. Systemic conditions related to financial system functionality include:

- As noted above, Coast Guard's core financial system configuration management process is not operating effectively due to inadequate controls over IT scripts. The IT script process was instituted as a solution primarily to compensate for system functionality and data quality issues.
- Financial system audit logs are not readily generated and reviewed, as some of the financial systems are lacking the capability to perform this task efficiently.
- Production versions of operational financial systems are outdated and do not provide the necessary core functional capabilities (e.g., general ledger capabilities). Financial systems functionality limitations are preventing the Coast Guard from establishing automated processes and application controls that would improve accuracy and reliability, and facilitate efficient processing of certain financial data such as:
  - Ensuring proper segregation of duties and access rights such as automating the procurement process to ensure that only individuals who have proper contract authority can approve transactions or setting system access rights within the fixed asset subsidiary ledger;
  - Maintaining sufficient data to support Fund Balance with Treasury related transactions, including suspense activity;
  - Maintaining adequate posting logic transaction codes to ensure that transactions are recorded in accordance with Generally Accepted Accounting Principles; and
  - Tracking detail transactions associated with intragovernmental business and eliminating the need for default codes such as Trading Partner Identification Number that cannot be easily researched.

Recommendations: We recommend that the Coast Guard's Chief Information Officer and Chief Financial Officer update the scripting policies and procedures to include additional and more detailed test documentation, develop training that addresses all aspects of script testing (including documentation of test documents) and provide training to appropriate CM staff, develop a RP with associated supporting business case(s) to address the database audit logging requirements, develop procedures and perform regular account revalidations for Serena to ensure privileges remain appropriate, and conduct an assessment over the ICOFR process related to identifying and evaluating scripts that have a financial statement impact.

APPLICATION CONTROLS

Application controls were not tested for the year ending September 30, 2010, due to the nature of the prior-year audit findings.

MANAGEMENT'S COMMENTS AND OIG RESPONSE

We obtained written comments on a draft of this report from Coast Guard's Chief Information Officer and Chief Financial Officer. Generally, Coast Guard agreed with all of our findings and recommendations. Coast Guard has developed a remediation plan to address these findings and recommendations. We have included a copy of the comments in Appendix D.

OIG Response
We agree with the steps that USCG's management is taking to satisfy these recommendations.

Appendix A

Description of Key Coast Guard Financial Systems and IT Infrastructure within the Scope of the FY 2010 DHS Financial Statement Audit

Below is a description of significant Coast Guard financial management systems and supporting IT infrastructure included in the scope of the DHS Financial Statement Audit – Coast Guard Component.

Locations of Audit: Coast Guard HQ in Washington, DC; the Coast Guard FINCEN in Chesapeake, Virginia (VA); the Operations Supply Center (OSC) in Martinsburg, West Virginia; Aviation Logistics Center (ALC) in Elizabeth City, North Carolina; and the Pay and Personnel Center (PPC) in Topeka, Kansas.

Key Systems Subject to Audit:

Core Accounting System (CAS)
CAS is the core accounting system that records financial transactions and generates financial statements for the Coast Guard. CAS is hosted at the Coast Guard's FINCEN, in Chesapeake, VA. The FINCEN is the Coast Guard's primary data center. CAS is a customized version of Oracle Financials. CAS interfaces with two other systems located at the FINCEN, WINS and the Financial and Procurement Desktop (FPD).

FPD
The FPD application is used to create and post obligations to the core accounting system. It allows users to enter funding, create purchase requests, issue procurement documents, perform system administration responsibilities, and reconcile weekly program element status reports. FPD is interconnected with the CAS system and is located at the FINCEN in Chesapeake, VA.

WINS
WINS is the document image processing system, which is integrated with an Oracle Developer/2000 relational database. WINS allows electronic data and scanned paper documents to be imaged and processed for data verification, reconciliation and payment. WINS utilizes MarkView software to scan documents and to view the images of scanned documents and to render images of electronic data received. WINS is interconnected with the CAS and FPD systems and is located at the FINCEN in Chesapeake, VA.

Joint Uniform Military Pay System (JUMPS)
JUMPS is a mainframe application used for paying USCG active and reserve payroll. JUMPS is located at the PPC in Topeka, Kansas.

Direct Access
Direct Access is the system of record and all functionality, data entry, and processing of payroll events is conducted exclusively in Direct Access. Direct Access is maintained by IBM Application On Demand (IBM AOD) in the iStructure data center facility at Tempe, AZ with a hotsite located in a Qwest data center in Sterling, VA. Coast Guard personnel that provide system support to Direct Access are located at Coast Guard HQ and PPC.

Global Pay (Direct Access II)
Global Pay provides retiree and annuitant support services. Global Pay is maintained by IBM Application On Demand in the iStructure data center facility at Tempe, AZ with a hotsite located in a Qwest data center in Sterling, VA. Coast Guard personnel that provide system support to Global Pay are located at Coast Guard HQ and PPC.

Shore Asset Management (SAM)
SAM is hosted at the Coast Guard's Operation System Center (OSC), in Martinsburg, WV. SAM provides core information about the Coast Guard shore facility assets and facility engineering. The application tracks activities and assist in the management of the Civil Engineering Program and the Facility Engineering Program.

