Department of Homeland Security

Office of Inspector General

IT Matters Related to the United States Coast Guard Component of the FY 2011 DHS Financial Statement Audit

OIG-12-49

March 2012

Office of Inspector General

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

March 14, 2012

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 fiscal (FY) 2011 DHS consolidated financial statement audit as of September 30, 2011. It contains observations and recommendations related to information technology internal control weaknesses that were summarized in the *Independent Auditors' Report* dated November 11, 2011 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 2011 consolidated financial statement audit and prepared this IT management letter. KPMG is responsible for the attached IT management letter 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 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
Suite 12000
1801 K Street, NW
Washington, DC 20006

February 16, 2012

Acting Inspector General
U.S. Department of Homeland Security

Chief Information Officer and

Chief Financial Officer
U.S. Coast Guard

We have audited the balance sheet of the U.S. Department of Homeland Security (DHS or Department) as of September 30, 2011 and the related statement of custodial activity for the year then ended (referred to herein as the "fiscal year (FY) 2011 financial statements"). The objective of our audit was to express an opinion on the fair presentation of these financial statements. We were also engaged to examine the Department's internal control over financial reporting of the balance sheet as of September 30, 2011, and statement of custodial activity for the year then ended, based on the criteria established in Office of Management and Budget, Circular No. A-123, *Management's Responsibility for Internal Control*, Appendix A. In connection with our audit, we also considered DHS' compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements that could have a direct and material effect on the FY 2011 financial statements.

Our *Independent Auditors' Report* issued on November 11, 2011, describes a limitation on the scope of our audit that prevented us from performing all procedures necessary to express an unqualified opinion on DHS' FY 2011 financial statements and internal control over financial reporting. In addition, the FY 2011 DHS *Secretary's Assurance Statement* states that the Department was unable to provide assurance that internal control over financial reporting was operating effectively at September 30, 2011.

A deficiency in internal control 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 material weakness is a deficiency, or 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. 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. In accordance with *Government Auditing Standards*, our *Independent Auditors' Report*, dated November 11, 2011, included internal control deficiencies identified during our audit, that individually, or in aggregate, represented a material weakness or a significant deficiency. This letter represents the separate limited distribution report mentioned in that report.

During our audit engagement, we noted certain matters in the areas of access controls, configuration management, security management, contingency planning, and segregation of duties with respect to DHS' financial systems general Information Technology (IT) controls which we believe contribute to a DHS-level significant deficiency that is considered a material weakness in IT controls and financial system functionality. We also noted that in some cases, financial system functionality is inhibiting DHS' ability to implement and maintain internal controls, notably IT applications controls supporting financial data processing and reporting. These matters are described in the *General IT Control Findings and Recommendations* section of this letter.

Although not considered to be a material weakness, we also noted certain other items during our audit engagement which we would like to bring to your attention. These matters are also described in the *General IT Control Findings and Recommendations* 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 are 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. We have provided a description of key DHS financial systems within the scope of the FY 2011 DHS financial statement audit engagement 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 (comments not related to IT) have been presented in a separate letter to the Office of Inspector General and the DHS Chief Financial Officer.

This report is intended solely for the information and use of DHS management, DHS Office of Inspector General (OIG), U.S. Office of Management and Budget (OMB), U.S. Government Accountability Office (GAO), 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, 2011

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE, AND APPROACH

We were engaged to audit DHS' balance sheet as of September 30, 2011, and the related statement of custodial activity for the year then ended, we performed an evaluation of general information technology controls (GITC) at Coast Guard, to assist in planning and performing our audit.

