Department of Homeland Security

Office of Inspector General

Information Technology Management Letter for the United States Coast Guard Component of the FY 2012 Department of Homeland Security Financial Statement Audit

OIG-13-63

April 2013

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

April 4, 2013

MEMORANDUM FOR: Rear Admiral Robert Day
Chief Information Officer
United States Coast Guard

Rear Admiral Stephen P. Metruck
Chief Financial Officer
United States Coast Guard

FROM: Frank Deffer
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the United States Coast Guard Component of the FY 2012 Department of Homeland Security Financial Statement Audit*

Attached for your action is our final report, *Information Technology Management Letter for the United States Coast Guard Component of the FY 2012 Department of Homeland Security Financial Statement Audit.* The independent accounting firm KPMG LLP (KPMG) performed the audit of Department of Homeland Security (DHS) financial statements as of September 30, 2012, and prepared this information technology (IT) management letter.

KPMG is responsible for the attached IT management letter dated December 20, 2012, and the conclusion expressed in it. We do not express an opinion on DHS' financial statements or internal controls or conclusions on compliance with laws and regulations. The DHS management concurred with all recommendations.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Sharon Huiswoud, Director, Information Systems Audit Division, at (202) 254-5451.

Attachment

KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

April 2, 2013

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, 2012, and the related statements of net cost, changes in net position, and custodial activity, and combined statement of budgetary resources for the year then ended (referred to as the "fiscal year (FY) 2012 financial statements"). We were also engaged to audit the Department's internal control over financial reporting of the FY 2012 financial statements. The objective of our audit engagement was to express an opinion on the fair presentation of the FY 2012 financial statements and the effectiveness of internal control over financial reporting of the FY 2012 financial statements.

In accordance with *Government Auditing Standards*, our *Independent Auditors' Report*, dated November 14, 2012, included internal control deficiencies identified during our audit engagement that, in aggregate, represented a material weakness in information technology (IT) controls and financial system functionality at the DHS Department-wide level. This letter represents the separate limited distribution report mentioned in that report, of matters related to U.S. Coast Guard (USCG or Coast Guard).

During our audit engagement, we noted certain matters in the areas of access controls, configuration management, security management, and segregation of duties with respect to Coast Guard's financial systems general information technology controls (GITC) which we believe contribute to a DHS Department-wide material weakness in IT controls and financial system functionality. These matters are described in the *General IT Control Findings and Recommendations* section of this letter.

The 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 Coast Guard financial systems within the scope of the FY 2012 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 (OIG) and the DHS Chief Financial Officer.

This report is intended solely for the information and use of DHS management, DHS OIG, U.S. Office of Management and Budget, 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

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE, AND APPROACH

In connection with our engagement to audit the financial statements of DHS as of and for the year ended September 30, 2012, we performed an evaluation of general Information Technology (IT) controls (GITCs) at Coast Guard, to assist in planning and performing our audit engagement. The *Federal Information System Controls Audit Manual* (FISCAM), issued by 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 statement 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 statement audit. FISCAM also provides guidance to auditors when considering the scope and extent of review that generally should be performed when evaluating GITCs and the IT environment of a federal agency. FISCAM defines the following five control functions to be essential to the effective operation of GITCs and the IT 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 general IT controls audit, 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 were also included in the scope of technical security testing.

In addition to GITC testing, application controls were tested for the year ending September 30, 2012, which were identified as key controls by the financial audit team.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2012, Coast Guard took corrective action to address four of the prior year IT control weaknesses. For example, Coast Guard made improvements by strengthening its entity-wide incident response program and improving controls over user access at the USCG Finance Center (FINCEN), Operations Systems Center (OSC), Surface Forces Logistics Center (SFLC), and the Aviation Logistics Center (ALC). However, during FY 2012, we continued to identify general IT control weaknesses at Coast Guard, where in aggregate, 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, 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 of 1996* (FFMIA).