Naval and Electronics Supply Support System (NESSS)
NESSS is one of four automated information systems that comprise the family of Coast Guard logistics systems. NESSS is a fully integrated system linking the functions of provisioning and cataloging, unit configuration, supply and inventory control, procurement, depot-level maintenance and property accountability, and a full financial ledger.

Aviation Logistics Management Information System (ALMIS)
ALMIS provides Coast Guard Aviation logistics management support in the areas of operations, configuration management, maintenance, supply, procurement, financial, and business intelligence. Additionally, ALMIS covers the following types of information: Financial, Budget, Planning, Aircraft & Crew Status, Training & Readiness, and Logistics & Supply. The Aviation Maintenance Management Information System (AMMIS), a subcomponent of ALMIS, functions as the inventory management/fiscal accounting component of the ALMIS application. The Aircraft Repair & Supply Center (ARSC) Information Systems Division (ISD) in Elizabeth City, North Carolina hosts the ALMIS application.

CG Treasury Information Executive Repository (CG Tier)
CG TIER is a financial data warehouse containing summarized and consolidated financial data relating USCG operations. It is one of several supporting applications within CAS Suite designed to support the core financial services provided by FINCEN. CG TIER provides monthly submissions to DHS Consolidated TIER.

Appendix B

FY 2010 Notices of IT Findings and Recommendations at Coast Guard

Notice of Findings and Recommendations – Definition of Severity Ratings:

Each NFR listed in Appendix B is assigned a severity rating from 1 to 3 indicating the influence on the DHS Consolidated Independent Auditor's Report.

1 – Not substantial

2 – Less significant

3 – More significant

The severity ratings indicate the degree to which the deficiency influenced the determination of severity for consolidated reporting purposes.

These rating are provided only to assist the Coast Guard in the development of its corrective action plans for remediation of the deficiency.

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2010

Department of Homeland Security
FY 2010 Information Technology – Coast Guard
Notices of Findings and Recommendations – Detail

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2010

Notification of Findings and Recommendations – Detail

United States Coast Guard

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CG-IT-10-01	We determined that the Contractor, Civilian, and Military Account Termination Notification Process is still in the planning stages. Requirements still need to be prioritized and cost estimates need to be developed in order to obtain funding. Coast Guard still plans on using Direct Access but will only implement this new process once Direct Access has been upgraded, however, the implementation date has not yet been finalized.	We recommend that Coast Guard Headquarters continue with the following efforts: 1) Develop a resource plan with associated supporting business case(s) to address account tracking for terminated, transferred, or retired contractor, military, and civilian personnel; and, 2) Continue existing planning efforts and develop, document, and implement enterprise-wide processes that will notify all impacted system owners of terminated, transferred, or retired contractor, military, and civilian personnel.		X	2
CG-IT-10-02	We determined that Coast Guard Headquarters incorporated Program Manager guidance to the Commandant Instruction, as Enclosure 3, so that the Program Managers could determine the correct risk level and position sensitivity designation. An All Coast Guard (ALCOAST) message was also released in June that stated all contractors must have a favorable fingerprint check and initiated or completed minimum	We recommend that Coast Guard Headquarters continue with the following efforts: 1) Continue to update existing contracts to include the new contractor background check requirements, and		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	background investigation in order to obtain a Common Access Card (CAC), effective immediately. This has resulted in two activities: 1) new contracts will incorporate these new requirements immediately; and 2) existing contracts will incorporate these new requirements when new task orders are issued, options are exercised, contract modifications are made, etc. Therefore, based upon the renewal/option date of a contract in place prior to the ALCOAST, it could take up to two years before all of the contractors throughout Coast Guard will meet these new requirements. Furthermore, as part of our analysis, we were unable to determine if Coast Guard had the capability to consistently produce a current and comprehensive list of all Coast Guard contractors to include valid background investigation information tied to the correct risk level and position sensitivity designation.	perform associated contractor background checks; 2) Continue to include new contractor background check requirements in new contracts, and perform associated background checks; and 3) Develop a resource plan with associated supporting business case(s) to address the need for a reporting mechanism for contractor risk level, position sensitivity designation, and associated background check.			
CG-IT-10-03	We determined that the Coast Guard will delay issuing any new or updated guidance/instructions until the Joint Reform Team (JRT) report/guidance has been issued and will continue to not comply with the DHS standards in regards to civilian background investigation and reinvestigations. Coast Guard will continue to vet civilian individuals based on the Office of Personnel Management requirements and associated methodology both in terms of initial background investigations and re-investigations. In addition, Coast Guard has created an organization-	We recommend that Coast Guard Headquarters continue with the following efforts: 1) Develop a resource plan with associated supporting business case(s) to address fixing the organization-wide background investigations report; and 2) Continue existing efforts to update, document, and implement the overall		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	wide automated report that shows the background investigation status of each civilian Coast Guard employee. However, Coast Guard is currently unable to consistently generate error-free reports. Coast Guard stated that the report could be corrected within 2 years if additional resources are provided.	Coast Guard personnel security process for civilian personnel, based upon the JRT report/guidance.			
CG-IT-10-04	From the period of October 1, 2009 through the November 29, 2009, adequate guidance was not in place for Coast Guard to properly assess the financial statement impact of changes to the production environment of CAS, FPD and WINS. During this time period, two CAS changes were implemented into production without a proper assessment of the financial statement impact of the proposed changes. Upon the effective date of the *Financial Impact Determination for Data Scripts and System Change Requests* Memorandum on November 30, 2009, Coast Guard began and continued to follow adequate guidance to properly assess the financial statement impact of changes to CAS, FPD and WINS.	No recommendation required. Coast Guard took appropriate corrective action during the current fiscal year to remediate the exception that was identified during this fiscal year.	X		1
CG-IT-10-05	We determined that some previously noted weaknesses were remediated (particularly in the second half of FY 2010), while other control deficiencies continued to exist. The remaining control deficiencies that were present throughout FY 2010 vary in significance, however three key areas that impact the Coast Guard	We recommend that Coast Guard: 1) Update the scripting policies and procedures to include additional and more detailed test documentation;		X	3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	Script control environment are: 1) Script Testing Requirements; 2) Script Testing Environment; and 3) Script Audit Logging Process. a. Script Testing Requirements: Limited testing requirements exist to guide FINCEN staff in the development of test plans and guidance over the functional testing that should be performed. Additionally, we determined that there are no detailed requirements over the review and testing of functional changes to the data. FINCEN only tracks and documents the number of transactions updated on scripts that have a financial impact and not the detailed dollar amounts associated with the financial impact transactions. b. Script Testing Environment: Not all script changes were tested in the appropriate CAS Suite test environments, as required. FINCEN management informed us that the testing environments, CAS4 and LUFSFQT3, were offline for these exceptions due to a refresh of the databases and that testers used CAS3 and Alpha as alternate testing environments instead. However, FINCEN management informed KPMG that these environments are refreshed on an as needed basis and no further information could be provided over how frequently the CAS3 and Alpha databases were refreshed to verify that the scripts were adequately tested in the appropriate environment. Furthermore, we determined that guidance is not provided over the	2) Develop training that addresses all aspects of script testing (including documentation of test documents) and provide training to appropriate CM staff; 3) Develop a resource plan with associated supporting business case(s) to address the database audit logging requirements; 4) Develop procedures and perform regular account revalidation for Serena to ensure privileges remain appropriate; and 5) Conduct an assessment over the ICOFR process related to identifying and evaluating scripts that have a financial statement impact.			