The *Federal Information System Controls Audit Manual* (FISCAM), issued by the GAO, formed the basis of our GITC evaluation procedures. The scope of the GITC 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 GITC 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 GITC audit procedures, we also performed technical security testing for key network and system devices. The technical security testing was performed within select Coast Guard facilities, 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 tested for the year ending September 30, 2011, which were identified by the financial audit team as being key controls.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2011, 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 located at the Operations Systems Center (OSC), Aviation Logistics Center (ALC), and USCG Finance Center (FINCEN); strengthening controls over audit log reviews at ALC; and improving data center controls at OSC and ALC. However, during FY 2011, we continued to identify general IT 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 2011, our IT audit work identified 21 IT findings; of which 16 were repeat findings from the prior year and 5 were new findings. In addition, we determined that Coast Guard remediated 11 IT findings identified in previous years. Specifically, the Coast Guard took actions to improve aspects of its system password settings, 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.

Collectively, these findings represent deficiencies in three of the five FISCAM key control areas. The FISCAM areas impacted included Security Management, Access Control, 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 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.

GENERAL IT CONTROL FINDINGS AND RECOMMENDATIONS

Findings:

Conditions: During the FY 2011 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 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 2011 testing, we noted that some previously identified control deficiencies were remediated, while other deficiencies continued to exist. Four key areas continue to impact the Coast Guard IT script control environment, as follows:

- Script testing – limited guidance exists to guide Coast Guard staff in the development of test plans and to support the completion of functional testing;
- Script audit logging – controls supporting audit logs are not consistently implemented to log privileged user actions, and to ensure that only approved scripts are executed;
- Script approvals and recertification – the recertification reviews conducted by the Coast Guard were not comprehensive to include all user roles associated with the Mashups and Dimensions systems. Additionally, the documentation retained in support of the reviews was not adequately completed in accordance with policy throughout the year; and
- Script recording – test and production data is not consistently recorded, and there are limited controls to ensure data accuracy. Additionally, field reconciliation discrepancies are not always consistently documented and explained.

In addition, we noted weaknesses in the script change management process as it relates to the Internal Control over Financial Reporting 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. 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.

We further noted that software change request forms for one of the key financial systems were not always appropriately authorized.

Access Controls

- Audit log reviews for key financial systems are not being conducted on all key information.
- New user access forms do not contain required supervisor approvals, as well as some new users were granted access before their form was approved.
- User roles were changed without required prior approval.
- Access review procedures (recertifications) 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.
- Data Center visitor access logs are not consistently completed fully and appropriately.

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.
- Background investigations for all contractor employees have not been completed.
- Not all Information Assurance (IA) professionals have the required certification or evidence of Continuing Professional Education (CPE) as required by Coast Guard policy.
- Support documentation for incident tickets did not provide sufficient evidence to determine whether the incidents were properly tracked and resolved.
- 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 below 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.

Weaknesses Observed During After Hours Physical Security Testing					
	Coast Guard Locations Tested				
Exceptions Noted (1)	**Coast Guard Headquarters (HQ)**	**Coast Guard Finance Center (FINCEN)**	**Surface Forces Logistics Center (SFLC)**	**Aviation Logistics Center (ALC)**	**Total Exceptions by Type**
Passwords (2)	3	5	6	3	**17**
Common Access Card	0	0	0	1	**1**
Server Names/IP Addresses	0	2	0	0	**2**
Access to Data Center (3)	0	0	0	1	**1**
Government Credit Card Number	0	0	0	1	**1**
For Official Use Only (FOUO) material	7	1	17	0	**25**
Personal Identifiable Information (PII)	0	3	0	0	**3**
Keys that opened cabinets that exposed an exception	1	0	0	0	**1**
Unsecured External Hard Drives	1	0	1	0	**2**
Unsecure Secure Toke IDs	1	0	0	0	**1**
Unsecured Laptops	1	0	0	0	**1**
Total Exceptions by Location	**14**	**11**	**24**	**6**	**55**

Source: Coast Guard management, OIG, and KPMG direct observation and inspection of work areas.
Note: The following number of cubicles/desks were examined for each location:
HQ – 35
FINCEN – 60
SFLC – 25
ALC – 25
(1) The number of exceptions may differ from the actual number of exceptions found at a cubicle/desk. For example, one cubicle had 3 passwords, but this was only recorded as 1 exception.
(2) Attempts to login to the systems with the identified passwords were not performed. However, we assumed that the identified passwords were valid passwords.
(3) With a temporary visitor badge, we were able to access the ALC data center.