In FY 2012, our IT audit work identified twenty-one (21) IT findings, of which fourteen (14) were repeat findings from the prior year, five (5) were new findings, and two (2) were new findings that were remediated within the current fiscal year. In addition, we determined that Coast Guard remediated four (4) IT findings identified in previous years. Specifically, the Coast Guard took actions to improve aspects of its recertification of user accounts, entity-wide incident response program, user access policies and procedures, and reviewing 'super user' accounts to ensure those users needed this level of access based on the concept of least privilege. 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 four of the five FISCAM key control areas. The FISCAM areas impacted included Security Management, Access Control, Configuration Management, and Segregation of Duties. 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 significantly improving, designed and operating IT script change control policies and procedures;
2. Unverified access controls through the lack of user access privilege re-certifications and segregation of duties;
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;
6. Inadequately applied configuration management processes and procedures; and
7. 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.

GENERAL IT CONTROLS AND FINANCIAL SYSTEM FUNCTIONALITY FINDINGS AND RECOMMENDATIONS

Findings:

During our engagement to audit the FY 2012 DHS financial statements, we identified the following Coast Guard IT and financial system control deficiencies. Our findings are divided into two groupings: 1) financial systems controls and 2) IT system functionality.

Related to IT Financial Systems Controls

Configuration Management

- Inconsistencies of data within the script record documentation existed.
- Configuration Management (CM) records did not contain all required approvals as required by Coast Guard policy.
- Functional Configuration Audits (FCAs) and Physical Configuration Audits (PCAs) were not completed as required by Coast Guard policy.
- Critical, high, and medium risk vulnerabilities existed relating to inadequate patches and CM.

Access Controls

- New user access forms do not contain required supervisor approvals, some signatures were illegible, as well as some new users were granted access before their form was approved.
- User roles were changed without required prior approval.
- Users were granted roles that were not documented on their user access form.
- 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. Furthermore, recertifications for some systems were not performed.
- Data Center visitor access logs are not consistently completed fully and appropriately.
- There is a lack of a consistent contractor, civilian and military account termination notification process for Coast Guard systems.
- Users had inappropriate access to audit log files.
- Audit log reviews for key financial systems are not being conducted on all key information, as well as not being reviewed by an independent party.

Segregation of Duties

- The system administrator and database administrator of one system can perform each other's duties, resulting in improper segregation of duties.

Security Management

- Background investigations for all civilian employees have not been completed at the Minimum Background Investigation (MBI) level as required by DHS guidance.
- Background investigations for all contractor employees have not been completed at the Background Investigation (BI) level as required by DHS guidance.
- Not all Information Assurance (IA) professionals have the required certification or evidence of Continuing Professional Education (CPE) as required by Coast Guard policy.
- 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.

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)	17	17	0
FINCEN	9*	5	0
SFLC	8	8	1
*KPMG called less than the total sample size since testing ceased when FINCEN management distributed a notification of social engineering attempts to all FINCEN employees.			

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 below table provides a summary of our testing results.

Weaknesses Observed During After Hours Physical Security Testing					
	Coast Guard Locations Tested				**Total Exceptions by Type**
Exceptions Noted (1)	**HQ**	**FINCEN**	**ALC**	**SFLC**	
Passwords (2)	7	0	1	4	**12**
Common Access Card	0	0	0	3	**3**
For Official Use Only	3	0	1	17	**21**
Personally Identifiable Information	3	1	1	9	**14**
Keys (3)	0	0	0	1	**1**
External Drive, Other Media	4	0	1	0	**5**
Unsecured Burn Bag (4)	1	0	0	0	**1**
Checks	0	3	3	0	**6**
Total Exceptions by Location	**18**	**4**	**7**	**34**	**63**

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 – 46
FINCEN – 80
ALC – 44
SFLC – 36

(1) There were cases of multiple exceptions in a single workspace, but the type of exception was only noted as 1 exception. For example, one cubicle had multiple 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) The key was to the government vehicle, which also contained the fleet card for the vehicle.
(4) Burn bag contained sensitive documentation.