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	use of alternate testing environments for the testing of scripts to ensure they are adequately tested. c. Script Audit Logging Process: The CAS, FPD, and Sunflower databases are logging changes to tables as well as successful and unsuccessful logins. However, no reconciliation between the scripts run and the changes made to the database tables is being performed to monitor the script activities and ensure that all scripts run have been approved through Change Management Script System or Serena. In addition, we noted that FINCEN has not established a formal process to monitor and review changes made to the Sunflower database including the tables and activities modified by the database administrators. During our test work, we noted weaknesses in the script change management process as it relates to the ICOFR process (e.g., the financial statement impact of the changes to the CAS Suite through the script change management process). While a process exists to identify, and route a script with potential financial statement impact through an assessment process, the review and determination over each script is primarily performed without structured/detailed procedures in place. Furthermore, the rationale documenting the impact of the script, whether deemed as having financial impact or not, is not documented and retained. In addition, within the CAS Suite environment, there are				

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	over 200 scripts run on a weekly basis and we noted that the financial statement impact assessment is essentially performed by a single branch, which has authorized only three people to assess the scripts.				
CG-IT-10-06	To complement our IT audit testing efforts as part of the FY 2010 DHS Financial Statement Audit and Audit of ICOFR, we also performed social engineering testing. During our social engineering testing, we were provided with seven users' passwords.	We recommend that Coast Guard Headquarters update the annual IA training to include more robust "phishing" and "social engineering" guidance and instruction and explicitly test individuals during the training on these topic areas.		X	2
CG-IT-10-07	A selection of newly created users of the JUMPS application was made to inspect whether applicable documentation was recorded and retained to identify authorized users. We determined that documentation was not retained for one of the five users selected. We performed inquiry procedures with management to determine that access was appropriately restricted for this user; however, no JUMPS Access Authorization Form could be located. On July 20, 2010, management remediated the exception by completing a new JUMPS Access Authorization Form for the noted user with a copy of the form being entered into the Coast Guard's imagining repository.	No recommendation required. Coast Guard took appropriate corrective action during the current fiscal year to remediate the exception that was identified during this fiscal year.	X		1
CG-IT-10-08	We determined that the Coast Guard TIER System password setting for lockout duration (PASSWORD_LOCK_TIME) is only configured to 0.0005 days (less than one minute). This setting was subsequently changed on 7/19/2010 to a setting of	No recommendation required. Coast Guard took appropriate corrective action during the current fiscal year to remediate the exception that was identified during this fiscal year.	X		1