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**
USCG Headquarters (HQ)	40	12	1
Coast Guard FINCEN	70	29	1
Surface Forces Logistics Center (SFLC)	40	19	3
Aviation Logistics Center (ALC)	40	20	6

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.

Configuration Management

- Continue to update the procedures, tools, and associated training to better address script record documentation reviews and provide training to impacted staff ;
- Continue to improve and better document the script audit logging processes and associated technical implementations in compliance with Coast Guard software development lifecycle (SDLC) and configuration management (CM) policies and procedures;
- Continue to improve and better document script approvals; define and implement script management and execution tool user access/account recertification procedures; and update associated training and provide that training to impacted staff;
- Continue to improve and better document script testing requirements and associated technical implementations and test environments in compliance with Coast Guard SDLC and CM policies and procedures;
- Continue to improve the script change management process and other associated internal controls as these relate to the financial statement impact of the changes to the CAS Suite financial databases;
- Continue to implement policy regarding approval of scripts that impact financial statements; and
- ALC management should update its Configuration Management/Quality Assurance (CM/QA) procedures to include a final comprehensive review step and associate signature prior to actual Software Change Request implementation. This will better ensure that all of the required change activities have been reviewed and verified prior to implementation.

Access Controls

- Include specific applicable DHS policy directive 4300A requirements and mechanisms by which these can be verified in the service provider's contract when that contract is re-competed in FY 2012;
- Update the test procedures to more thoroughly address the management of identified test account and other accounts used for maintenance purposes;
- Complete its legal review of the Coast Guard's account authorization retention policy and implement standard operating procedures to support it;
- Update the SFLC NESSS (Naval and Electronics Supply Support System) Access/User Control Process Guide to a) not allow phone call approvals, and b) update the account profile review processes to further reduce the risks associated with the lack of logging associated with user profile changes;
- Continue with implementing its new and more robust audit tool and account review/recertification process;

- Update its NESSS account management procedures and associated e-mail notifications to require an explicit acknowledgement of review by the supervisor and change the account recertification completion date to coincide with the end of the fiscal year;
- Review current NESSS roles and make any adjustments to these roles so that the allowable actions do not exceed those necessary to accomplish assigned tasks in accordance with organizational missions and business functions;
- Centralize, integrate, and enforce the requesting, management, review, and reporting of the addition, modification, and deletion of NESSS users;
- Enhance existing OSC data center policies and procedures to include content of the visitor logs and their associated reviews; and
- Develop and provide additional visitor training to staff who have access to the data center floor and who may also escort visitors on the data center floor.

Security Management

- Continue to vett the FINCEN staff through the Minimum Background Investigation (MBI) clearance process and identify the positions that have financial impact and proceed with MBIs for those positions;
- Continue to identify and record the contractor positions that have a financial impact and proceed with MBIs for those positions;
- Continue to improve its IA Professional certification tracking and data gathering procedures to better ensure accurate representation of IA Professional competencies and continue to incorporate IA Certification clauses into applicable contracts;
- Continue existing efforts to plan, develop, document, and implement enterprise-wide processes that will notify all impacted system owners of terminated, transferred, or retired contractor, military , and civilian personnel;
- Review and update its Incident Response procedures to better address incident ticket management including ticket closure and required supporting document.
- Define and implement an Incident Response Ticket review, tracking, and audit process that is automated to the greatest extent possible using tools such as Trusted Agent FISMA (TAF) and/or other project management systems to support long term and enterprise-wide efforts.
- Update Coast Guard Instruction/Policy to require quarterly physical security sweeps and to require Information System Security Officers (ISSOs) to conduct quarterly social engineering and physical security inspections of their areas and canvas personnel to confirm that their unit is employing good security practices;
- Update the Security Awareness and Training content to reflect the lasts requirements from the Committee on National Security Systems, Department of Defense, and DHS policy pertaining to the physical protection of sensitive information;
- Instruct ISSOs and other USCG security officers to more rigorously enforce COMDTINST 5500.13 as defined in the “Administrative Action” section which identifies proper procedures for responding to first, second, third, and fourth violations of policy;
- Review and update the Coast Guard’s Security Awareness and Training content to enhance the social engineering and phishing discussions; and

- Direct units to perform supervised social engineering tests to further reinforce annual training and best practices.