Related to Financial System Functionality

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:

- The Coast Guard's core financial system configuration management process relies on an IT script process as a solution primarily to compensate for system functionality and data quality issues.
- 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).
- The budgetary module of the core financial system is not activated. As a result, key attributes (e.g., budget fiscal year) are missing and potential automated budgetary entries (e.g., upward adjustments) are not possible. This has created the need for various manual workarounds and non-standard adjustments (i.e., topsides) to be implemented.
- 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:
  - Receipting for goods and services upon delivery. As a result, the Coast Guard records a manual estimate of potential receipted goods and services at year end in the general ledger;
  - 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 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 Chief Information Officer (CIO) and Chief Financial Officer (CFO), in coordination with the DHS Office of Chief Financial Officer (OCFO) and the DHS Office of the Chief Information Officer (OCIO)**,** make the following improvements to Coast Guard's financial management systems and associated information technology security program.

Configuration Management:

- Provide training to employees to facilitate standardized script testing procedures to ensure consistent compliance with FINCEN CM policies and procedures.
- Update its CM procedures to ensure that all proper reviews and associated approvals are obtained for every System Change Request prior to implementation.
- Update its CM procedures to include a final review step to ensure that a complete FCA is performed for each system change, including a PCA.
- Implement its improved CM plan and provide appropriate training to ensure that it is followed.
- Update its procedures to ensure that patches are applied within a time interval consistent with the criticality of the vulnerability, or that risk is reduced to an acceptable level.

Access Controls:

- Update user guides to ensure that forms are completed and signed before the user account is provided with a username and password.
- Update policies and procedures to ensure proper approval is obtained on user access forms before access or changes are made.
- Collaboratively work with DHS Headquarters on a policy compliance strategy and implementation in regards to a 100% user recertification.
- Complete the implementation of new user revalidation procedures.
- Update its procedures to retain documentation of user account reviews and evidence showing completion of annual user account rectification.
- Implement appropriate monitoring controls around visitor procedures to ensure that data center visitor logs are reviewed for completeness.
- Improve existing enterprise-wide processes to ensure that impacted system owners are consistently notified of terminated, transferred, or retired contractor, military, and civilian personnel.
- Remove inappropriate access to system audit logs from users without a business justification commensurate with job responsibilities.
- Issue a Request for Proposal for a new contract to be awarded that requires the service provider to provide audit log review results as well as issue a report in accordance with Statement on Standards for Attestation Engagements No. 16.
- Fully implement the planned Security Information and Event Management tool to ensure that audit logs are reviewed appropriately.

Segregation of Duties:

- Update the risk analysis in regards to segregating duties between the system and database administrator.

Security Management:

- Implement appropriate monitoring controls around personnel security processes to ensure that FINCEN staff and contractors in positions with financial impact are consistently and fully adjudicated through the MBI and BI clearance processes, respectively.
- Implement appropriate monitoring controls around IA Professional certification tracking and data gathering procedures to ensure that records of IA Professional competencies are consistently documented and maintained and IA Certification clauses are incorporated into applicable contracts.
- Perform internal social engineering testing to re-enforce training and best practices.
- Update the Security Awareness Training to reflect best practices pertaining to physical protection of sensitive information and to advise employees of possible administrative actions.

Financial System Functionality:

We recommend that the Coast Guard's CIO and CFO make necessary improvements to the financial management systems and their supporting IT security.

APPLICATION CONTROLS

Select application controls were tested for the year ending September 30, 2012, and no issues were identified associated with those applications selected for test work.

Appendix A

Description of Key Coast Guard Financial Systems and IT Infrastructure within the Scope of the FY 2012 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 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 (WINS) and the Financial and Procurement Desktop (FPD).

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 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 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 general 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 Information Systems Division in 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.

Integrated Aids to Navigation Information System (IATONIS)

IATONIS is a comprehensive system for managing and reporting on Aids to Navigation and related navigational matters. IATONIS incorporates the Local Notice to Mariners, which is the USCG's primary means for disseminating information concerning changes to aids to navigation, menaces to navigation, and other timely items of interest to mariners. Additionally, it produces the Light List, the USCG's official list of all aids to navigation.