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	"UNLIMITED" which requires an administrator to unlock the account. We observed and noted that this change was made by Coast Guard.				
CG-IT-10-09	To complement our IT audit testing efforts as part of the FY 2010 DHS Financial Statement Audit and Audit of ICOFR, we also performed after-hours physical security testing. We performed after-hours physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects include physical access to media and equipment that houses financial data and information residing on a Coast Guard employee's/contractor's desk, which could be used by others to gain unauthorized access to systems housing financial information. During our after-hours physical security testing, we identified the following: • 9 instances of passwords found near desktop computer; • 13 instances of FOUO information unsecured; • 4 instances of PII unsecured; • 16 instances of unsecured external hard drives; • 4 instances of unsecured secure token IDs; • 3 instances of unsecured laptop computers; • 1 instance of a computer terminal root command left unattended;	We recommend that Coast Guard: 1) Update the annual IA training to include more robust office "physical security" and "clean desk" guidance and instruction and explicitly test individuals during the training on these topic areas; and 2) Implement enterprise-wide and site-specific processes for verifying the effectiveness of this training via mechanisms such as scheduled and ad hoc desk checks, training follow-ups, and other management controls.		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	• 1 instance of a network directory structure map left unattended; • 1 instance of an active on-session computer left unsecured; • 3 instances of IP addresses left unsecured; and • 1 USCG Badge left unsecured.				
CG-IT-10-10	During our FY 2010 follow-up test work, we determined that the *Role-Based Industry Standards for USCG IA Professionals* Commandant Instruction had been renamed *Information Assurance Professional Certifications* and was formally issued on March 23, 2010. The Instruction stated that all military employees assigned to an IA role must obtain a required certification within 12 months of the Commandant Instruction issue date (*i.e.*, March 23, 2011), and all civilian employees currently in an IA role would be granted a waiver within 12 months of the Commandant Instruction issue date. Although Coast Guard has taken corrective actions to remediate this prior year NFR, we determined that since the corrective actions are planned for completion by March 2011, they were not completed in FY 2010 (i.e., all IA professionals who are required to obtain/maintain a professional certification within a year of the date of the Instruction did not obtain a certification by the end of FY 2010). Our testing noted that eight (8) or 3.9% of Coast Guard IA professionals out of the total population of 205 have the required certification for their	We recommend that Coast Guard: 1) Continue to implement Commandant Instruction *Information Assurance Professional Certification;* and. 2) Improve and utilize its manual tracking process until such time that the Direct Access implementation is in place.		X	1

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	prescribed level on file. Furthermore, we noted that 59 or 28.7% of Coast Guard IA professionals have not provided evidence of industry-based training. In addition, through our testing, we could not determine the number of IA professionals that had been granted waivers for the certification requirement. We also noted that 14 Coast Guard System Administrators were not listed as being part of the 205 Coast Guard IA professionals.				
CG-IT-10-11	During the FY 2010 IT Audit, a selection of users added to the CG TIER application for the fiscal year was made to inspect whether proper documentation was recorded and retained for identify authorized users. We determined that documentation was not retained for one of the two CG TIER users selected. Upon further inquiry with management, we were informed that the identified CG TIER user was authorized access by the Financial Branch Chief; however, the email approval had been lost.	We recommend that Coast Guard take the follow actions: 1) For the user identified during testing, complete and retain all appropriate access request documentation; and 2) Update the CG TIER account management procedures to effectively track and retain user access documentation.	X		1
CG-IT-10-12	During our FY 2010 test work, we were informed by the Coast Guard that an annual review of 100% of the Direct Access user accounts with greater than read-only access (and their associated privileges) has not been performed for this fiscal year. Coast Guard also informed us that all Direct Access accounts created and/or modified during the fiscal year have been reviewed as part of the normal transfer and	We recommend that Coast Guard: 1) Develop a resource plan with associated supporting business case(s) to address the 100% account review requirement; 2) Continue to coordinate with the DHS Chief Information Security Officer's (CISO) office to determine and		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	aging processes; however, our testing did not extend to validate this statement. Based upon a risk based decision, the Coast Guard has designed a process to review a subset of users that represent the greatest risk to Direct Access. This annual review would cover approximately 743 Direct Access users. The scope of the review includes users with payment approval, security administrator permissions, all contractors, and users with update/delete permissions. However, since this subset review does not cover 100% of the Direct Access user accounts with greater than read-only access (and their associated privileges) as required by DHS, we consider this NFR to be re-issued.	formalize the frequency and depth/breadth of effective reviews that address the perceived risk. Based upon the results of these discussions with the DHS CISO's office, the Coast Guard will modify procedures and develop, if applicable, required waivers/exceptions to reflect an adequate percentage of Direct Access user accounts to be reviewed; and 3) Continue to use its existing risk-based account review efforts until such time that the procedures are updated in response to the activities associated with the second recommendation.			
CG-IT-10-13	As part of this year's testing, we identified one security configuration management weakness (i.e., outdated operating system software) on hosts supporting CAS, FPD, and NESSS, as well as those systems' network infrastructure and associated workstations.	We recommend that Coast Guard: 1) Develop a resource plan with associated supporting business case(s) to address the installation of Service Pack 3 on all applicable Windows XP workstations and/or upgrade the operating systems of these workstations to the Coast Guard's Vista-based Standard Image 6.0; 2) Develop a resource plan with associated supporting business case(s)	X		1