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 continue to lack the capability to perform this task efficiently.
- The Coast Guard is unable to routinely query its various general ledgers to obtain a complete population of financial transactions, and consequently must create many manual custom queries that delay financial processing and reporting processes.
- A key Coast Guard financial system is limited in processing overhead cost data and depreciation expenses in support of the property, plant and equipment financial statement line item.
- Production versions of 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, 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 detailed 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 weaknesses related to functional testing, audit logging, approvals and recertifications, and the documentation and review of script records) and provide training to appropriate CM staff, improve the script change

management process and other associate internal controls as they relate to the financial impact of the changes, and make necessary improvements to financial management systems and supporting IT security.

APPLICATION CONTROLS

Select application controls were tested for the year ending September 30, 2011, and no issues were identified associated with those applications selected for testwork.

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2011

Appendix A

Description of Key Coast Guard Financial Systems within the Scope of the FY 2011 DHS Financial Statement Audit

Below is a high-level description of significant Coast Guard financial management systems included in the scope of the DHS Financial Statement Audit – Coast Guard Component.

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 Virginia (VA). The FINCEN is the Coast Guard's primary data center. CAS interfaces with two other systems located at the FINCEN, the Workflow Imaging Network System and the Financial and Procurement Desktop.

Financial Procurement Desktop (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 VA.

Workflow Imaging Network System (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 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 Pay and Personnel Center (PPC) in 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 in Arizona (AZ) with a hot site located in a Qwest data center in VA.

Global Pay (Direct Access II)
Global Pay provides retiree and annuitant support services. Global Pay is maintained by IBM AOD in the iStructure data center facility in AZ with a hot site located in a Qwest data center in VA.

Shore Asset Management (SAM)
SAM is hosted at the Coast Guard's Operation System Center (OSC) in West Virginia. SAM provides core information about the USCG 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. SAM data contributes to the shore facility assets full life cycle Program management, facility engineering full life cycle Program management and rationale to adjust the USCG mission needs through planning, budgeting, and project funding. SAM also provides real property inventory and management of all shore facilities, in addition to the ability to manage and track the facilities engineering equipment and maintenance of that equipment.

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 North Carolina (NC) hosts the ALMIS application. The AMMIS, a subcomponent of ALMIS, functions as the inventory management/fiscal accounting component of 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.

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2011

Appendix B

FY 2011 Notices of IT Findings and Recommendations at Coast Guard

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2011

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 Auditors 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 DHS in prioritizing the development of its corrective action plans for remediation of the deficiency.

Appendix B

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2011

FY 2011 NFR #	NFR Title	FISCAM Control Area	2011 Severity Rating	New Issue	Repeat Issue
CG-IT-11-01	Security Awareness Issues Associated with Physical Protection of Sensitive Information	Access Controls	2		X
CG-IT-11-02	Direct Access and Direct Access II User and System Administrator Account Management and Approval	Access Controls	1	X	
CG-IT-11-03	Coast Guard TIER resource owners' identification of authorized users	Access Controls	1		X
CG-IT-11-04	Weaknesses Related to Information Assurance Professionals' Required Certifications	Security Management	1		X
CG-IT-11-05	Configuration Management Controls over the Scripting Process	Configuration Management	3		X
CG-IT-11-06	Civilian Background Investigations	Security Management	2		X
CG-IT-11-07	Contractor Background Investigations	Security Management	2		X
CG-IT-11-08	Security Awareness Issues Associated with the Social Engineering Testing	Security Management	2		X
CG-IT-11-09	Operations Systems Center Data Center Visitor Access Logs	Access Controls	1	X	
CG-IT-11-10	Direct Access and Direct Access II Audit Logging and General IT Control Validation	Access Controls	2		X
CG-IT-11-11	AMMIS Software Change Requests Process	Configuration Management	1		X
CG-IT-11-12	Shore Asset Management and Naval and Electronics Supply Support System Audit Log Review	Security Management	1		X
CG-IT-11-13	Direct Access System User Account Recertification	Access Controls	2		X
CG-IT-11-14	NESSS Access Authorizations	Access Controls	2		X
CG-IT-11-15	Lack of Consistent Contractor, Civilian, and Military Account Termination Notification Process for Coast Guard Systems	Security Management	2		X
CG-IT-11-16	Naval & Electronics Supply Support System Users Who Have Admin Capabilities	Access Controls	2		X