Appendix B

FY 2012 Notices of IT Findings and Recommendations at Coast Guard

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2012

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CG-IT-12-01	Lack of Consistent Contractor, Civilian, and Military Account Termination Notification Process	Access Controls		X
CG-IT-12-02	Civilian Background Investigations	Security Management		X
CG-IT-12-03	Contractor Background Investigations	Security Management		X
CG-IT-12-04	Inappropriate Access to JUMPS SMF Audit Logs	Access Controls	X	
CG-IT-12-05	Direct Access & Direct Access II Audit Logging	Access Controls		X
CG-IT-12-06	OSC Data Center Visitor Access Logs	Access Controls		X
CG-IT-12-07	Physical Configuration Audits of NESSS System Changes	Configuration Management	X	
CG-IT-12-08	Direct Access and Direct Access II PeopleSoft System Administrator and Security Administrator Accounts	Access Controls	X	
CG-IT-12-09	Security Awareness Issues Identified During Social Engineering Testing at Surface Forces Logistics Center	Access Controls		X
CG-IT-12-10	Security Awareness Issues Associated with Physical Protection of Sensitive Information	Access Controls		X
CG-IT-12-11	Weaknesses related to IA Professionals' Required Certifications	Security Management		X
CG-IT-12-12	Naval & Electronics Supply System User Access	Access Controls		X
CG-IT-12-13	AMMIS Software Change Requests Process	Configuration Management		X
CG-IT-12-14	Configuration Management Controls over the Scripting Process	Configuration Management		X
CG-IT-12-15	Direct Access User Account Recertification	Access Controls		X
CG-IT-12-16	Access and Configuration Management Controls – Vulnerability Assessment	Configuration Management		X
CG-IT-12-17	IATONIS Audit Log Review	Access Controls	X	
CG-IT-12-18	IATONIS Separation of Duties	Segregation of Duties	X	
CG-IT-12-19	Functional Configuration Audits of IATONIS System Changes	Configuration Management	X	

Department of Homeland Security
United States Coast Guard
Information Technology Management Letter
September 30, 2012

FY 2012 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CG-IT-12-21	NESSS User Recertification	Access Controls		X
CG-IT-12-22	IATONIS Account Recertification	Access Controls	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, 2012

NFR #	Description	Disposition	
		Closed	Repeat
CG-IT-11-01	Security Awareness Issues Associated with Physical Protection of Sensitive Information		X
CG-IT-11-02	Direct Access and Direct Access II User and System Administrator Account Management and Approval	X	
CG-IT-11-03	CG-TIER resource owners' identification of authorized users	X	
CG-IT-11-04	Weaknesses Related to IA Professionals' Required Certifications		X
CG-IT-11-05	Configuration Management Controls over the Scripting Process		X
CG-IT-11-06	Civilian Background Investigations		X
CG-IT-11-07	Contractor Background Investigations		X
CG-IT-11-08	Security Awareness Issues Associated with the Social Engineering Testing		X
CG-IT-11-09	OSC Data Center Visitor Access Logs		X
CG-IT-11-10	Direct Access and Direct Access II Audit Logging and General IT Control Validation		X
CG-IT-11-11	AMMIS Software Change Requests Process		X
CG-IT-11-12	SAM and NESSS Audit Log Review	X	
CG-IT-11-13	Direct Access System User Account Recertification		X
CG-IT-11-14	NESSS Access Authorizations		X
CG-IT-11-15	Lack of Consistent Contractor, Civilian, and Military Account Termination Notification Process for Coast Guard Systems		X
CG-IT-11-16	Naval & Electronics Supply Support System Users Who Have Admin Capabilities	X	
CG-IT-11-17	ALMIS User Recertification	X	
CG-IT-11-18	Non-Compliance with FFMIA – Information Technology	X	
CG-IT-11-19	Weaknesses Associated with the Coast Guard Security Incident Database and Ticket System	X	
CG-IT-11-20	Access and Configuration Management Controls – Vulnerability Assessment		X
CG-IT-11-21	Naval and Electronics Supply Support System User Account Recertification		X

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or you may call 1 (800) 323-8603; or fax it directly to us at (202) 254-4297.

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