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
		to address the server operating system upgrades to include a technical analysis to ensure Windows 2003 server upgrades do not adversely affect system operation; and 3) Based upon the results of Recommendation 1 and Recommendation 2, schedule and perform the upgrades and/or patches of the impacted servers and workstations.			
CG-IT-10-14	During our FY 2010 audit test work, we sampled 25 new user accesses for NESSS that were granted during the fiscal year to determine if an access authorization form had been completed, if the access had been timely approved by the user's supervisor, and that the forms were retained. Based upon our testing, we were unable to obtain 9 of the 25 user access forms. In addition, evidence of supervisory approval for 9 of the 25 sampled users was not available.	We recommend the Coast Guard's Operation Systems Center (OSC) update the NESSS account management Standard Operating Procedure (SOP) to provide clear guidance regarding the use of user access forms and update the access form to include an approval signature line.	X		2
CG-IT-10-15	During the FY 2010 audit test work, Aviation Logistics Center (ALC) visitor logs for the fiscal year were obtained to determine whether proper documentation was recorded and retained for the verification of individuals visiting the ALC Data Center and Facility. Our testing determined that the ALC Customer Support Desk did not properly complete the visitor logs during the FY 2010 audit period. Specifically, from a total of 190 visitor log entries for the fiscal year, 33 visitor log	We recommend that Coast Guard: 1) Develop and maintain a SOP to ensure that the ALC Data Center Access Control list is kept current and that its quarterly review is documented and maintained; and	X		1

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	entries did not have the Date-Out and Time-Out fields completed and 31 visitor log entries did not have the Sponsor field completed. Additionally, the ALC Data Center Access Listing was obtained to determine whether a review of the access listing was conducted and evidence of the review was performed and maintained. Our testing determined that the evidence of reviews of the Data Center Access for the FY 2010 period was not maintained. Therefore, we could not determine that the Data Center Access Listing had been properly reviewed during the year.	2) Re-emphasize to all ALC Support Desk personnel (through training), the importance of properly maintaining the visitor log and to ensure it is filled out completely and accurately.			
CG-IT-10-16	During the FY 2010 IT Audit, the AMMIS password configuration settings were obtained and tested to determine whether they complied with DHS policy. Our testing determined that the AMMIS subsystem password configuration settings do not comply with all of the required DHS password guidelines. Specifically, AMMIS password configuration settings did not comply with the following DHS password policy: • Contain a combination of alphabetic, numeric, and special characters – the AMMIS password requires a combination of alphabetic, numeric, or special characters; and • Not be the same as the previous eight passwords. The AMMIS password configuration is set to be the same as the previous six passwords.	We recommend that the Coast Guard configure the AMMIS application to enforce the strong password and password history requirements described in the DHS Management Directive 4300A Policy Directive and to update all impacted Certification & Accreditation and system documentation accordingly.	X		1