CG-IT-11-17	ALMIS User Recertification	Access Controls	2		X
CG-IT-11-18	Non-Compliance with FFMIA – Information Technology	Security Management	3		X
CG-IT-11-19	Weaknesses Associated with the Coast Guard Security Incident Database and Ticket System	Security Management	1	X	
CG-IT-11-20	Access and Configuration Management Controls – Vulnerability Assessment	Configuration Management	2	X	
CG-IT-11-21	Naval and Electronics Supply Support System User Account Recertification	Access Controls	2	X	

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, 2011

		Disposition	
NFR #	**Description**	**Closed**	**Repeat**
CG-IT-10-01	Lack of Consistent Contractor, Civilian, and Military Account Termination Process for Coast Guard Systems		X
CG-IT-10-02	Contractor Background Investigations		X
CG-IT-10-03	Civilian Background Investigations		X
CG-IT-10-04	Lack of implemented guidance related to financial statement impact assessment within the change control process	X	
CG-IT-10-05	Configuration Management Controls Over the Scripting Process		X
CG-IT-10-06	Security Awareness Issues associated with the Social Engineering Testing		X
CG-IT-10-07	JUMPS Authorized Users Tracking Weakness	X	
CG-IT-10-08	Coast Guard TIER System – Password Settings	X	
CG-IT-10-09	Security Awareness Issues Associated with Physical Protection of Sensitive Information		X
CG-IT-10-10	Weaknesses with Specialized Role-based Training for Individuals with Significant Security Responsibilities		X
CG-IT-10-11	Coast Guard TIER resource owners' identification of authorized users		X
CG-IT-10-12	User Account Recertification - Direct Access Application		X
CG-IT-10-13	Access and Configuration Management Controls – Vulnerability Assessment	X	
CG-IT-10-14	NESSS Access Authorizations		X
CG-IT-10-15	ALC Data Center and Facility Controls	X	
CG-IT-10-16	AMMIS Password Configuration	X	
CG-IT-10-17	Security Awareness Issues associated with Social Engineering Testing – Follow-up Testing		X
CG-IT-10-18	AMMIS Audit Log Review	X	
CG-IT-10-19	ALMIS User Recertification		X
CG-IT-10-20	AMMIS Software Change Requests Process		X
CG-IT-10-21	NESSS User Access Recertification		X
CG-IT-10-22	SAM and NESSS Audit Log Review		X
CG-IT-10-23	OSC Data Center Access Reviews	X	
CG-IT-10-24	Non-Compliance with FFMIA) – Information Technology		X
CG-IT-10-25	FINCEN Configuration Management Testing Approval Process	X	
CG-IT-10-26	ALC Information Technology Policies and Procedures	X	
CG-IT-10-27	NESSS Password Configuration	X	
CG-IT-10-28	Direct Access Audit Logging		X

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

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 e-mail your request to our OIG Office of Public Affairs at DHS-OIG.OfficePublicAffairs@dhs.gov. For additional information, visit our OIG website at www.oig.dhs.gov or follow us on Twitter @dhsoig.

OIG HOTLINE

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

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

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

- E-mail us at DHSOIGHOTLINE@dhs.gov; or

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

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