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	Additionally, our testing determined that the current ALMIS System Security Plan (SSP), which includes the system level requirements of the AMMIS subsystem, states that the implemented password configuration does not comply with the current DHS password policy. Specifically, the ALMIS SSP states that the password cannot be the same as the previous 6 passwords; however, DHS guidance states that passwords cannot be the same as the previous 8 passwords.				
CG-IT-10-17	To complement our IT audit testing efforts as part of the FY 2010 DHS Financial Statement Audit and Audit of ICOFR, we also performed social engineering testing. During our social engineering testing, we were provided with 7 users' passwords. This was the second round of social engineering testing conducted as part the FY 2010 DHS Financial Audit and Audit of Internal Control over Financial Reporting. Our initial testing occurred back on June 30th and July 1st, 2010. Our initial testing resulted in Coast Guard IT-NFR-10-06 being issued. The testing approach and scope for the second round of testing was the same as the initial round. During our 2nd round social engineering testing, we were provided with two users' passwords.	We recommend that Coast Guard implement the recommendations presented in Coast Guard IT-NFR-10-06. No additional actions are required.		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
CG-IT-10-18	Our testing determined that the evidence of reviews over the AMMIS audit logs for the FY 2010 audit period was not maintained by ALC. Therefore, we could not determine if the AMMIS audit logs had been properly reviewed during the year. Additionally, our testing determined that reviews of all deactivated AMMIS accounts may not have been performed and evidence of the reviews was not maintained by the ALC. Therefore, we could not determine whether deactivated AMMIS accounts had been properly monitored and reviewed during the year. Lastly, we were informed by the ALC that the AMMIS audit logs were not being reviewed by an individual that is considered independent to the process. We noted that an AMMIS system administrator is responsible for reviewing the AMMIS audit logs.	We recommend that Coast Guard: 1) Update the AMMIS Standard Operating Procedures to address the audit log review and retention procedures; and 2) Implement separation of duties for the AMMIS audit log reviews.	X		2
CG-IT-10-19	Our testing determined that evidence of a review and recertification of the 11,306 users with "Update" privilege in ALMIS was not maintained by the ALC. Therefore, we could not determine that ALMIS user accounts had been properly reviewed and recertified during the year.	We recommend that Coast Guard: 1) Develop a resource plan with associated supporting business case(s) to address the 100% account review requirement; 2) Continue to coordinate with the DHS CISO's office to determine and formalize the frequency and depth/breadth of effective reviews that address the perceived risk.	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
		Based upon the results of these discussions with the DHS CISO's office, the Coast Guard will modify procedures and develop, if applicable, required waivers/exceptions to reflect an adequate percentage of ALMIS user accounts to be reviewed; and 3) Continue to use its existing risk-based account review efforts until such time that the procedures are updated in response to the activities associated with the second recommendation.			
CG-IT-10-20	Our testing determined that the AMMIS Software Change Request Forms were not appropriately authorized. Specifically, for the four AMMIS software changes made during the fiscal year, two of the software change request forms were not signed by the Division Chief.	We recommend that Coast Guard establish and follow a management review process to ensure that any new AMMIS Software Change Requests processed will be reviewed by the PC team for the proper/required signatures.	X		1
CG-IT-10-21	During our FY10 audit test work over the Naval and NESSS recertification process, we noted that 32 users were assigned the role FLS_USR_ADM_GRP within the NESSS application. This role grants the ability to add, modify, and delete user accounts. In addition, two of these users were system administrators. This number of users with this elevated role was considered excessive based upon the ratio of this role to the NESSS user	Coast Guard took appropriate corrective action to remediate the exception that was identified and no additional corrective actions are required.	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	population. On October 7, 2010, OSC management remediated the condition by reducing the number of users with the FLS_USR_ADM_GRP role down to six.				
CG-IT-10-22	We determined that OSC had updated the policies and procedures for System Administrators and Database Administrators to include more detail and instructions on entering sufficient evidence regarding the weekly non-independent audit log reviews documented and tracked in the ClearQuest Ticketing system. We also noted that the monthly SAM audit log reviews were being conducted by an independent team. Although OSC has taken steps to remediate the prior year conditions by updating the policies and completing the monthly independent reviews, we determined that the 3 sampled months of SA and DBA audit log reviews did not have sufficient detail on the ClearQuest tickets. Specifically, we identified the following: • 1 of the 3 SA monthly reviews did not have a searchable title; • 2 of the 3 SA monthly reviews did not include results of the audit log review (i.e., audit logs had no exceptions.); • 3 of the 3 DBA monthly reviews did not list the logs that were included in the review; and	We recommend that Coast Guard: 1) Update the SAM and NESSS audit log review procedures within the Standard Operating Procedures to include more detail in the ClearQuest Tickets including recording the results of the review of the audit logs; 2) Implement similar separation of duties for the NESSS audit log reviews as have been implemented for the SAM audit log reviews; and 3) Continue with ongoing efforts for identifying, designing, and implementing automated tools to assist in audit log collection, storage, analysis, and reporting which will further improve consistency, timeliness, and accuracy of the reviews when compared with labor and time intensive manual processes.		X	2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	• 3 of the 3 DBA monthly reviews did not have results of the audit log reviews. As a result of limitations of the underlying operating system of the Shore Asset Management System AM system: • The servers do not automatically alert in the event of an incident; and • The server operating systems do not inherently provide audit reduction and report generation capability. Furthermore, the OSC has not implemented a centralized log solution for audit log reduction and reporting, and automated alert notifications. <u>NESSS Audit Logs:</u> During our FY 2010 test work for the NESSS, we noted that daily and weekly audit log reviews are performed by the NESSS System Administrator. The weekly audit log reviews are documented in the ClearQuest system with a running ticket for the calendar year. Each week's review is added to the ClearQuest ticket. However, we determined that there is not sufficient detail in the ClearQuest ticket in recording the results of the review of the audit logs. Furthermore, as similar to SAM audit log review process listed above, OSC has not implemented a centralized log solution for audit log reduction and reporting, and automated alert notifications. In addition, the weekly reviews are performed by the				

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	NESSS System Administrator, who is not considered an independent party as required by DHS MD 4300A.				
CG-IT-10-23	During the FY 2010 audit test work, the OSC data center access listing was obtained in order to determine whether a review of the access listing was conducted and evidence of the review was maintained. OSC informed us that they perform a review of the data center access on a quarterly basis. However, our testing determined that the evidence of reviews concerning OSC data center access for FY 2010 was not maintained. Therefore, we could not determine whether the OSC data center access listing had been properly reviewed during the year.	We recommend that Coast Guard develop detailed procedures for: 1) Quarterly data center access reviews to include validating that users have a physical need to access the data floor; and 2) Methods for maintaining the review documentation.	X		1
CG-IT-10-24	During prior financial statement audits dating back to FY 2003, we noted that the implementation and oversight of the Coast Guard's information security controls needed various improvements. In FY 2010, continued improvements have been made in the areas of access controls, entity-level controls, and configuration management. Improvements in the IT control environment were identified at each of the Coast Guard financial processing locations where IT audit was previously conducted. However, significant improvements are still warranted in the area of script configuration management controls for the key financial systems located at the FINCEN. Script configuration management control is the subject of the significant control deficiencies identified and	We recommend that Coast Guard: 1) Continue to implement and improve upon the monitoring of compliance with DHS, Coast Guard, and Federal security policies and procedures in the areas of script configuration management controls to include the use of the automated tools deployed at the FINCEN; and 2) Develop and implement corrective action plans to address and remediate the NFRs issued during the FY 2010 audit.		X	3

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	recommendations that were developed during the audit. Other weaknesses continued to exist, to a lesser extent, in the areas of access controls and entity-wide security at each of the Coast Guard financial processing locations. These continued weaknesses require Coast Guard to continue with the implementation of their corrective actions plans and monitoring efforts. 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 FFMIA.				
CG-IT-10-25	During our FY 2010 year-end IT roll-forward audit testing procedures, we determined that one (1) of the five (5) FPD, Production Implementation Request (PIR) forms tested was not signed off on by the analyst/submitter/implementer as required per the FINCEN PIR form.	The process for obtaining written sign-off on PIR forms has recently been replaced with an automated workflow process that eliminates the need for written approvals; therefore no additional corrective actions are required.	X		1
CG-IT-10-26	During the FY 2010 audit test work, we determined that ALC policies and procedures for the following control areas are not adequately detailed to provide clear and complete control descriptions for each of the following processes: • Physical Access to the data center and systems in the data center; • Access to Program Libraries; • Segregation of Duties in support of the AMMIS	We recommend that Coast Guard develop, document, communicate, train, test, and continuously maintain policies and procedures for the cited control and process areas.	X		2

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	application; • AMMIS Audit Log Review and Retention; • Backups and Data Restoration; and • Offsite Storage of Backup media.				
CG-IT-10-27	The NESSS' Oracle *verify_function* in the SYS schema is incorrectly configured and does not include verification of special characters for passwords.	We recommend that Coast Guard review and update the Oracle *verify_function* in the SYS schema to include the verification of special characters for passwords.	X		1
CG-IT-10-28	During our FY 2010 audit test work, we followed up with Coast Guard management and were notified that this Direct Access audit logging weakness, noted in FY 2009, cannot be resolved until Direct Access is updated to PeopleSoft version 9. There is no current timeline for the upgrade to take place. The following conditions were noted last year and are still open in FY 2010. Not all Direct Access failed logon attempts are logged or reviewed; and account management audit logs for the Direct Access application are not reviewed on a monthly basis, which is a requirement set forth within DHS Policy.	We recommend that Coast Guard continue with the PeopleSoft 9.0 upgrade and PeopleSoft Portal implementation.		X	1

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2010

Appendix C

Status of Prior Year Notices of Findings and Recommendations and Comparison to Current Year Notices of Findings and Recommendations at Coast Guard

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2010

		Disposition	
NFR #	**Description**	**Closed**	**Repeat**
CG-IT-09-10	Contractor Background Investigation Weakness		10-02
CG-IT-09-14	Weaknesses with Specialized Role-based Training for Individuals with Significant Security Responsibilities		10-10
CG-IT-09-23	SAM Audit Log Review Weakness		10-22
CG-IT-09-25	WINS Access Controls Need Strengthening	X	
CG-IT-09-31	Weaknesses Exist in the Configuration Management Controls Over the Scripting Process		10-05
CG-IT-09-32	Lack of Documented Contractor Tracking System Reconciliation Procedures	X	
CG-IT-09-33	Lack of a Consistent Contractor, Civilian, and Military Account Termination Process for Coast Guard Systems		10-01
CG-IT-09-34	WINS Change Control Weakness	X	
CG-IT-09-40	Civilian Background Investigation Weakness		10-03
CG-IT-09-42	Non-Compliance with FFMIA – Information Technology		10-24
CG-IT-09-43	Recertification Weakness within the User Management System (UMS)	X	
CG-IT-09-45	FINCEN data center access is not restricted to appropriately authorized personnel	X	
CG-IT-09-46	Configuration and Patch Management - Vulnerability Assessment	X	
CG-IT-09-49	JUMPS Audit Log Review Weakness	X	
CG-IT-09-50	Audit Trail Weaknesses within the Direct Access Application		10-28
CG-IT-09-51	Audit Trail Weaknesses within the Global Pay Application	X	
CG-IT-09-52	Recertification Weakness within the Direct Access Application		10-12
CG-IT-09-53	Security Awareness Issues Associated with the Protection of Sensitive Information		10-06

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

Commandant
United States Coast Guard

2100 Second Street, S.W. Stop 7101
Washington, DC 20593-7101
Staff Symbol: CG-6
Phone: (202) 475-3500
Fax: (202) 475-3930
Email: Robert.E.Day@uscg.mil

5500

FEB 24 2011

Reply to: CG-632
Attn of: Bruce Krebs
(202) 475-3585

MEMORANDUM

From: R.E. Day, RDML
COMDT (CG-6)

K.A. Taylor, RDML
COMDT (CG-8)

To: Mr. Frank Deffer
Assistant Inspector General
Information Technology Audits

Subj: RESPONSE TO INFORMATION TECHNOLOGY MANAGEMENT LETTER FOR THE U.S. COAST GUARD COMPONENT OF THE FISCAL YEAR 2010 DHS INTEGRATED AUDIT

Ref: (a) DHS OIG Memo dtd 14 Feb 2011

1. In response to reference (a), thank you for the DHS Office of the Inspector General's (OIG) thorough, independent review of the general Information Technology (IT) controls associated with the USCG financial processing environment, IT infrastructure, and overall security program. This process, combined with other proactive activities, helps the USCG improve its Information Security (INFOSEC) posture.

2. The OIG identified several conditions and findings that require corrective actions by the USCG. The USCG concurs with the basis for the conditions and findings that were documented in the FY10 IT Notice of Findings and Recommendations (NFRs) and summarized within the IT Management Letter. Specific details of those findings, and their potential impacts, will be discussed early in the FY11 audit during the prior year's review process.

3. During the course of the audit, the USCG conducted a series of root cause analyses and determined the most appropriate method(s) for addressing identified weaknesses based upon system capabilities and resources. The USCG continues to implement and execute corrective actions to address the underlying conditions and findings to mitigate risk and improve security. These corrective actions (i.e., Plans of Action and Milestones (POA&Ms)) are developed, monitored, and reported via the DHS Trusted Agent FISMA (TAF) tool. FY10 IT NFR remediation is overseen by the USCG CIO's Office (CG-6), with the exception of IT NFR CG-IT-10-05 (scripts) which is led by the USCG CFO's Office (CG-8).

4. With respect to the Material Weakness associated with IT NFR 10-05, the USCG has established a team to address the root causes associated with Configuration Management Controls Over the Scripting Process. The NFR material weakness is based on the financial

SUBJ: RESPONSE TO INFORMATION TECHNOLOGY MANAGEMENT LETTER FOR THE U.S. COAST GUARD COMPONENT OF THE FISCAL YEAR 2010 DHS INTEGRATED AUDIT

5500

FEB 24 2011

impact of the scripts, related to Internal Controls Over Financial Reporting (ICOFR). In addition, there is still some remediation work underway with IT general controls with script testing requirements, environment, and the logging process.

5. The USCG understands the need to continuously improve IT security operations and has demonstrated this commitment by proactively seeking ways to improve controls governing the script process. The majority of the USCG system-oriented IT NFRs will be mitigated as they were identified during the audit or early within FY11. The USCG looks forward to working with the DHS OIG during the FY10 audit, where we anticipate confirmation of our corrective action approach through measurable, tangible results.

Copy: CG-63
CG-65
CG-84
CG-85

Report Distribution

Department of Homeland Security

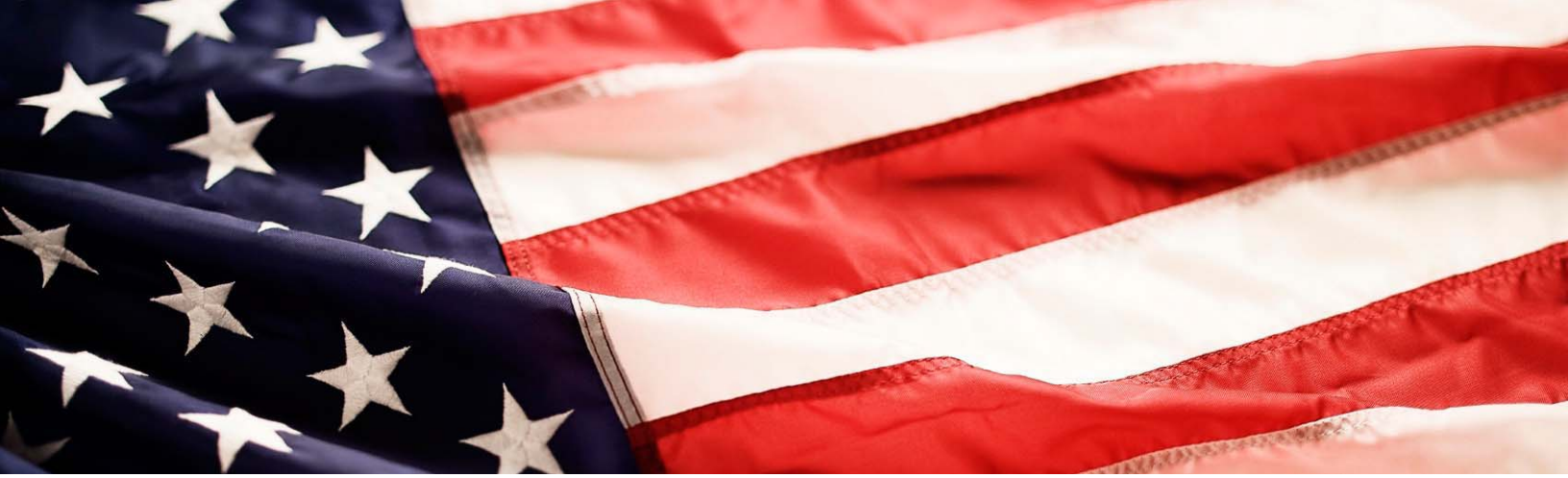
Secretary
Deputy Secretary
General Counsel
Chief of Staff
Deputy Chief of Staff
Executive Secretariat
Under Secretary, Management
Commandant, USCG
DHS Chief Information Officer
DHS Chief Financial Officer
Chief Financial Officer, USCG
Chief Information Officer, USCG
Chief Information Security Officer
Assistant Secretary for Office of Policy
Assistant Secretary for Office of 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) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

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

• Call our Hotline at 1-800-323-8603;

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

• Email us at DHSOIGHOTLINE@dhs.gov; or

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

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